



C. L. Brumback

Primary Care Clinics

Health Care District Palm Beach County

BOARD OF DIRECTORS

December 11, 2019

12:45 P.M.

Meeting Location

1515 N. Flagler Drive, Suite 101

West Palm Beach, FL 33401

If a person decides to appeal any decision made by the board, with respect to any matter at such meeting or hearing, he will need a record of the proceedings, and that, for such purpose, he may need to ensure that a verbatim record of the proceedings made, which record includes the testimony and evidence upon which the appeal is to be based.

**BOARD OF DIRECTORS MEETING
AGENDA**

December 11, 2019

**1515 N Flagler Drive, Suite 101
West Palm Beach, FL 33401**

1. Call to Order – James Elder, Chair

- A. Roll Call
- B. Affirmation of Mission: To provide compassionate, comprehensive health services to all Palm Beach County residents, through collaboration and partnership, in a culturally sensitive environment.

2. Agenda Approval

- A. Additions/Deletions/Substitutions
- B. Motion to Approve Agenda

3. Awards, Introductions and Presentations

- A. Operational Site Visit (OSV) informational session.
(Genua Consulting, LLC)
- B. 2019 AHRQ Safety Culture Survey Results.
(Martha Hyacinthe)

4. Disclosure of Voting Conflict

5. Public Comment

6. Meeting Minutes

- A. **Staff recommends a MOTION TO APPROVE:**
Board Meeting Minutes of October 30, 2019. [Pages 1-11]

7. Consent Agenda – Motion to Approve Consent Agenda Items

All matters listed under this item are considered routine and action will be taken by one motion. There will be no separate discussion of these items unless a Commissioner or person so requests, in which the item will be removed from the general order of business and considered on its normal sequence on the Agenda.

A. ADMINISTRATION

7A-1 RECEIVE AND FILE:

December 2019 Internet Posting of District Public Meeting.
<https://www.hcdpbc.org/resources/public-meetings>

7. Consent Agenda – Motion to Approve Consent Agenda Items (continued)

- 7A-2 **RECEIVE AND FILE:**
Attendance tracking. [Page 12]
- 7A-3 **Staff Recommends a MOTION TO APPROVE:**
Bylaws Update.
(Valerie Shahriari) [Pages 13-38]
- 7A-4 **Staff Recommends a MOTION TO APPROVE:**
Contracts Policy Adoption.
(Valerie Shahriari) [Pages 39-40]
- 7A-5 **Staff Recommends a MOTION TO APPROVE:**
Compliance Policy Updates.
(Deborah Hall) [41-123]
- 7A-6 **Staff Recommends a MOTION TO APPROVE:**
IT Policies Adoption.
(Patricia Lavelly) [124-232]

B. FINANCE

- 7B-1 **Staff Recommends a MOTION TO APPROVE:**
C. L. Brumback Primary Care Update of Current Charge Master.
(Joel Snook) [Pages 233-257]
- 7B-2 **Staff Recommends a MOTION TO APPROVE:**
Finance Policies Adoption.
(Joel Snook) [Pages 258-265]

8. Regular Agenda

A. ADMINISTRATION

- 8A-1 **RECEIVE AND FILE:**
Executive Director Leadership Performance Results 2019.
(Thomas Cleare) [Pages 266-268]
- 8A-2 **RECEIVE AND FILE:**
Board Self-Evaluation Tallied Results 2019.
(Thomas Cleare) [Pages 269-272]

8. Regular Agenda (continued)

8A-3 **RECEIVE AND FILE:**

2019 Palm Beach County Community Health Assessment and Lakeside Medical Center Community Health Needs Assessment.
(Thomas Cleare) [Under Separate Cover]

B. EXECUTIVE

8B-1 **RECEIVE AND FILE:**

Executive Director Informational Update.
(Dr. Belma Andric) [Pages 275-276]

C. OPERATIONS

8C-1 **Staff Recommends a MOTION TO APPROVE:**

Operations Reports – November 2019.
(Dr. Hyla Fritsch) [Pages 277-298]

D. CREDENTIALING AND PRIVILEGING

8D-1 **Staff Recommends a MOTION TO APPROVE:**

Licensed Independent Practitioner Credentialing and Privileging
(Sarah Gonzalez) [Pages 299-301]

E. QUALITY

8E-1 **Staff Recommends a MOTION TO APPROVE:**

Patient Relations Report.
(David Speciale) [Pages 302-305]

8E-2 **Staff Recommends a MOTION TO APPROVE:**

Quality Report.
(Dr. Ana Ferwerda) [Pages 306-311]

- 9. VP and Executive Director of Clinic Services Comments**
- 10. Board Member Comments**
- 11. Closed Risk Meeting [Under Separate Cover]**

12. Establishment of Upcoming Meetings

January 29, 2020 (HCD Board Room)

12:45pm Board of Directors

February 26, 2020 (HCD Board Room)

12:45pm Board of Directors

March 25, 2020 (HCD Board Room)

12:45pm Board of Directors

April 29, 2020 (HCD Board Room)

12:45pm Board of Directors

May 27, 2020 (HCD Board Room)

12:45pm Board of Directors

June 24, 2020 (HCD Board Room)

12:45pm Board of Directors

July 29, 2020 (HCD Board Room)

12:45pm Board of Directors

August 26, 2020 (HCD Board Room)

12:45pm Board of Directors

September 30, 2020 (HCD Board Room)

12:45pm Board of Directors

October 28, 2020 (HCD Board Room)

12:45pm Board of Directors

November 25, 2020 (HCD Board Room)

12:45pm Board of Directors

December 16, 2020 (HCD Board Room)

12:45pm Board of Directors

13. Motion to Adjourn

The logo features a stylized white cross with horizontal lines, set within a dark blue circle. The background consists of several diagonal blue stripes of varying shades, creating a dynamic, sunburst-like effect.

Health Care District of Palm Beach County

Dedicated to the health of our community

AHRQ Safety Culture Survey 2019 Results

Martha Benghie Hyacinthe, MSN-FNP, MBA(c), CPHRM, SSBB
Director, Corporate Risk Management

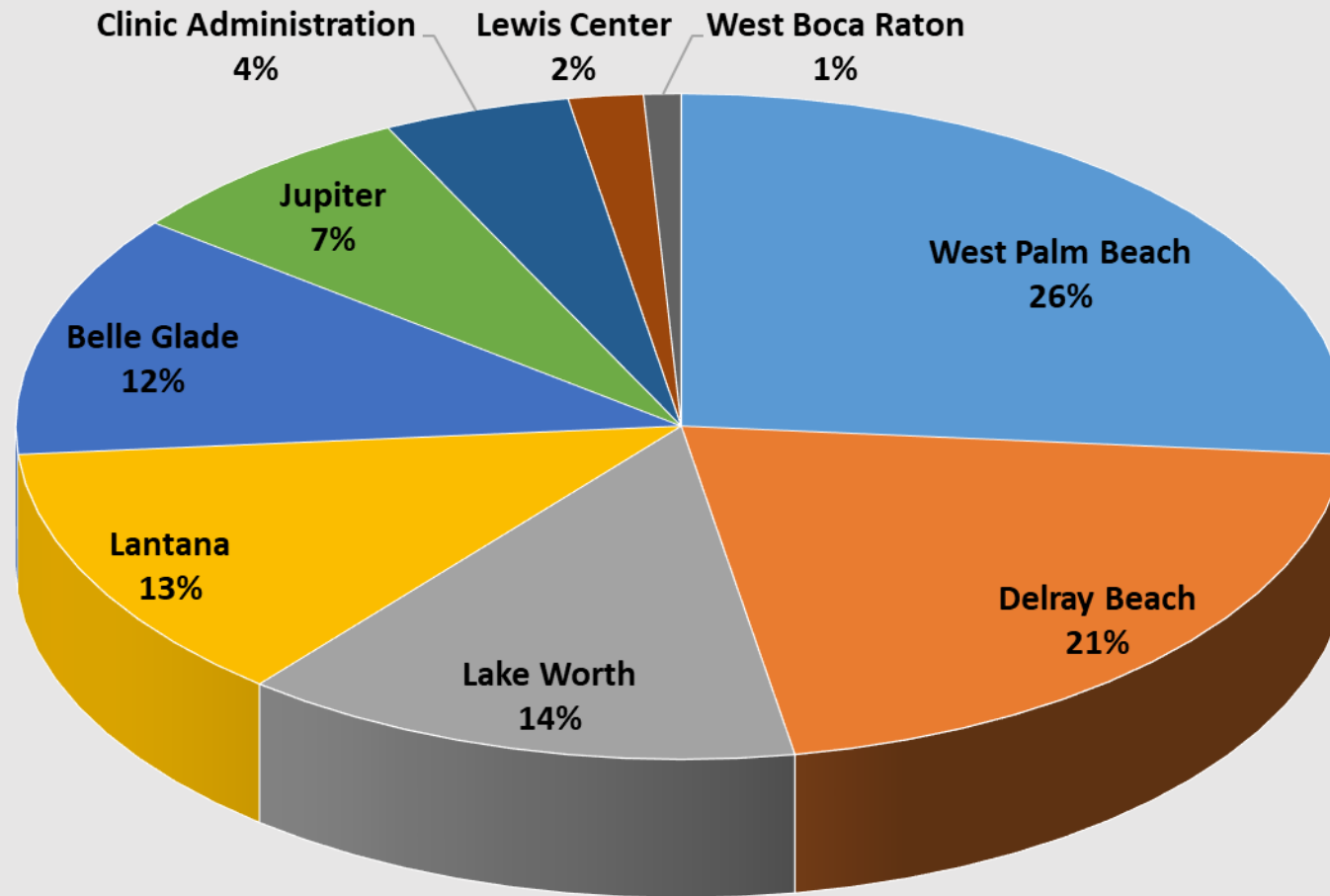


AHRQ Survey Overview

- **Purpose**
 - Raise staff awareness about patient safety
 - Identify strengths and areas for patient safety culture improvement
 - Examine trends in patient safety culture change over time
 - Evaluate the cultural impact of patient safety initiatives and interventions
- **Survey composition:**
 - 7 sections
 - 65 questions including those in the subsections
- **Survey**
 - Conducted for a period of **15 days** (October 1-15)
 - Opportunity provided to all primary care clinics employees via SharePoint & Email.
 - **110 total surveys submitted in 2019**
 - **46 total submitted in 2018**
- **Results (2019)**
 - Overall - Positive
 - 15 questions data will be shared

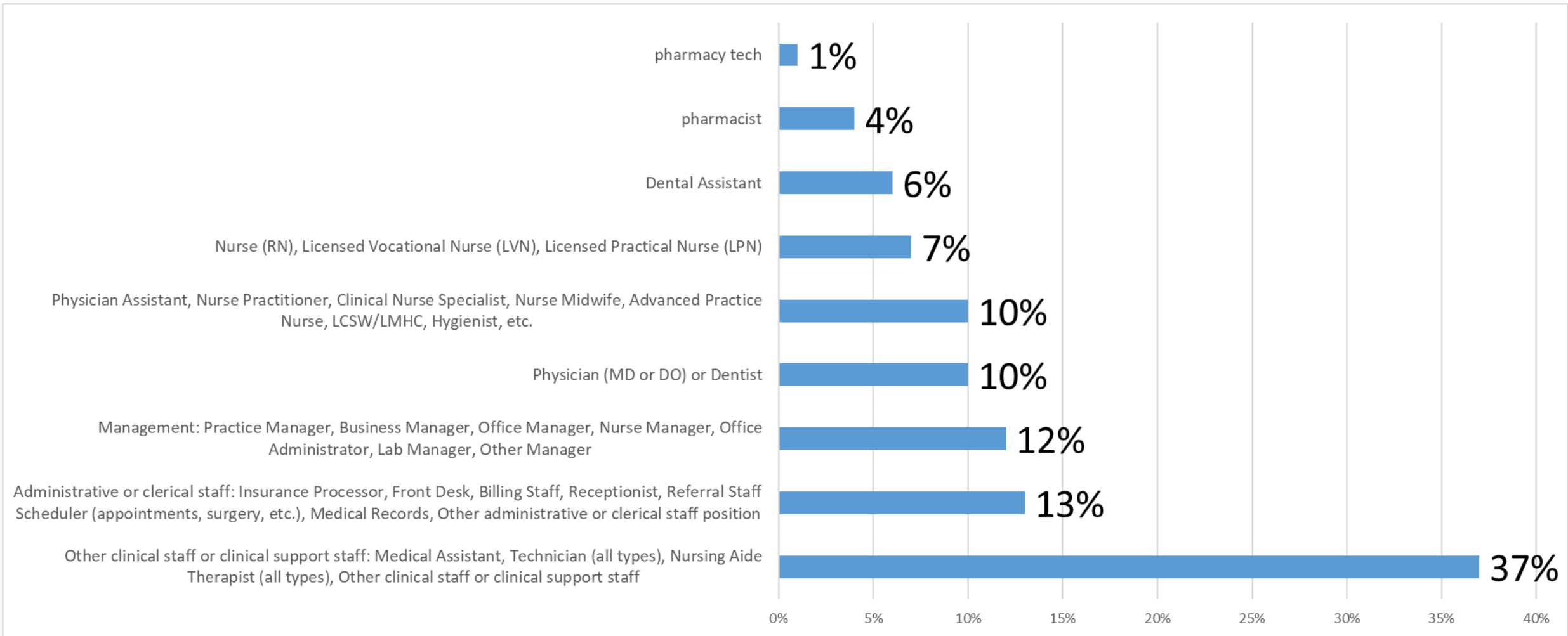


Clinic locations



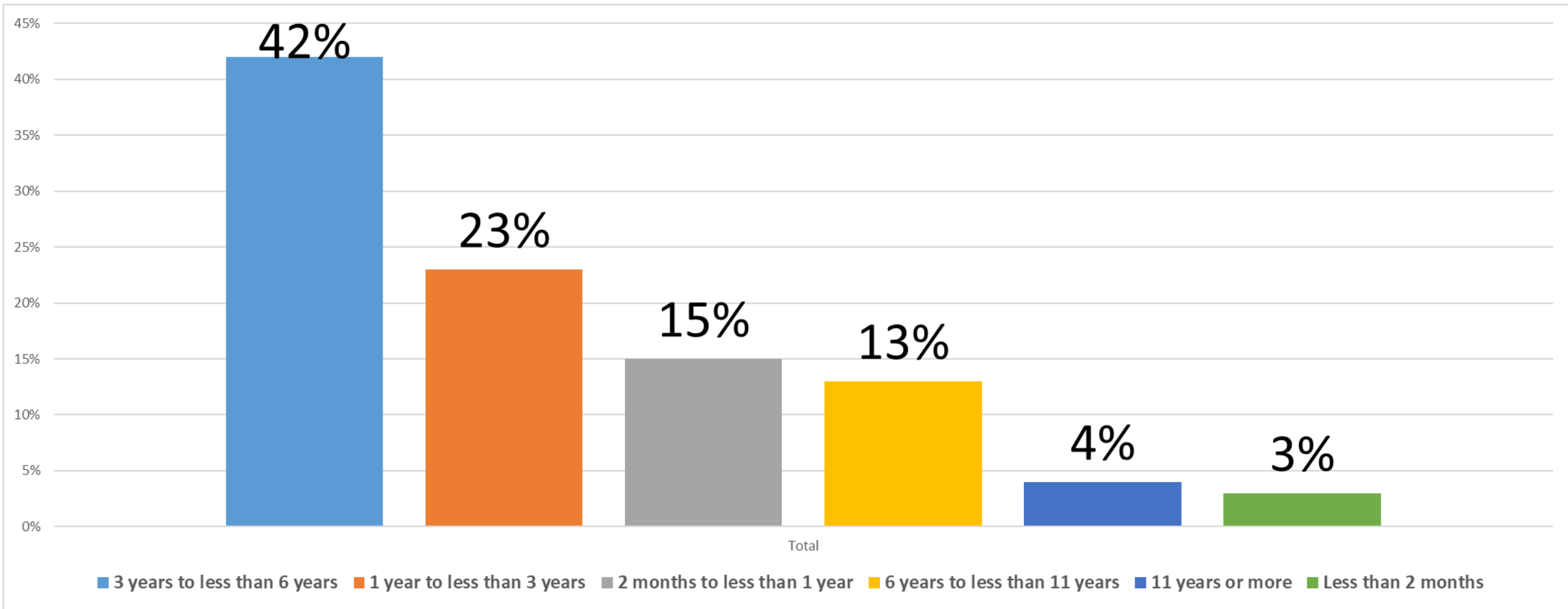


What is your position in this office? Check ONE category that best applies to your job.



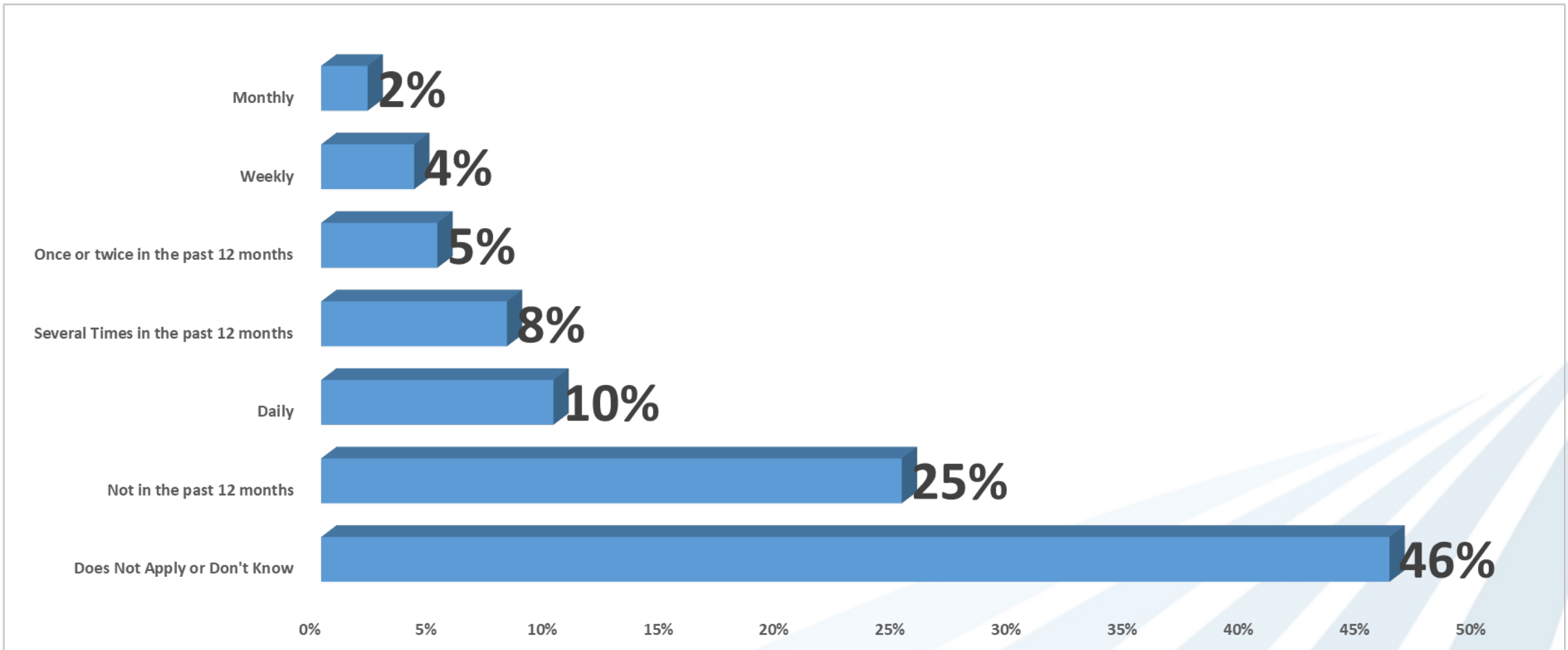


How long have you worked in this medical office location?



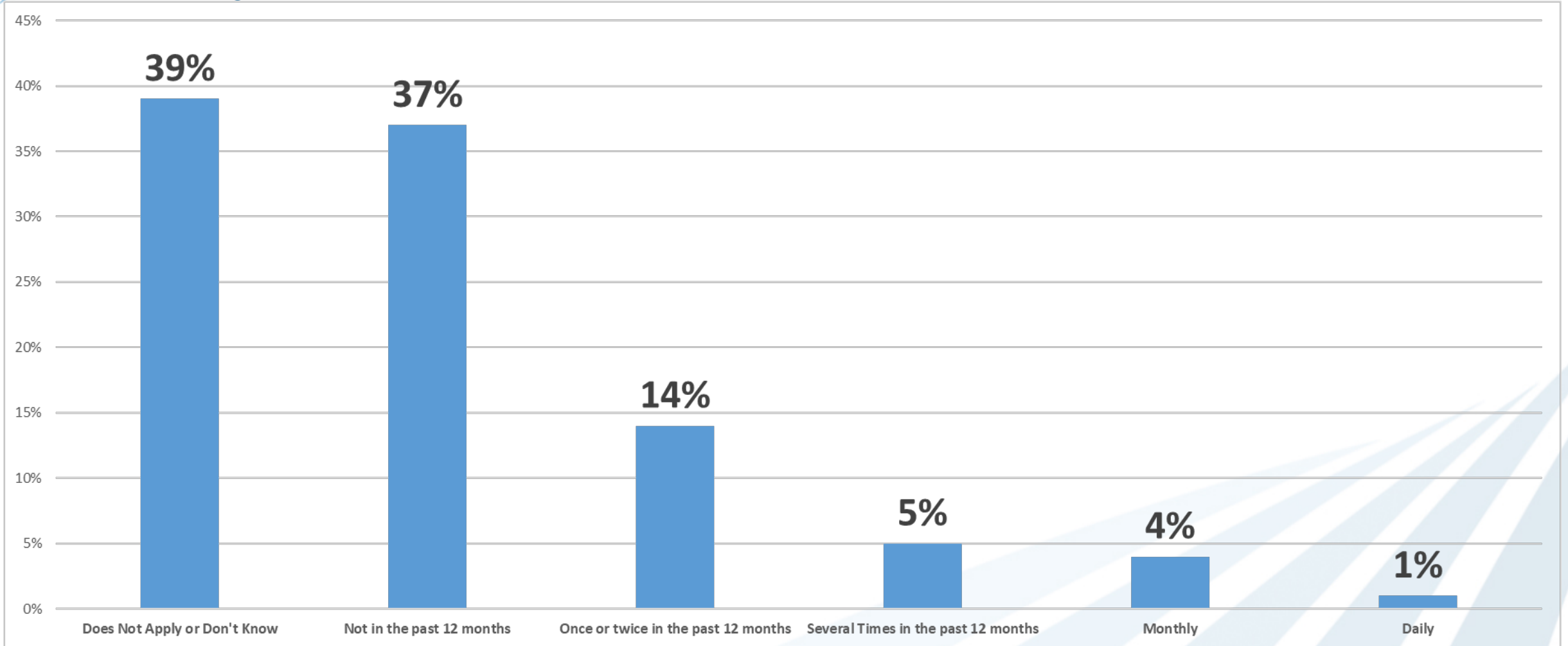


The following items describe things that can happen in medical offices that affect patient safety and quality of care. In your best estimate, how often did the following things happen in your medical office OVER THE PAST 12 MONTHS? [ACCESS TO CARE - A patient was unable to get an appointment within 48 hours for an acute/serious problem]



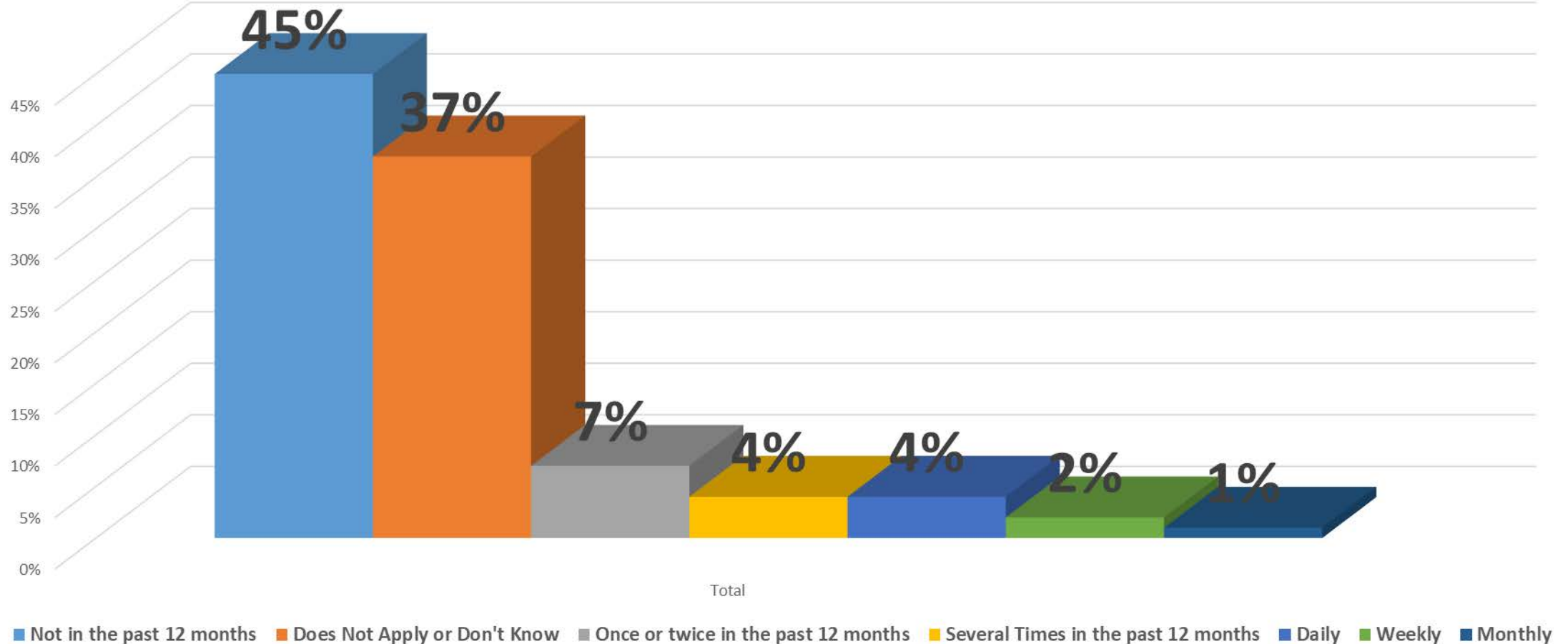


The following items describe things that can happen in medical offices that affect patient safety and quality of care. In your best estimate, how often did the following things happen in your medical office OVER THE PAST 12 MONTHS? [PATIENT IDENTIFICATION - The wrong chart/medical record was used for a patient]



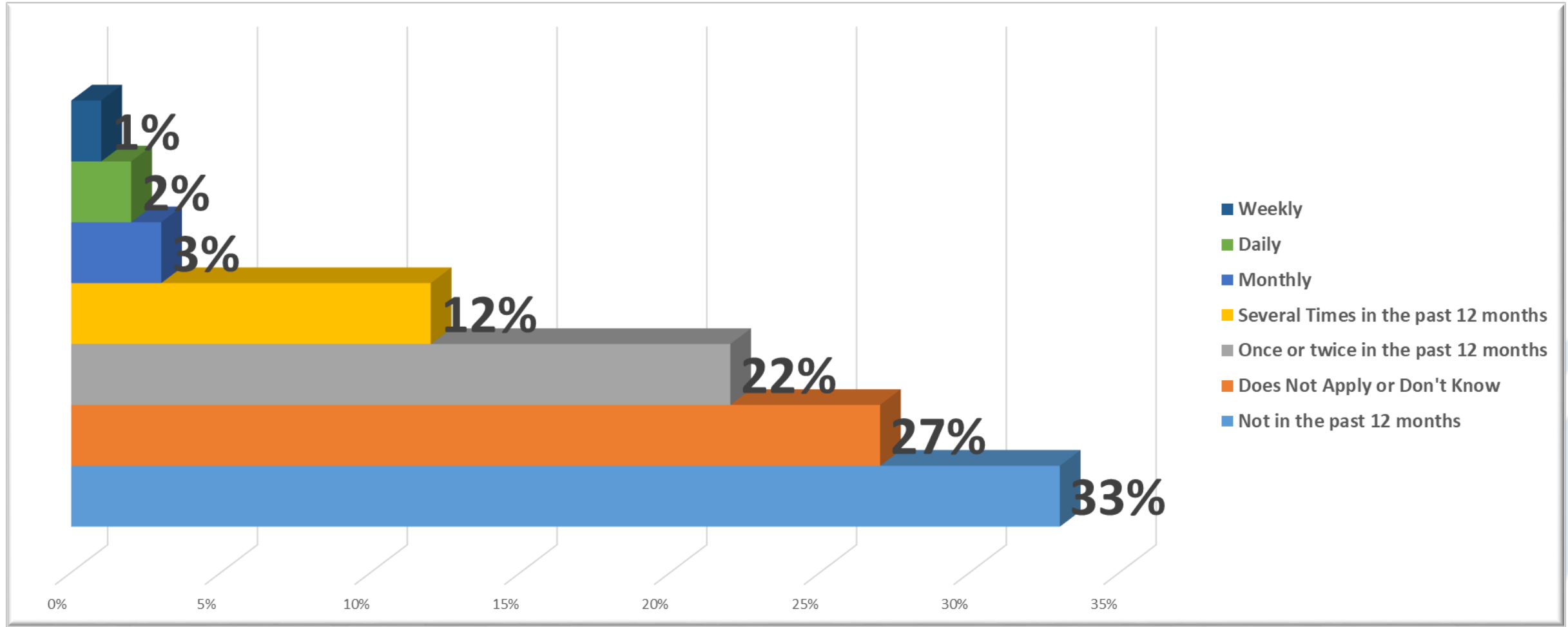


The following items describe things that can happen in medical offices that affect patient safety and quality of care. In your best estimate, how often did the following things happen in your medical office OVER THE PAST 12 MONTHS? [CHARTS/MEDICAL RECORDS - A patients chart/medical record was not available when needed]



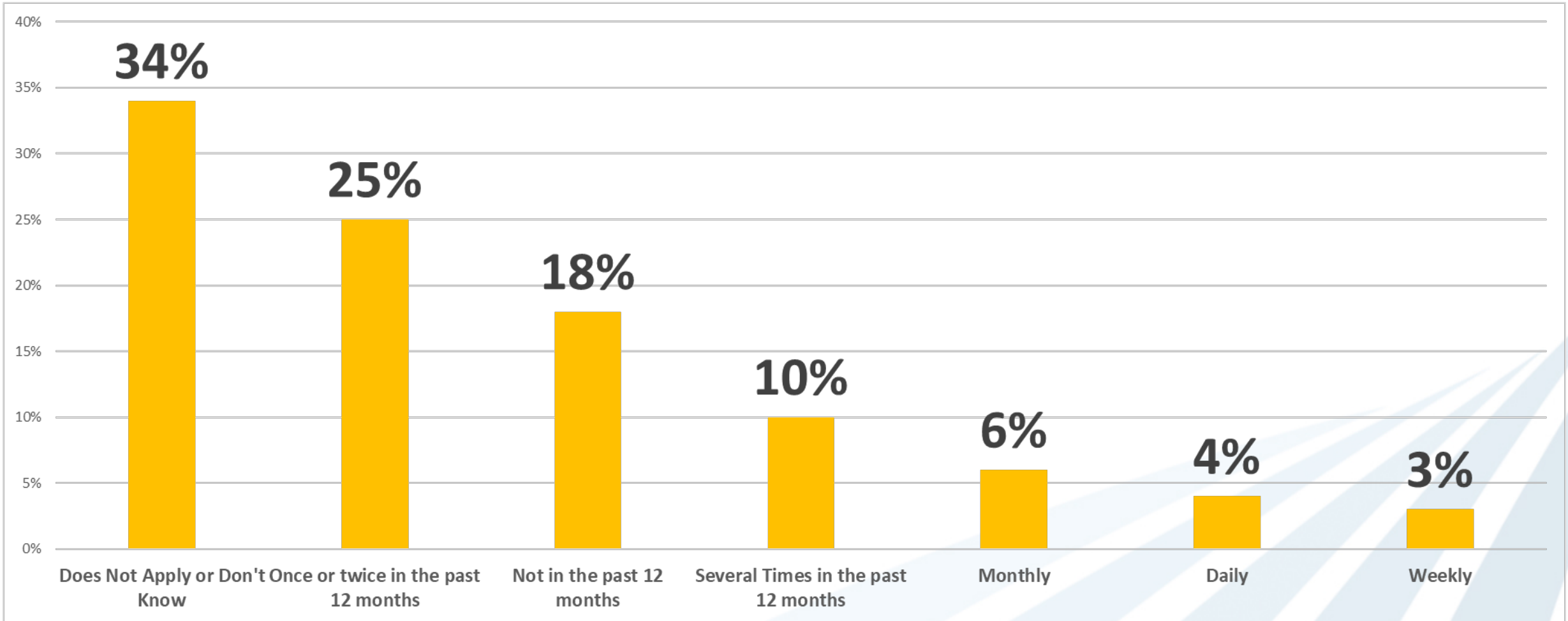


The following items describe things that can happen in medical offices that affect patient safety and quality of care. In your best estimate, how often did the following things happen in your medical office **OVER THE PAST 12 MONTHS?** [CHARTS/MEDICAL RECORDS - Medical information was filed, scanned, or entered into the wrong patients chart/medical record]



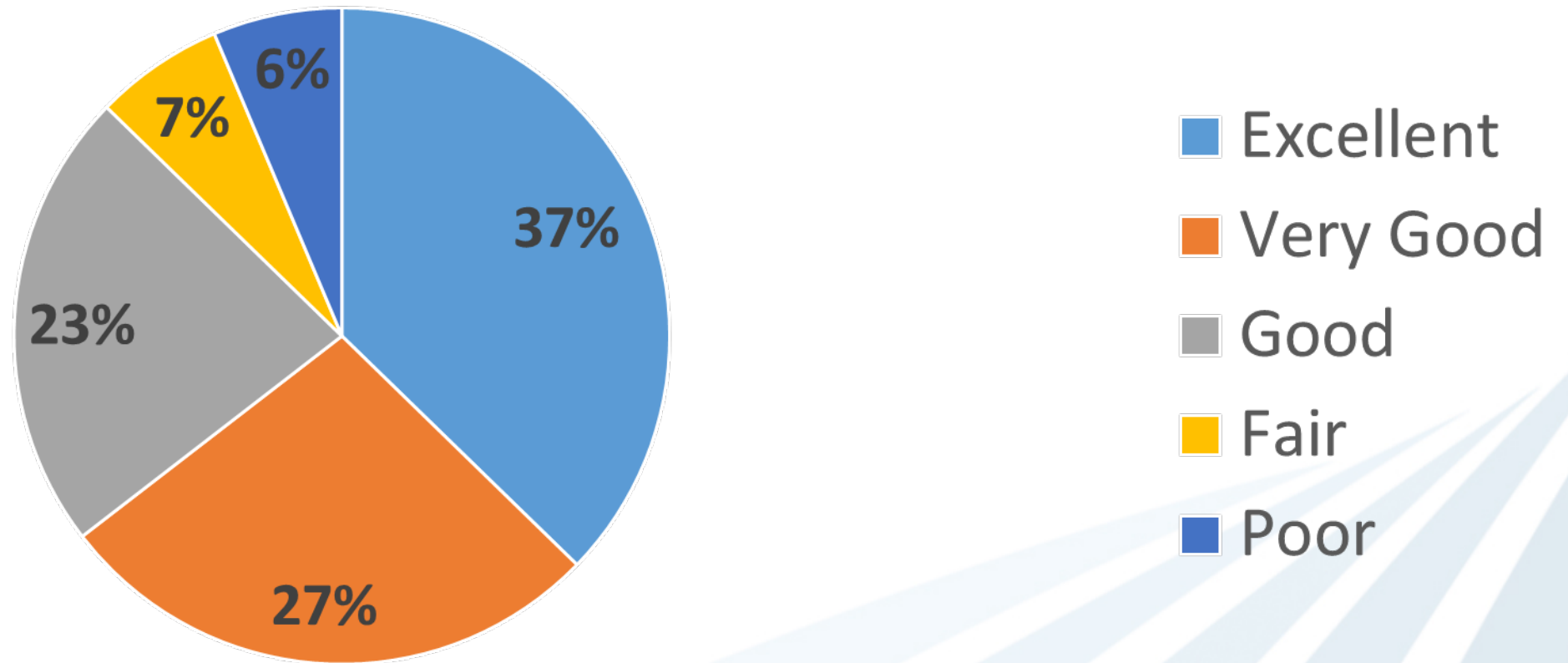


The following items describe things that can happen in medical offices that affect patient safety and quality of care. In your best estimate, how often did the following things happen in your medical office OVER THE PAST 12 MONTHS? [MEDICAL EQUIPMENT - Medical equipment was not working properly or was in need of repair or replacement]



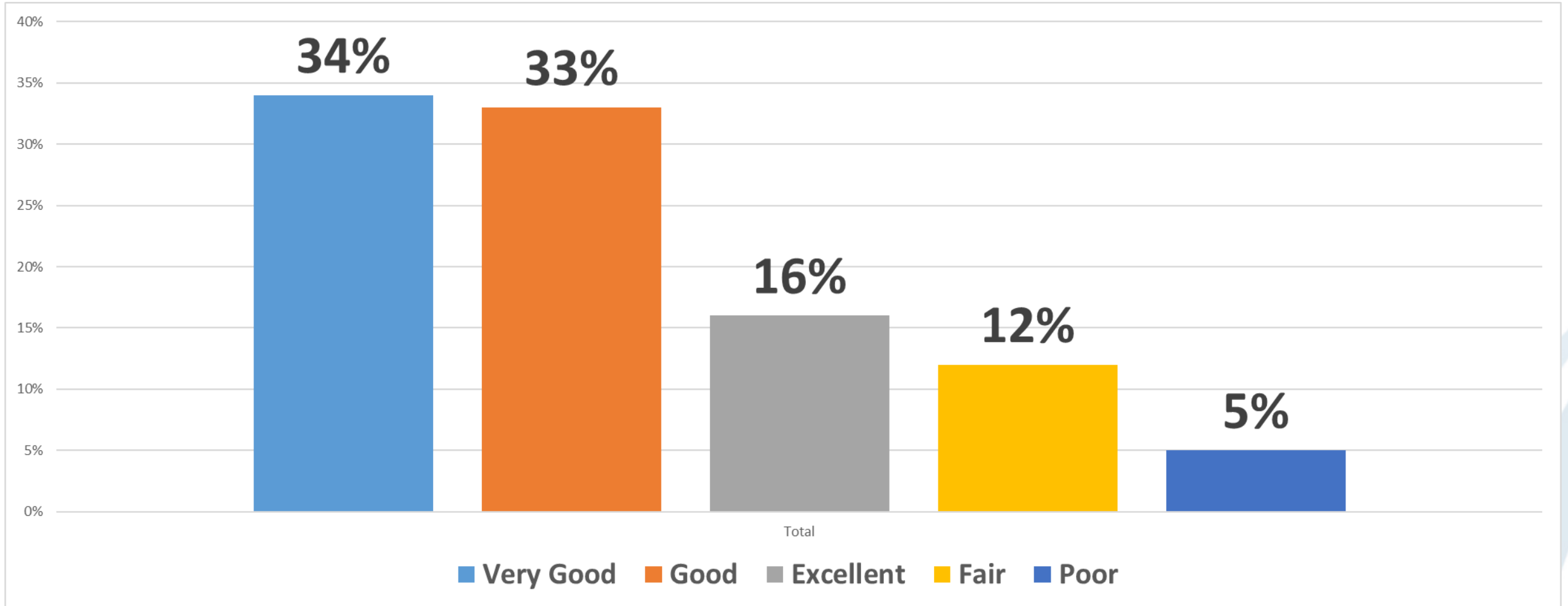


Overall Ratings on Quality: Overall, how would you rate your medical office on each of the following areas of health care quality? [Equitable - Provides the same quality of care to all individuals regardless of gender, race, ethnicity, socioeconomic]



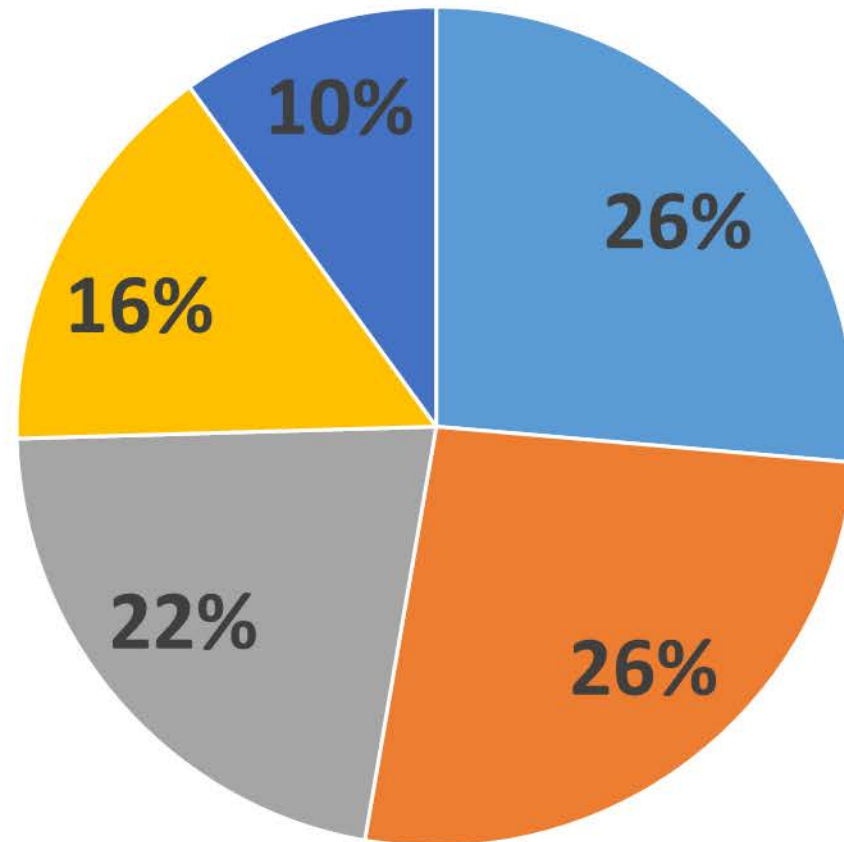


Overall Ratings on Quality: Overall, how would you rate your medical office on each of the following areas of health care quality? [Efficient - Ensures cost-effective care (avoids waste, overuse, and misuse of services)]





Overall Ratings on Quality: Overall, how would you rate your medical office on each of the following areas of health care quality? [Timely - Minimizes waits and potentially harmful delays]



Fair

Good

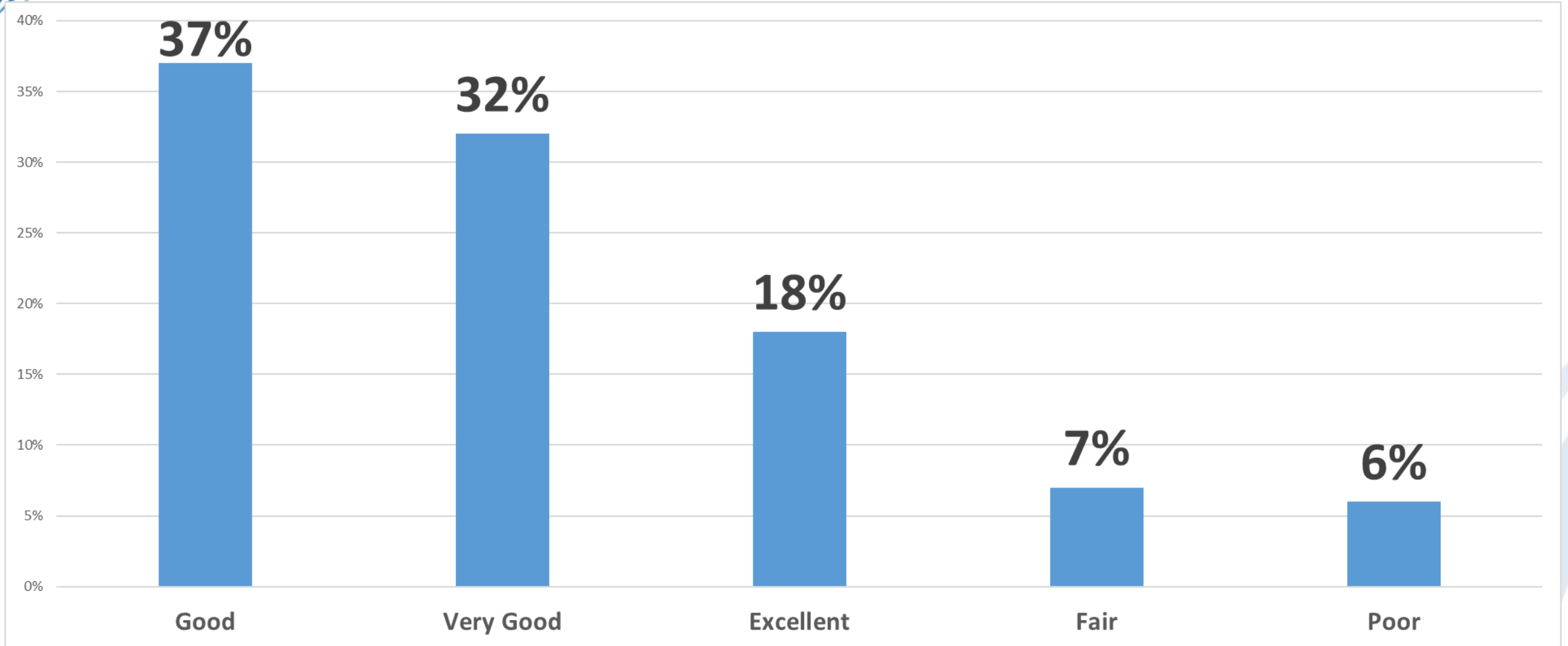
Very Good

Poor

Excellent

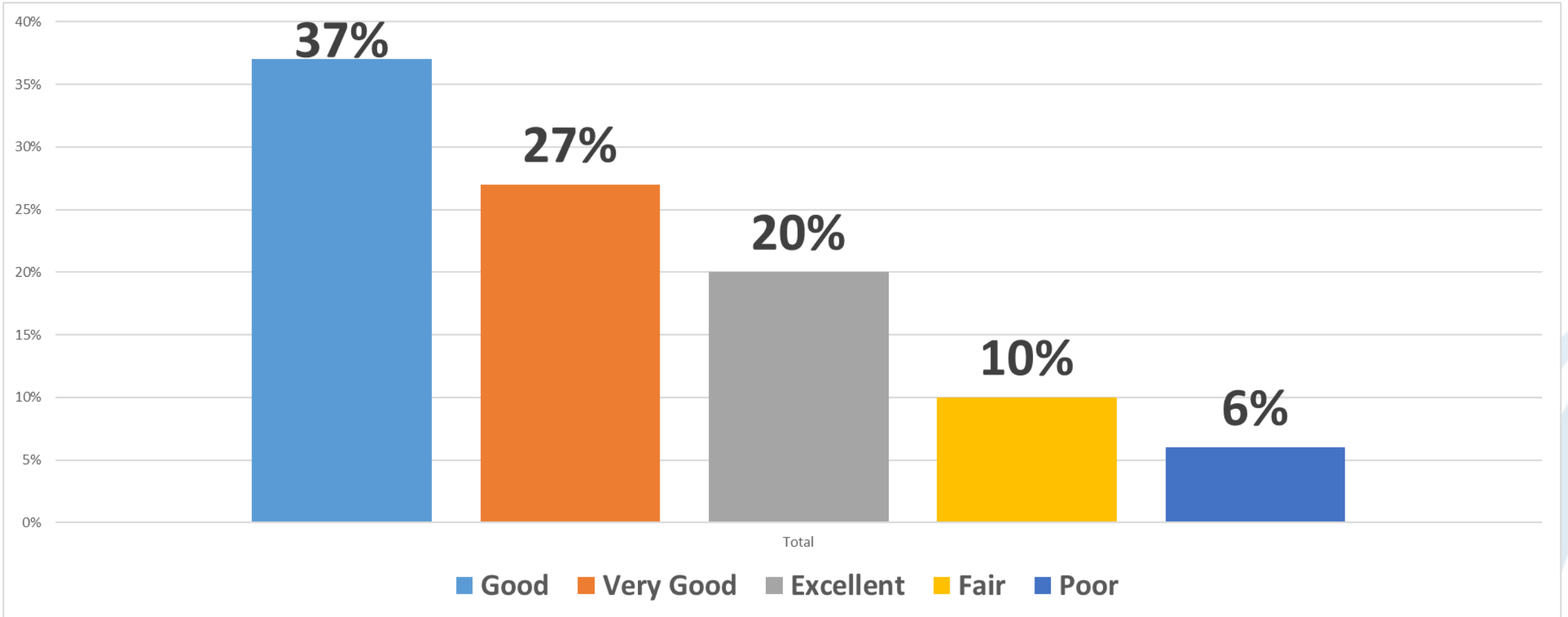


Overall Ratings on Quality: Overall, how would you rate your medical office on each of the following areas of health care quality? [Effective - Is based on scientific knowledge]



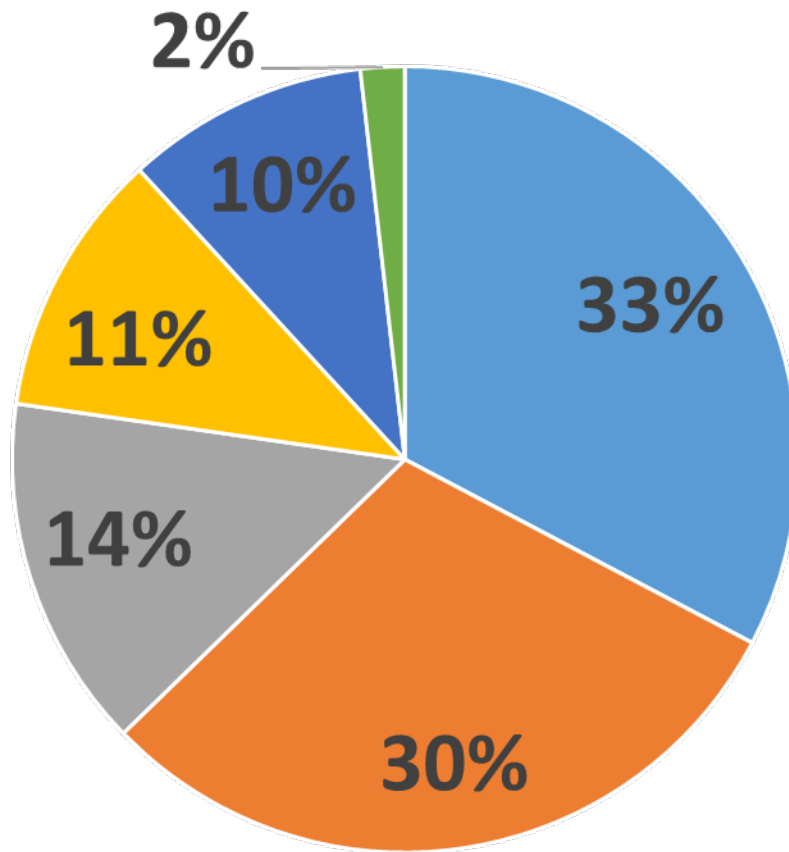


Overall Ratings on Quality: Overall, how would you rate your medical office on each of the following areas of health care quality? [Patient Centered - Is responsive to individual patient preferences, needs, and values]





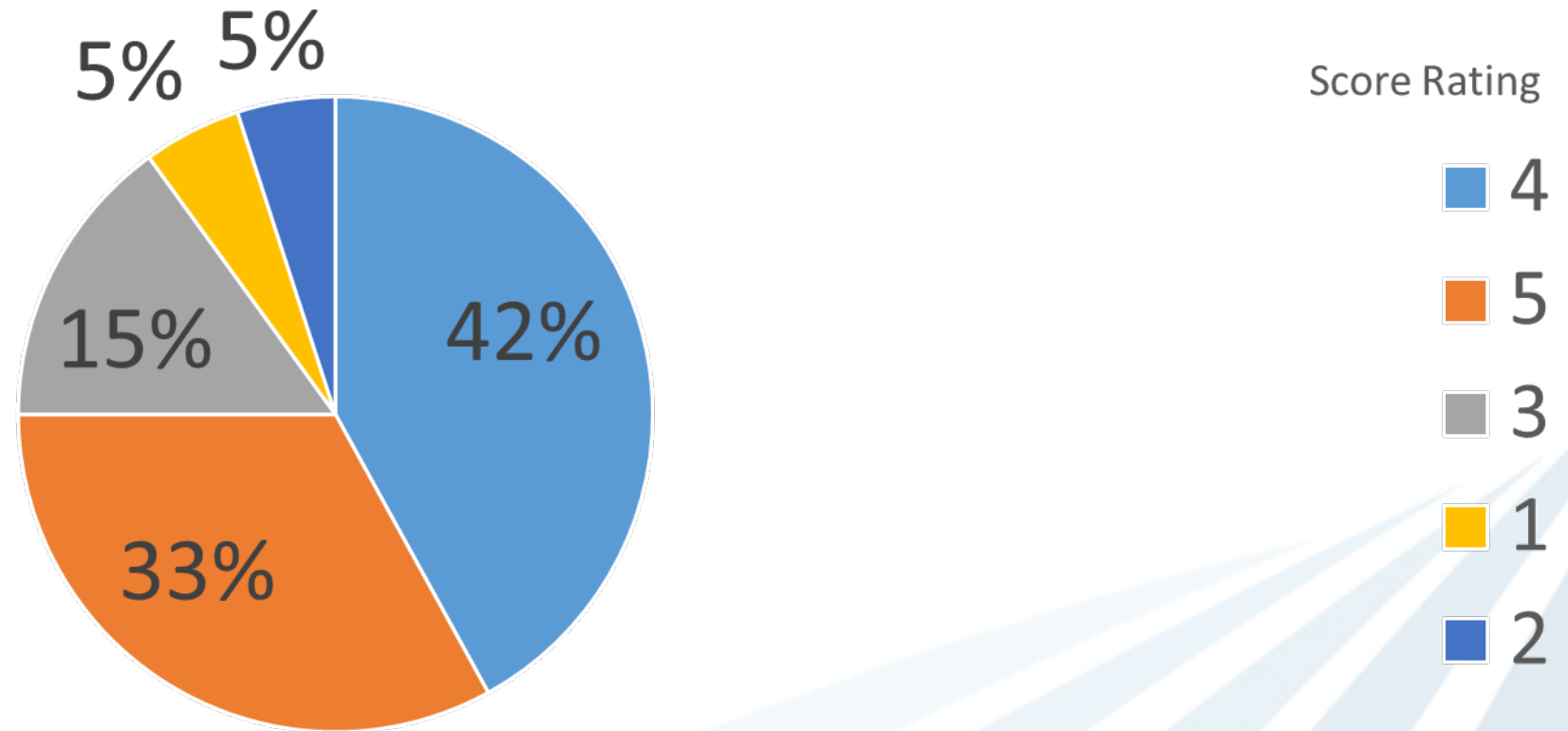
How much do you agree or disagree with the following statements? [After this office makes changes to improve the patient care process, we check to see if the changes worked]



- Agree
- Strongly Agree
- Neither Agree nor Disagree
- Strongly Disagree
- Does Not Apply or Don't Know



Overall Rating on Patient Safety: Overall, how would you rate the systems and clinical processes your medical office has in place to prevent, catch, and correct problems that have the potential to affect patients?



**District Clinic Holdings, Inc.
d.b.a. C.L. Brumback Primary Care Clinics
Board of Directors Meeting
Summary Minutes
10/30/2019**

Present: James Elder, Chairperson; Mike Smith, Treasurer; John Casey Mullen; Irene Figueroa, Secretary; Julia Bullard
Excused: Gary Butler, Vice Chairperson; Marjorie Etienne
Absent: Lisa Strickland

Staff: Dr. Belma Andric, CMO, VP & Executive Director of Clinical Services; Valerie Shahriari, General Counsel; Joel Snook, VP & Chief Financial Officer; Dr. Hyla Fritsch, Director of Clinic Operations and Pharmacy Services; Darcy Davis, CEO; Tamelia Lakraj-Edwards, Quality Manager; Ana Szogi, Data Reporting Analyst; Martha Hyacinthe, Director of Risk; Dr. Ana Ferwerda, Medical Director; Andrea Steele, Quality Director; Deborah Hall, VP & Chief Compliance & Privacy Officer; Sarah Gonzalez, Director of Credentialing and Provider Services; David Speciale, Patient Relations Manager; Shauniel Browne, Risk Manager

Minutes Transcribed By: Jonathan Dominique

Meeting Scheduled For: 12:45 PM

Meeting Began at: 12:51 PM

AGENDA ITEM	DISCUSSION	ACTION
1. Call to Order 1A. Roll Call 1B. Affirmation of Mission	Mr. Elder called the meeting to order. Roll call was taken.	The meeting was called to order at 12:51pm
2. Agenda Approval	Mr. Elder called for an approval of the meeting agenda.	

<p>2A. Additions/Deletions/ Substitutions</p> <p>2B. Motion to Approve Agenda Items</p>	<p>Correction of the Mangonia Park Address added to the Consent agenda</p> <p>The agenda for the October 2019 meeting was approved as sent digitally to board members in the board package.</p>	<p>Figuroa. A vote was called, and the motion passed unanimously.</p>
<p>3. Awards, Introductions and Presentations</p> <p>3A. “Homeless Coalition Award” video</p>	<p>Dr. Andric presented the “Homeless Coalition Award” Video. Mr. Smith asked if these videos are accessible to outside persons, Ms. Davis explained that they are available on both the external and internal HCD sites.</p>	<p>No action necessary.</p>
<p>4. Disclosure of Voting Conflict</p>	<p>None.</p>	<p>No action necessary.</p>
<p>5. Public Comment</p> <p>5a. Motion To Amend the Approved Agenda</p>	<p>None.</p> <p>There was an error in the approved agenda, and the Board wishes to add an item (The Executive Director’s Annual Evaluation) that was present in the board packet, but was inadvertently omitted from the agenda. Therefore, the board would like to revise the agenda and add Item 8A-2.</p>	<p>No action necessary.</p> <p>VOTE TAKEN: Mr. Smith made a motion to amend the agenda. The motion was duly seconded by Mr. Elder. A vote was called, and the motion passed unanimously.</p>
<p>6. Meeting Minutes</p> <p>6A Staff Recommends a MOTION TO APPROVE: Board meeting minutes of September 25, 2019</p>	<p>There were no changes or comments to the minutes dated September 25, 2019.</p> <p>The minutes dated September 25 is in need of correction on page 9 where the vote listed ‘Ms. Butler’ instead of ‘Mr. Butler’.</p>	<p>VOTE TAKEN: Ms. Figuroa made a motion to approve the Board meeting minutes of September 25, 2019 as presented. The motion was duly seconded by Mr. Mullen. A vote was called, and the motion passed unanimously.</p>

<p>6B Staff Recommends a MOTION TO Withdraw Approval: Board meeting minutes of September 25, 2019</p> <p>6C Staff Recommends a MOTION TO APPROVE with Revised Correction: Board meeting minutes of September 25, 2019</p>	<p>Ms. Bullard made a motion to approve the Board minutes of September 25, 2019 with Revised Correction.</p>	<p>VOTE TAKEN: Mr. Smith made a motion to withdraw the board’s approval of the Board meeting minutes of September 25, 2019 as presented. The motion was duly seconded by Ms. Bullard. A vote was called, and the motion passed unanimously.</p> <p>VOTE TAKEN: Ms. Butler made a motion to approve with Revised Correction Board meeting minutes of September 25, 2019 as presented. The motion was duly seconded by Mr. Smith. A vote was called, and the motion passed unanimously.</p>
<p>7. Consent Agenda – Motion to Approve Consent Agenda Items</p>		<p>VOTE TAKEN: Mr. Mullen made a motion to approve the consent agenda as presented. The motion was duly seconded by Ms. Figueroa A vote wasw called, and the motion passed unanimously.</p>
<p>7A. ADMINISTRATION</p>		
<p>7A-1. Receive & File: October 2019 Internet</p>	<p>The meeting notice was posted.</p>	<p>Receive & File. No further action necessary.</p>

Posting of District Public Meeting		
7A-2. Receive & File: Attendance tracking	Attendance tracking was updated.	Receive & File. No further action necessary.
7A-3. Receive & File: Proposed Schedule for 2020 Board Meetings	Clinic Board Meeting Schedule Proposed for the 2020 Calendar Year	Receive & File. No further action necessary.
7B. FINANCE		
7B-1. Receive & File: C. L. Brumback Primary Care Clinics Finance Report August 2019.	Finance Report for September 2019 presented and reviewed in the Finance Committee meeting.	Receive & File. No further action necessary.
7B-2. Receive & File: C. L. Brumback Primary Care Clinics Proposed Budget for FY 2020	Proposed budget for Fiscal Year 2020	Motion referenced above, no further action necessary.
8. REGULAR AGENDA		
8A. ADMINISTRATION		
8A-1. Staff Recommends a MOTION TO APPROVE: Appointments of Tammy Jackson-Moore to the Clinic Board	<p>Thomas Cleare, VP of Strategy Presented the Following candidate.</p> <p>Tammy Jackson-Moore has submitted an application for consideration for appointment to the District Clinic Holdings, Inc. Board of Directors. Ms. Jackson-moor is the newly appointed board member on the Health care District's Board. The appointment of Ms. Jackson-Moore to the Clinics Board will create a valuable link between the Clinics Board and the</p>	VOTE TAKEN: Mr. Elder made a motion to approve the appointment of Ms. Tammy Jackson-Moore to the Clinic Board. The motion was duly seconded by Mr. Smith. A vote was called, and the motion passed unanimously.

	Health Care District's Board. Ms. Jackson-Moore is a resident of the Glades who has served as a strong advocate in the community and volunteered on several community boards.	
8A-2. Staff Recommends a MOTION TO APPROVE: Executive Director Evaluation	Ms. Darcy Davis, CEO provided her evaluation of Dr. Belma Andric in her role as Executive director of Clinic Services.	VOTE TAKEN: Mr. Smith made a motion to approve Ms. Davis's Evaluation of Dr. Belma Andric. The motion was duly seconded by Mr. Mullen. A vote was called, and the motion passed unanimously.
8B. EXECUTIVE		
8B-1. Receive & File: Executive Director Informational Update	A letter was received from AHCA stating that we can open with a fire watch. In contact with HRSA Project Officer about Scope Verification for this new site. The Clinic opened doors on 10/21/2019 right next to Addiction Stabilization Center. Change In Scope approval from HRSA was submitted on 10/1/2019, but Notice of Award has not yet been received. HRSA Project Officer has been contacted via phone twice to discuss the Change In Scope approval and it anticipated in a matter of days. Dr. Andric also extended an invitation to the board members to tour our new Addiction and Stabilization clinic. The New electronic management system Converge Point to house all Clinic and Health Care District Policies, Procedures, Protocols and Standard Operating Procedures is currently in testing phase with the hope of being live by December 2019. Board Chair will no longer sign Policies, but they will still be brought to the Board for either Approval (Clinic) or Adoption (HCD). The Mock HRSA Audit is scheduled for the week of December 9-13. November 27 th meeting is the day before Thanksgiving. The Mock	Receive & File. No further action necessary.

	FTCA Audit is scheduled for the week of January 27-31.	
8C. OPERATIONS		
<p>8C-1. Staff Recommends a MOTION TO APPROVE: Operations Reports – September 2019</p>	<p>Overall encounters year to date is 115,296. Number of encounters in September across all categories is slightly lower than the previous month most likely due to the Labor Day Holiday and days missed due to Hurricane Dorian.</p> <p>Data for the Residents will now be presented separately in the Productivity graphs, and targets have been adjusted accordingly for our Residency Preceptors creating a more comprehensive snapshot reflective of actual work based on rendering provider.</p> <p>The Mobile Van participated in an outreach at the Port of Palm Beach for the Hurricane Dorian Bahamian refugees. The Mobile Van had 57 encounters that day for Adult and Pediatric Care, Women’s Health, and Behavioral Health services.</p> <p>Mr. Smith asked if encounters are the same as visits. Dr. Andric explains that the difference between encounters and visits is what falls under the umbrella of “billable”.</p>	<p>VOTE TAKEN: Mr. Mullen made a motion to approve the September Productivity Summary Report as presented. The motion was duly seconded by Ms. Bullard. A vote was called, and the motion passed unanimously.</p>
<p>8C-2. Staff Recommends a MOTION TO APPROVE: Dental Nominal Fee Survey Assessment</p>	<p>This report presents the results of the 2019 Targeted Patient Survey focusing on the C.L. Brumback Primary Care Clinic Dental nominal sliding fee.</p> <p>In September 2019, the Health Care District Patient Access Management Department polled patients of the C. L. Brumback Dental Clinic via telephone. In this survey, adult patients of the Dental Clinics were</p>	<p>VOTE TAKEN: Mr. Mullen made a motion to approve Dental Nominal Fee Survey Assessment as presented. The motion was duly seconded by Mr. Smith. A vote was called, and the motion passed unanimously.</p>

	<p>asked if they experienced any challenges or barriers with the nominal fee of \$30.00.</p> <ul style="list-style-type: none"> - Total Responses received: 714 - Response Rate: 36% - Percent agreeable with \$30 minimum: 89% <p>Based on the response received, we believe that a majority of our patients feel that our Dental nominal fee is fair.</p>	
<p>8D. QUALITY</p>		
<p>8D-1. Staff Recommends a MOTION TO APPROVE Patient Relations Reports and Dashboard</p>	<p>Mr. David Speciale, Patient Relations Manager presented the following reports.</p> <ul style="list-style-type: none"> - Quarterly Patient Relations Dashboard Q2 <p>23 Complaints and grievances (n= 37,071 encounters)</p> <ul style="list-style-type: none"> - 9 Complaints - 14 Grievances - The data shows a downward trend in comparison to the previous quarter (33 total). 	<p>VOTE TAKEN: Mr. Smith made a motion to approve the Patient relations Dashboard as presented. The motion was duly seconded by Mr. Mullen A vote was called, and the motion passed unanimously.</p>

	<ul style="list-style-type: none"> - Everything was resolved in a timely manner. - 27 Compliments - Trending upward from previous quarter - Approximately the same around this time last year. <p>- Patient Satisfaction Survey June – August 2019</p> <ul style="list-style-type: none"> - Population Surveyed 10% of total Population served - Adult Medical was 66% of the appointment types for those surveyed - Majority of the patients have been with the clinics between 1-3 years. - Mr. Speciale will look to survey more patients on their initial visit to the CLBPCC - Patient wait time trends (as perceived by the patient) our higher perceived wait times have decreased. - Majority of patients would recommend our practice to other patients. - Majority of patients would refer other patients to their providers. - There will be more targeted surveys conducted to look into provider performance 	
--	---	--

	<ul style="list-style-type: none"> - Clinic Operations ratings have been very positive for the most part. - Mr. Speciale will look to breakdown the data per clinic and show trends over time for each clinic. - Clinic provider and staff ratings have also been positive. <p>Mr. Speciale went on to read letters from patients.</p> <p>Ms. Mastrangelo asked about the method of data collection for the surveys. Mr. Speciale informed Ms. Mastrangelo that the PCC has completely transitioned to electronic data collection. The Clinic Administrative team is in the process of finding a vendor that would provide better software for data collection.</p> <p>Ms. Jackson-Moore asked if there was data available from the Pharmacy. Dr. Andric informed Ms. Moore that the pharmacy falls under a different branch of the health care district, but we can provide the data every once in a while to keep the board up to date.</p>	
<p>8D-2. Staff Recommends a MOTION TO APPROVE Quality Council Reports</p>	<p>Dr. Ana Ferwerda, Interim Medical Director presented the following:</p> <p><u>PATIENT SAFETY & ADVERSE EVENTS</u> Patient safety and risk, including adverse events, peer review and chart review are brought to the board “under separate cover” on a quarterly basis.</p>	<p>VOTE TAKEN: Mr. Mullen made a motion to approve the Quality Council Report as presented. The motion was duly seconded by Ms. Figueroa. A vote was called, and the motion passed unanimously.</p>

PATIENT SATISFACTION & GRIEVANCES

The patient satisfaction surveys are currently being administered in all the clinics. West Palm Beach Clinic leads in survey completion with a 19.8% completion rate. Patient compliments have reached an all time high with the majority recorded at the WPB clinic.

QUALITY ASSURANCE & IMPROVEMENT

Of the 14 UDS Measures: 7 exceeded the HRSA Goal and 7 were short of the HRSA Goal. Interventions were defined. We are in the process of implementing care teams, a patient centric concept which incorporates the primary care provider and ancillary staff working together to meet patient specific needs. We are evaluating clinic workflows in order to facilitate patient care. Performance metrics are being evaluated as month to month trends. The clinic analysis will be displayed on the quality boards in the clinics and the individual provider analysis will be presented to that provider during their one on one with Medical Director.

UTILIZATION OF HEALTH CENTER SERVICES

Due to Hurricane Dorian, Labor Day weekend closures and elimination of evening clinics productivity is slightly lower when compared to previous months. We are evaluating the registration process in the clinics in order to develop a standardized and effective workflow. Mobile van provided assistance at the Port of Palm beach on 9/7/2019 for Hurricane Dorian relief. 57 patients were evaluated and treated

**C. L. Brumback Primary Care Clinics
Board of Directors**

Attendance Tracking

	1/30/19	2/27/19	3/26/19	3/27/19	4/24/19	5/28/19	6/26/19	7/31/19	8/28/19	9/25/19	10/30/19	11/27/19	12/18/19
James Elder	X	X	X	X	X	X	X	X	X	X	X	X	
Irene Figueroa	X	X	X	X	A	X	X	X	X	X	X	X	
John Casey Mullen	X	X	X	X	X	X	E	X	X	X	X	X	
Shanti Howard	E	X	E	X	X	X							
Cory M. Neering	X	E	E	E	X	X	E	X	A				
Joan Roude	X	X											
Joseph Morel	X	X	X	X	X	A	X	E					
Julia Bullard	X	X	X	X	X	X	E	E	X	X	X	E	
Mike Smith		X	X	X	X	X	X	X	X	E	X	E	
Gary Butler				X	X	X	X	X	X	X	E	X	
Lisa Strickland									E	X	E	A	
Marjorie Etienne											E	X	
Melissa Mastrangelo											X	X	
Tammy Jackson-Moore											X	X	

X= Present

C= Cancel

E= Excused

A= Absent

DISTRICT CLINIC HOLDINGS, INC.
BOARD OF DIRECTORS
December 11, 2019

1. Description: Bylaws Updates

2. Summary:

This agenda item presents the District Clinic Holdings, Inc. update to the bylaws.

3. Substantive Analysis:

The HRSA Compliance Manual requires that the Bylaws define “healthcare” when referring to Patient Board Members who earn 10% or more of their income from the healthcare industry. The Bylaws have been updated to define healthcare.

4. Fiscal Analysis & Economic Impact Statement:

	Amount	Budget
Capital Requirements	N/A	Yes <input type="checkbox"/> No <input type="checkbox"/>
Annual Net Revenue	N/A	Yes <input type="checkbox"/> No <input type="checkbox"/>
Annual Expenditures	N/A	Yes <input type="checkbox"/> No <input type="checkbox"/>

Reviewed for financial accuracy and compliance with purchasing procedure:

N/A

 Joel H. Snook
 VP & Chief Financial Officer

5. Reviewed/Approved by Committee:

N/A

 Committee Name

 Date Approved

DISTRICT CLINIC HOLDINGS, INC.
BOARD OF DIRECTORS
December 11, 2019

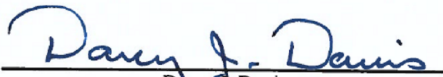
6. Recommendation:

Staff recommends the Board approve the Bylaws Updates.

Approved for Legal sufficiency:



Valerie Shahriari
VP & General Counsel



Darcy J. Davis
Chief Executive Officer

Amended
Bylaws
of
District Clinic Holdings, Inc.

**Amended
Bylaws
of
District Clinic Holdings, Inc.**

Section 1	Statutory Authority
Section 2	Name
Section 3	Purpose
Section 4	Officers
Section 5	Objectives
Section 6	Powers
Section 7	Board Member Responsibilities
Section 8	Member Composition
Section 9	Term of Office
Section 10	Officers
Section 11	Committees
Section 12	Meetings
Section 13	Authority
Section 14	Amendments

DISTRICT CLINIC HOLDINGS, INC.

AMENDED BY-LAWS

Section 1 – Statutory Authority

- 1.1 Statutory Authority. These Bylaws have been adopted as the Bylaws of the District Clinic Holdings, Inc. (“Clinics”) governing board of said Clinics pursuant to authority conferred upon that same governing board by Section 330 of the Public Health Service Act.
- 1.2 Health Care District of Palm Beach County. The term “District,” as used in these Bylaws, means the Health Care District of Palm Beach County and all affiliated entities.

Section 2 – Name

- 2.1 District Clinic Holdings, Inc. will be known as the “C.L. Brumback Primary Care Clinics” which shall be the common business name of the clinics.
- 2.2 Board Name. This authority shall be known as the C.L. Brumback Primary Care Clinics Board of Directors. (hereinafter referred to as the “Board”)

Section 3 – Purpose

- 3.1 Purpose. The purpose of the Board is to ensure that persons have access to high quality comprehensive health services, and that such health services are provided without regard to any persons race, color, national origin, ancestry, religion, sex, marital status, sexual orientation, age, physical handicap, medical condition, medical history, genetics, evidence of insurability, or claims history in compliance with all applicable State, Federal and local laws and regulations.

Section 4 – Offices

- 4.1 Offices. The Board shall have and continuously maintain its principal office at the Health Care District of Palm Beach County administrative office located at 1515 N Flagler, Suite 101, West Palm Beach, FL 33401.

Section 5 – Objectives

- 5.1 The objectives of the Board are as follows:

- a. Improvement of the general health status of the community through the promotion of preventive health services and early identification and treatment of the disease.
- b. Identification and referral of individuals in need of health and social services.
- c. Participation in the development of the Federal grant application.
- d. Monitoring services provided by the clinics to ensure that community needs are being met within the constraints of the agency.
- e. Ensure that professional standards are maintained.
- f. Interpret the health needs of the community to clinic administrative staff and interpret the services provided by the clinics, to the community.

Section 6 – Powers

6.1 General Powers. The Board is vested with authority and responsibility to provide for the comprehensive planning and delivery of adequate health care services, including, but not limited to, clinical services for the citizens of Palm Beach County, particularly medically needy citizens. For those purposes, the Board shall have and may utilize all enumerated general powers as set forth in the Health Care Act, including but not limited to:

- a. To approve and recommend the budget of the clinic operations annually. Monthly financial reports will be provided to the Governing Board at the regularly scheduled meetings. An annual financial audit and financial report by an independent auditor will be submitted to the Governing Board.
- b. To be responsible for approving the selection and dismissal of the Executive Director within the guidelines of the Health Care District of Palm Beach County Personnel Policies and Procedures.
- c. To provide input from the community, regarding appropriate matters, including, but not limited to, the health care needs of the community served.
- d. To continually provide information about the accessibility of services to the community and the clinic's responsiveness to those needs.
- e. To provide guidance regarding services and their priorities; and to establish how these priorities should be ranked as they pertain to program development.
- f. To provide a viable link with the community, engaging in community education, public relation activities and other activities which promote community identification and understanding of the clinics and services provided.
- g. To provide a nucleus in the community which reaches out to local agencies, governmental entities, and foundations, etc., to support the clinics financially and otherwise.

- h. Establish and approve general policies for the clinics. The Board acknowledges that the District is the public entity co-applicant and is permitted to retain the responsibility of establishing fiscal and personnel policies as detailed in PIN 1998-12, Part II Section 330, Governance Requirements, which states “[w]hen the public entity's board does not meet health center composition requirements, a separate health center governing board may be established. The health center board must meet all the membership requirements and perform all the responsibilities expected of governing boards except that the public entity may retain the responsibility of establishing fiscal and personnel policies. The health center board can be a formally incorporated entity and it and the public entity board are co-applicants for the health center program. When there are two boards, each board's responsibilities must be specified in writing so that the responsibilities for carrying out the governance functions are clearly understood.”
- . The Board shall work collaboratively with the District to specify each board’s responsibilities, in writing so that the responsibilities of carrying out the governance functions are clearly understood by both boards.
- i. To be responsible for evaluating health care activities including services utilization patterns, productivity of the clinics, patient satisfaction, achievement of project objectives, and development of a process for hearing and resolving patient grievances.
- j. To assure that the clinics are operated in compliance with applicable federal, state and local laws, rules and regulations.
- k. To adopt health care policies, including scope and availability of services, location and hours of services.
- l. To assure compliance with the approved Quality Assurance Plan.
- m. To establish and review policies regarding the conduct of the federally funded project.
- n. Responsible for evaluating the clinics projects and achievements at least annually, and using the knowledge gained to revise its mission, goals, objectives, plans, and budgets as may be appropriate and necessary.
- o. Responsible for the annual performance evaluation of the Executive Director.
- p. To recruit, appoint, re-appoint, credential and discipline the Licensed Independent Practitioners of the Clinics and to approve policies to be adopted by the Clinics. The term Licensed Independent Practitioner shall mean any individual, as permitted by law and regulation, and also by the Clinics, to provide care and services without direction or supervision within the scope of the individual’s license and consistent with the privileges granted by the organization. The foregoing shall be in accordance with applicable state, federal and local laws, rules and regulations, and in accordance with the standards of any applicable accrediting body. The Board may, in its discretion, delegate duties related to the

performance of recruitment, appointment, credentialing and discipline of medical staff to the appropriate Medical Director/Dental Director except that recommendations regarding appointment, credentialing and discipline shall be presented to the Board by the Medical Director for consideration and final vote.

Section 7 – Board Member Responsibilities

7.1 *Key function and responsibilities.*

- a. Attends and participates in all Board meetings.
- b. Each board member should be prepared for the meetings (i.e., read reports and minutes provided prior to the meetings and be familiar with the agenda), ask questions (as appropriate).
- c. Express his/her opinion and be respectful of the opinion of other members.
- d. Act in the best interests of the clinics at all times.
- e. Ensure confidentiality of clinics' information.
- f. Conflicts of Interest. Board members shall not enter into contracts or other arrangements or transactions that would be, or would give the appearance of, a conflict of interest. Further:
 1. Board members are subject to the provisions of Florida law pertaining to public officials avoiding conflicts of interest including, but not limited to, Ch. 112, Florida Statutes, the Code of Ethics for Public Officers and Employees, as well as any and all other applicable standards established by the applicable regulatory and accreditation agencies
 2. No Board member, administrator, employee or representative of the Clinics, nor any other person, organization or agency shall, directly or indirectly, be paid or receive any commission, bonus, kickback, rebate or gratuity or engage in any fee-splitting arrangement in any form whatsoever for the referral of any patient to the District or Clinics.

Section 8 – Membership Composition

- 8.1 Orientation. As new members are elected or appointed to the Board they shall receive an orientation regarding CL Brumback Primary Care Clinics Board to include, but not be limited to, their authority and responsibility under the 330 grant requirements, legal status, and relation to the Health Care District of Palm Beach County and a review of these By-Laws.
- 8.2 The Board shall consist of 9-13 members.
- 8.3 A majority of the Board members will be users of the clinic's services. These members will be representatives of the individuals receiving services at any of the clinics.

- 8.4 The user Board members as appropriately defined in the Bylaws are consistent with applicable law, regulations and policy.
- 8.5 User Board members are defined as individuals who are (or, for planning grantees, will be) served by the clinics and who utilize the clinics as their principal source of primary care and who have used the clinic's services within the last two years.
- 8.6 Non-User Board members must live or work in one of the clinic's service areas.
- 8.7 No more than half of the remaining members of the Board may be individuals who derive more than 10% of their annual income from the health-care industry. Healthcare industry is defined as "hospitals and other healthcare institutions, nurses, doctors, dentists, and other licensed healthcare professionals whose primary responsibility is providing primary preventive and therapeutic healthcare services".
- 8.8 The remaining members of the board must be representatives of the community where the project's catchment area is located and shall be selected for their expertise in community affairs, local government, finance, and banking, legal affairs, trade unions and other commercial and industrial concerns or social service agencies within the community.
- 8.9 No member of the Board shall be an employee of the clinics, or spouse, child, parent, brother or sister by blood or marriage of such an employee. The Executive Director may be a non-voting, ex-officio member of the Board.
- 8.10 No Board member, employee, consultant or those providing services and or goods to the Clinics may pursue any personal activity that will involve a conflict-of-interest or use their official position to make secret or private profits and will treat all matters of the clinics as confidential. Board members will not use or give the appearance of using their position for the purpose of financial gain. "Financial gain" includes financial interest, gifts, gratuities, favors, nepotism and bribery. Political favors will also be considered improper. Board members must identify any conflict-of-interest they may have regarding a particular matter and abstain from discussing of voting in the matter.
- 8.11 No Board members should act or speak, or otherwise indicate that they are authorized to act or speak, on behalf of the entire Board without express Board approval/consent.
- 8.12 Recommendation for Board membership shall be from the community being served.
- 8.13 One Board position shall be filled by the District Chair, or his/her designee, by appointing a member of the District's Governing Board in accordance with that body's applicable bylaws.
- 8.14 One Board member shall serve on the Finance and Audit Committee of the District's Governing Board and one Board member shall serve on the Quality, Patient Safety, and Compliance Committee of the District's Governing Board.

Section 9 – Term of Membership

- 9.1 Board membership will be for a period of three (3) years starting in January of each year and terminate

in December of the third year. No Board member shall serve more than two (2) consecutive terms. If at any time there is a question concerning the length of the term of office for any Board member, the Governing Board will decide through any appropriate means the term of the questioned incumbent.

9.2 Selection of New Board Member(s) for open Member positions. The selection of new Board members to fill any vacancy then existing may or to replace any member whose Term is ended, will be as follows:

- a. Vacancies on the Board due to the termination, resignation or death of a Member prior to the expiration of his/her Term may be filled within sixty (60) days of the vacancy by a majority vote of the Members at the next regular meeting, or at a special meeting called for that purpose, from those eligible persons recommended by the Nominating/Membership Committee. The newly elected member will serve for the unexpired term of the Member position being filled and shall be eligible to seek reappointment upon expiration of such term.
- b. Members eligible to serve for a second 3-year term may apply for reappointment according to the procedures instituted by the Nominating Committee and approved by the Board. When a vacancy is anticipated to occur at the completion of any Member's 3-year term, the Nominating Committee shall submit names of eligible persons to the Board for consideration at least one month prior to the annual meeting of the Board, and the Board shall select those persons to fill the anticipated vacancy by a majority vote at the annual meeting. In selecting its new members, the Board will use the criteria set out in Section 8.

9.3 Membership on the board may be terminated by resignation of a member or by resolution of the Board after any member has three (3) unexcused absences. For purposes of these Bylaws, an unexcused absence occurs when a Board member fails to attend a regularly scheduled meeting and fails to give advance notice of such absence to the Executive Director who will notify the Chair. After two (2) unexcused absences, the secretary shall send the member a reminder. On the third unexcused absence, the Board shall take action to terminate membership and the individual shall be so advised. The migrant/seasonal farm worker who is absent due to job obligation will be granted and excused absence without restrictions.

9.4 Board member can be removed for cause including, but not limited to:

- a. Repeated failure to attend Board meetings, or for conduct detrimental to the interests of the clinics.
- b. Refusing to act in a manner consistent with the clinic's mission and priorities.
- c. Individual is suspended or debarred from participation in federal programs.

9.5 Each member will be entitled to one (1) vote.

- a. Membership shall be designated as Consumer, Health Care Provider, Community Representative, or Migrant/Seasonal Farm worker.
- b. Voting Conflict. No member shall cast a vote on any matter that could result in direct or

indirect financial benefit to such member or otherwise give the appearance of or create a conflict of interest as defined in Ch. 112, Florida Statutes. Nothing in the foregoing shall prevent Board Members from voting upon matters of Board Compensation as set forth in Section 10.5.

Section 10 – Officers

- 10.1 Corporation officers shall be elected by the Members at the Annual Meeting in May of each year for a one (1) year term of office. Any officer may be elected to serve consecutive terms in the same office, but may not serve more than two consecutive one-year terms in the same office.
- 10.2 Removal of Officers. Any officer of the Board may be removed from office, with or without cause, by a majority vote of the Board of Directors at any meeting of the Board where a quorum exists.
- 10.3 Vacancies. Any time there is a vacant officer position, the Board may elect a replacement officer at its next regular meeting to serve out the remainder of the term of office, and any person so elected shall not have the remaining term count for purposes of calculating the ‘two consecutive one-year terms’ referenced in Section 10.1.
- 10.4 The officers and their duties for this organization shall be:

10.4.1 Chairperson

- a. To preside over all meetings and to appoint all committee and councils.
- b. The Chairperson or such representative selected by the Board shall be authorized to act for the Board, and assume on its behalf the obligations imposed by the terms and conditions of any award and Public Health Service regulations. Such execution shall constitute the acceptance by the Board of the terms and conditions of the Grant and obligate it to perform its function under the approved project in accordance with the terms thereof.
- c. The Chairperson shall be the Board’s sole and primary liaison for external affairs including serving as Board’s representative to the media.
- d. Appoint a Board member to attend District governing Board meeting in conjunction with the Executive Director, solely in advisory capacity to enhance oversight and communication between each organization

10.4.2 Vice Chairperson

- a. The Vice-Chairperson shall succeed to the office of the Chairperson if the office becomes vacant or if otherwise the chairperson in otherwise unable to perform his/her duties.
- b. To assume the duties as assigned by the Chairperson in his/her absence.
- c. Perform such duties as assigned by the Chairperson or Board of Directors.

10.4.3 Secretary

- a. The secretary shall be responsible for ensuring recording and maintaining of the minutes of all meetings of the governing Board, and shall perform such duties as may be assigned by the Chairperson of the Board. The Secretary or designee shall distribute copies of minutes of all Board and/or committee meetings to all members of the Board.
- b. To monitor the minutes of all meeting of the Board and Executive Committee.
- c. To assure that his/her designees notifies members of all Board meetings and conferences.
- d. To advise staff members regarding correspondence.
- e. To monitor, review and approve the preparation of the agendas.

10.4.4 Treasurer

- a. To review monthly and/or periodic financial reports prior to presentation to the Board during scheduled meetings.

10.5 Compensation

Members shall serve without compensation except the Board may authorize and establish policies governing the reimbursement of certain reasonable expenses, such as mileage, incurred to attend meetings.

Section 11 – Committees

11.1 There shall be an Executive/By-Law Committee comprised of the officers of the Board. This committee shall meet as provided in these Bylaws and as otherwise deemed necessary by the Chairperson. The Chairperson shall serve as the Committee chair and the Executive Director will serve as a non-voting, *ex officio*, member of the Executive Committee. The Executive Committee shall:

- a. Act as advisor to the Chairperson;
- b. Exercise the powers of the Board between regular Board meetings, except that the Executive Committee may not take final action to amend these bylaws, remove a board member from office, hire or remove the Executive Director, or sell or acquire assets;
- c. Report to the Board at its next regular meeting on any official actions it has taken;
- d. Annually review and recommend to the Board any necessary change to the bylaws; and
- e. Annually review the performance of the Executive Director for report to the Board.
- f. Serve as the ad hoc Personnel Committee as needed.

11.2 Vacancies of the Executive committee occur when there is a vacant officer position. The

vacancy is filled with the election of a member to serve out the officer's remaining term (See Section 10).

- 11.3 The Standing Committees shall be the Finance Committee, Quality Council and Planning Committee.
- 11.4 The Membership/Nominating Committee shall be an ad hoc committee, activated and populated at the direction of the Chairperson to recruit and nominate individuals to fill vacancies of the Governing Board. The Membership/Nominating Committee shall, if requested, review, edit, and submit proposed revisions to policies and procedures for the recruitment, screening and orientation of potential new Board members and present to the Board information on eligible persons to fill vacancies. This committee shall, if requested, assist in development of a board orientation program. The Executive Director, or his/her designee, will serve as a no voting, ex-officio member of this committee.
- 11.5 The Planning Committee shall oversee the clinic's goals and objectives, and develop a strategic planning workshop for the Board to be held at least every three (3) years. The Executive Director, or his/her designee, will serve as a non-voting, ex-officio member of this committee.
- 11.6 The Quality Council shall review and make recommendations for clinical services, monitor progress of Health Care Plan objectives, review Clinical Outcome measures audits, monitor and review Quality Assurance and Continuous Quality Improvement, Principles of Practice, credentialing, community needs survey data, patient satisfaction survey, and recommend new clinical programs. The Quality Council will meet on a monthly basis. The Executive Director, or his/her designee, will serve as a non-voting, ex-officio member of this committee.
- 11.7 The Standing Committees will meet as set forth in these Bylaws and will provide a report of its meeting(s) during the next Board meeting following the Committee meeting, and make any recommendations for Board action, which will then become part of the Board documents.
- 11.8 Proxy: An absent member shall not be allowed to vote by proxy
- 11.9 Members of the Planning Committee and Quality Council may also include non-board members with specific areas of expertise that support the mission of that committee.
- 11.10 The Finance Committee shall review the budget, expenditures, and all other financial reports related to the operations of the C.L. Brumback Primary Care Clinics. The Finance Committee will report to the full Board of Directors. The Finance Committee will meet on a monthly basis, and may include clinic staff employees. The Executive Director, or his/her designee, will serve as a non-voting, ex-officio member of this committee.

Section 12 – Meeting

- 12.1 Regular meetings shall be held monthly. Time and place shall be determined by Board.

- 12.2 Special meetings may be called by the Chairperson whenever Board business cannot be held until the next regular meeting.
- 12.3 Meetings shall conform to the requirements of Ch. 286, Florida Statutes (“Government in the Sunshine Act”), including the taking and maintenance of meeting minutes, and such minutes shall be retained by District in accordance with the requirements of the State of Florida’s Record Retention Schedules GS1-SL (State and Local Government Agencies), GS4 (Public Health Care Facilities and Providers), and/or any other applicable Schedule(s), regarding Minutes of Official Meetings.
- 12.4 The Annual Meeting shall coincide with the Regular meeting held during the Month of May and shall hold the election of officers to take office commencing on the next January 1.
- 12.5 Quorum shall consist of a majority of the members of the Governing Board as then constituted, for the regular scheduled meetings and the special called meetings. Once a quorum is established for any meeting it remains for the duration of the meeting unless one or more members permanently absents him/herself from the premises of the meeting and the sum of the remaining members falls below the number needed for a quorum.
- 12.6 Official actions of the Board may be conducted by telephone provided that such meeting complies with the requirements of the Government in the Sunshine Act.

Section 13 – Authority

The parliament authority of the Governing Board shall be used based on ROBERTS RULE OF ORDER (current edition), unless contrary procedure is established by the Articles of Incorporation, these Bylaws, standing rule, or by resolution of the Board of Directors.

Section 14 – Amendments

These By-Laws may be amended or repealed by a vote from the majority of the total membership of the Governing Board. Proposed changes to the By-Laws must be submitted to the Board at a regularly scheduled meeting and voted on at the succeeding regularly scheduled meeting. Changes in the By-Laws are subject to approval by the Governing Board, Health Care District of Palm Beach County, and the Regional Office of the Department of Health and Human Services.

Section 15 – Dissolution of the Corporation

In the event of the liquidation, dissolution or winding up of the corporation whether voluntary, or involuntary, or operation of law, the Board of Directors of the Corporation shall dispose of the assets of the Corporation in conformance with Federal and State of Florida law, as modified by the regulations promulgated by designated oversight agency or department, and in accordance with the Corporation’s Articles of Incorporation.

CERTIFICATE

This certifies that the foregoing constitutes the Bylaws of District Clinics Holdings, Inc., amended and adopted by the Members of the Corporation at a meeting held on the ~~March 28, 2018~~ December 11, 2019.

BY: _____

~~Wanda D. Casey~~ Irene Figueroa
Secretary

**Approved as to form and
Legal Sufficiency**

BY: _____

General Counsel

HISTORY OF DISTRICTCLINIC HOLDINGS,INC. BYLAWS

The initial Bylaws of the District Clinic Holdings, Inc. Board were first adopted on the 24th day of January, 2013. Amendments made subject to Section 14 of the District Clinic Holdings, Inc. Bylaws are listed below:

Change Number	Date of Adoption	Section(s) Amended
1	March 28, 2013	<p>Title Pages amended to read:</p> <p>Section 11.3 relating to the Finance Committee deleted and</p> <p>Section 11.9 amended to remove reference to Finance Committee.</p>
2	May 23, 2013	<p>Section 2.1 amended to remove the following: “Thus, as used in these bylaws, the terms “Board” shall mean the C.L. Brumback Health Clinic Board of Directors.”</p> <p>Section 6.1m amended to remove ability to establish and revise policies.</p> <p>Section 6.1q amended to remove the following: “Within its discretion to file article of dissolution and dissolve the corporation.</p> <p>Section 8.10 “The Board shall ensure that the provision is made applicable to all employees, consultants and those providing goods and or services to the Center.” deleted.</p>

Section 11.1 removed requirement to make recommendations to full Board.

Section 11.7 removed “The Personnel Committee shall review staffing needs and recommends changes in staffing levels when deemed desirable. While the Board’s personnel policies shall be consistent with those of the Health Care District the Board must tailor its personnel policies to the clinical operations of the corporation.” To dissolve the Personnel Committee.

Section 11.8 removed “The Finance Committee shall review the budget, expenditures, and financial policies and make recommendations to the Board in regard to certain concerns. While the Board’s financial policies shall be consistent with those the Health Care District the Board must tailor its financial policies to the clinical operation of the corporation.” To dissolve Finance Committee.

3

August 1, 2013

Section 2.1 amended to include: “hereinafter referred to as the “Board”)

Section 6.1m amended to include establishment of policies.

4

August 9, 2013

Section 6.1q added power to:
“Facilitate the annual Chief
Executive Officer performance
evaluation process.”

Section 8.10 amended to
include: “...employee,
consultant or those providing
services and or goods to the
Clinic...”

Section 2.1 established for
clarification regarding
common business name

Section 2.2 replaced Health
Clinic Board with Primary
Care Clinics Board of
Directors

Section 6.1.b replaced Project
with Executive

Section 6.1.h removed “To
adopt and be responsible for
operating and personnel
policies and procedures,
including selection and
dismissal procedures, salary
and benefits scales and
employee grievance
procedures within the
guidelines of the Health Care
District of Palm Beach County
Personnel Policies and
Procedures” and amended to
include ability to establish and
approve general policies for
the clinics as stated in PIN
1998-12, Part II Section 330,
Governance Requirements.

Section 6.1.m amended to
include ability to establish
policies

Section 6.1.q amended to establish responsibility for the Executive Director's annual performance evaluation

Section 8.1 amended to include the common business name, CL Brumback Primary Clinics

Section 8.9 amended to replace previously referenced project director with Executive Director

Section 8.11 amended to include "...otherwise indicate that they are authorized to act or speak..."

Section 8.13 added

Section 9 amended to read:
Term of Membership

Section 9.1 amended to clarify membership length of terms

Section 9.2 added for establishment of selecting New Board Members.

Section 9.2.a added to establish requirements for filling vacancies on the Board due to termination, resignation, or death of a Member.

Section 9.2.b added to establish procedure for member reappointment instituted by the Nominating Committee

Section 9.3 amended to define an unexcused absence

Section 9.4 amended to read: “Board member can be removed for cause including, but not limited to:”

Section 9.4.a “...causes include the” deleted

Section 9.5 regarding Board vacancies was deleted, became section 9.2.a

Section 10.1 amended to become Section 10.4

Section 10.1 included to establish election of officers by Members

Section 10.2 added in order to establish process for removal of officers.

Section 10.3 added to establish election of a replacement officer on a vacant position.

Section 10.4.d. deleted: “The Chairperson, or his/her designee, shall represent the board before the news.”

Section 10.4.d reads: “The Chairperson shall be the Board’s sole and primary liaison for external affairs including serving as Board’s representative to the media.”

Section 10.4.e added to read: “Appoint a Board member to

attend District governing Board meeting in conjunction with the Executive Director, solely in advisory capacity to enhance oversight and communication between each organization.”

Section 10.4.e amended to include ability to review and approve agendas.

Section 10.5 added: “the Board may authorize and establish policies governing the reimbursement of certain...”

Section 11.1 replaced clinic’s director with Executive Director. Added “The Executive Director, or his/her designee, will serve as a non-voting, ex-officio member of this committee.

Section 11.2 included for establishment of a Personnel Committee

Section 11.3 removed “The Executive Committee of the Board shall consist of the Officers of the Board”

Section 11.4 added requirement to develop policies and procedures for recruitment, screening and orientation of potential new Board members and present information to the Board on eligible persons to fill vacancies.

Section 11.5 added: “The Executive Director, or his/her designee, will serve as a non-voting, ex-officio member of this committee.”

Section 11.6 amended to read that the Clinical Committee is to be also known as the Quality Committee.

Section 11.7 amended to include requirement for committees report to include any recommendations for Board action

Section 11.9 deleted
Committee members

Section 11.10 added to read:

The Finance Committee shall review the budget, expenditures, and all other financial reports related to the operations of the C.L. Brumback Priamary Care Clinics. The Finance Committee will report to the full Board of Directors. The Finance Committee will meet on a monthly basis, and may include clinic staff employees. The Finance Committee will meet on a monthly basis. The Executive Director, or his/her designee, will serve as a non-voting, ex-officio member of this committee. Section 13 added: “unless contrary procedure is established by the Articles of Incorporation, these Bylaws, standing rule, or by resolution of the Board of Directors.

February 18, 2014

Section 15 added for requirement for disposing of assets in the event of dissolution of the Corporation

Section 11 renumbered for efficiency.

Section 8.2 amended to increase the number of Board members to 10-13.

Section 10.3 added: to serve out the remainder of the term of office, and any person so elected shall not have the remaining term count for purposes of calculating the 'two consecutive one-year terms' referenced in 10.1.

Section 11.3 amended to establish process for filling vacancy of an officer position.

Section 12.3 added: "Meetings shall conform to the requirements of Ch. 286, Florida Statutes ("Government in the Sunshine Act"), including the taking and maintenance of meeting minutes, and such minutes shall be retained by District in accordance with the requirements of the State of Florida's Record Retention Schedules GS1-SL (State and Local Government Agencies), GS4 (Public Health Care Facilities and Providers), and/or any other applicable Schedule(s)), regarding Minutes of Official Meetings".

Section 12.4 added to read:
“Effective in 2014, the Annual Meeting shall coincide with the Regular meeting held during the month of May and the election of officers to hold office commencing in the next fiscal year shall be held. In order to transition to this new schedule, the election of officers held in November 2013 for terms to continue through December 31, 2014, shall remain unchanged. The election to be held in May 2014 shall be for the officers whose terms shall commence on January 1, 2015, and each election that follows shall select the officers whose terms shall commence on the following January 1”.

Section 12.5 previously section 12.3 added “unless one or more members permanently absents him/herself from the premises of the meeting and the sum of the remaining members falls below the number need for a quorum”.

Section 12.6 previously section 12.4 amended to include condition to comply with Government in the Sunshine Act requirement.

Section 6.1.o Remove provision, it is duplicative of audit language in Section 6.1.a

Added Section 6.1.q

6

April 24, 2014

Added Section. 7.1.f to establish Board member responsibilities regarding Conflicts of Interest

Section 9.5.b added.

Section 10.4.1 removed subsection b (Chairperson shall have the same right to vote on matters as any other Board member)

Replaced Section 11.1 with the following: There shall be an Executive/Bylaw Committee comprised of the officers of the Board. This committee shall meet as provided in these Bylaws and as otherwise deemed necessary by the Chairperson. The Chairperson shall serve as the Committee chair, and the Executive Director will serve as a non-voting, *ex officio* member of the Executive Committee. The Executive Committee shall:

- a. Act as advisor to the Chairperson;
- b. Exercise the powers of the Board between regular Board meetings, except that the Executive Committee may not take final action to amend these bylaws, remove a board member from office, hire or remove the Executive Director, or sell or acquire assets;
- c. Report to the Board at its next regular meeting on any official actions it has taken;
- d. Annually review and recommend to the Board any necessary change to the bylaws; and Annually review the

		performance of the Executive Director for report to the Board
7	May 26, 2015	Amended Section 6.1.q to include Licensed Independent Practitioner and term of same. Addition of Dental Director.
8	March 28, 2018	Amended Section 4.1 to update administrative address. Addressed grammatical errors throughout.
9	December 11, 2019	<u>Amended Section 8.7 to define healthcare.</u>

**DISTRICT CLINIC HOLDINGS, INC.
BOARD OF DIRECTORS
DECEMBER 11, 2019**

1. Description: Contracts Policy

2. Summary:

This item presents a corporate contracts policy.

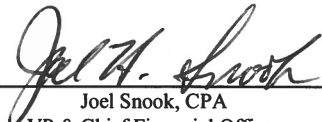
3. Substantive Analysis:

The Contracts policy was approved by the Health Care District Board on May 9, 2012. The corporate policy is attached for reference.

4. Fiscal Analysis & Economic Impact Statement:

	Amount	Budget
Capital Requirements	N/A	Yes <input type="checkbox"/> No <input type="checkbox"/>
Annual Net Revenue	N/A	Yes <input type="checkbox"/> No <input type="checkbox"/>
Annual Expenditures	N/A	Yes <input type="checkbox"/> No <input type="checkbox"/>

Reviewed for financial accuracy and compliance with purchasing procedure:



 Joel Snook, CPA
 VP & Chief Financial Officer

5. Reviewed/Approved by Committee:

N/A

 Committee Name

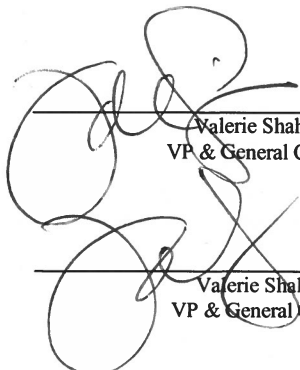
N/A

 Date Approved

6. Recommendation:


Staff recommends the Board approve the adoption of the Health Care District's Contracts Policy

Approved for Legal sufficiency:



 Valerie Shahriari
 VP & General Counsel

 Valerie Shahriari
 VP & General Counsel



 Dr. Belma Andric
 Chief Medical Officer, VP & Executive Director
 of Clinic Services

POLICY

Policy Title: **Contracts**

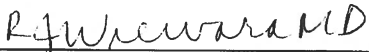
Effective Date: 05/09/2012

Department: **LEGAL**

Policy Number: N/A

POLICY

The District must review, approve and document all proposed contracts prior to execution by the District. This includes circumstances in which the District seeks to purchase goods and/or services and where the District seeks to acquire rights and/or obligations with respect to another person, entity or agency. To minimize legal and operational exposure, the District shall implement procedures to facilitate adequate review, approval, and thorough documentation prior to contract execution.

APPROVED BY	DATE
 Ronald J. Wiewora, MD, MPH, Chief Executive Officer	7/24/12
Health Care District Board	05/09/12

POLICY REVISION HISTORY

Original Policy Date

05/09/2012

Revisions

JUL 26 2012

DISTRICT CLINIC HOLDINGS, INC.
BOARD OF DIRECTORS
December 11, 2019

1. Description: Compliance Policy Updates

2. Summary:

Ongoing review and revision of policies is critical to an effective compliance program. The Compliance Department reviewed and revised Compliance policies in order to:

- Concretely demonstrate to employees and the community the District's strong commitment to honest and responsible provider and corporate conduct
- Ensure consistent processes, structures, and ongoing compliance
- Keep employees and the District current with regulatory and industry best practices

3. Substantive Analysis:

The Compliance Department reviewed and revised the following compliance policies:

- Non-Monetary Compensation for Physicians and Immediate Family Members
- Overpayments and Refunds Policy
- Gifts and Gratuities
- Non-Retaliation
- Physician Employment
- Standards of Conduct
- Business Associate Agreements
- Compliance Hotline
- False Claims Prevention
- Governmental Investigation
- Compliance Investigation
- Refund and Overpayment
- Non-Discrimination
- Standards of Conduct Acknowledgement Form

DISTRICT CLINIC HOLDINGS, INC.
BOARD OF DIRECTORS
December 11, 2019

4. Fiscal Analysis & Economic Impact Statement:

	Amount	Budget
Capital Requirements	N/A	Yes <input type="checkbox"/> No <input type="checkbox"/>
Annual Net Revenue	N/A	Yes <input type="checkbox"/> No <input type="checkbox"/>
Annual Expenditures	N/A	Yes <input type="checkbox"/> No <input type="checkbox"/>

Reviewed for financial accuracy and compliance with purchasing procedure:

N/A

 Joel H. Snook
 VP & Chief Financial Officer

5. Reviewed/Approved by Committee:

Quality, Patient Safety &
 Compliance Committee

 Committee Name

10Dec2019

 Date Approved

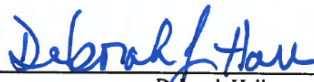
6. Recommendation:

Staff recommends the Clinic Board approve the adoption of the Compliance policy updates.

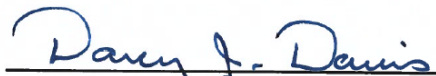
Approved for Legal sufficiency:



 Valerie Shahriari
 VP & General Counsel



 Deborah Hall
 VP, Chief Compliance and Privacy Officer &
 Internal Audit



 Darcy J. Davis
 Chief Executive Officer

Business Associate Agreement Policy and Procedure

Policy #:	HDCOM106	Effective Date:	10/11/2019
Business Unit:	HCD Shared Policies	Last Review Date:	
Approval Group:	HCD Compliance Policy	Document Owner(s):	Compliance
Board Approval Date:			

PURPOSE

To document the process for establishing the requirements and obligations of the Health Care District of Palm Beach County (“District”) when contracting with a person or another entity to perform healthcare activities and functions on its behalf that may involve the use of Protected Health Information (“PHI”).

SCOPE

This policy applies to the Health Care District of Palm Beach County and its Affiliated Entities, including, Lakeside Medical Center, E.J. Healey Center, Physician Practice Offices, Primary Care Clinics, School Health, Pharmacy, Aeromedical, Managed Care, and Trauma.

BACKGROUND

Although the HIPAA Privacy Rule applies only to covered entities, most health care providers and health plans do not carry out all of their health care activities and functions by themselves. Instead, they often use the services of a variety of other persons or businesses. The Privacy Rule permits covered entities and health plans to disclose protected health information to these “business associates” if the providers or plans obtain satisfactory assurances that the business associate will use the information only for the purposes for which it was engaged by the covered entity, will safeguard the information from misuse, and will help the covered entity comply with the covered entity’s duties under the Privacy Rule. Covered entities may disclose protected health information to an entity in its role as a business associate only to help the covered entity carry out its health care functions – not for the business associate’s independent use or purposes, except as needed for the proper management and administration of the business associate.

DEFINITIONS

Business Associate – an individual or entity, other than a workforce member of a covered entity, that performs an activity or function on behalf of a covered entity such as the District, that: involves the use, disclosure, or creation of PHI on behalf of a Covered Entity such as claims processing or administration, data analysis, processing administration, utilization review, quality assurance, billing, benefit management, practice management and re-pricing; or provides certain services to a covered entity such as legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services to a covered entity that involves access by the business associate to PHI. A “Business Associate” also is a subcontractor that creates, receives, maintains or transmits PHI on behalf of another business associate. A member of the covered entity’s workforce is not a business associate. However, a covered health care provider, health plan, or health care clearinghouse can be a business associate of another covered entity.

Business Associate Contract – a written agreement between a business associate (“BA”) and a covered entity that: establishes the permitted uses and disclosures of PHI by the BA; the safeguards the BA must employ to prevent unauthorized use and disclosure of PHI including the requirements of the HIPAA Security Rule regarding electronic PHI (“ePHI”); reporting requirement for any breaches or uses/disclosures not included in the contract; requires the BA to make available to HHS its internal practices, books and records relating to the contract; and sets forth the requirements of the BA upon termination of the contract.

Health Care Operations: any activities of the District that are related to the function covered under HIPAA

Including but not limited to: quality assessment and improvement activities, competency evaluations for medical staff, contracting for health insurance or health benefits, medical review, legal services, auditing functions, business planning and development, business management and administrative activities and resolution on internal grievances.

HIPAA Rules – mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

Disclosure: means the release, transfer, provision of access to, or divulging in any other manner of PHI outside of the District.

Protected Health Information (“PHI”) is information, including demographic information, created or received by the District, relating to the past, present, or future physical or mental health of a patient, member, or resident or the past, present, or future payment for the provision of health care for a

patient, member or resident. PHI identifies the patient, member or resident if there is reasonable basis to believe the information can identify the patient, member or resident.

Treatment: the provision, coordination or management of health care related services by one or more health care

providers, including the coordination or management of health care by a health care a health care provider with a third party; consultation between health care providers relating to a patient or the referral or patient or the referral of a patient for health care from one health care provider to another.

Use: with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

POLICY

The District will enter into a written contract with any person or entity, including a subcontractor, hereafter referred to as a business associate agreement, whenever the business relationship, service or activity may involve with the use and disclosure of PHI as defined by HIPAA Rules. Any such written contract or agreement must:

1. Describe the permitted and required uses of protected health information by the business associate;
2. Provide that the business associate will not use or further disclose the protected health information other than as permitted or required by the contract or as required by law; and
3. Require the business associate to use appropriate safeguards to prevent a use or disclosure of the protected health information other than as provided for by the contract.

Further, if the District knows of a material breach or violation by the business associate of the contract or agreement, the District will take reasonable steps to cure the breach or end the violation, and if such steps are unsuccessful, to terminate the contract or arrangement. If termination of the contract or agreement is not feasible, the District will report the problem to the Department of Health and Human Services (HHS) Office for Civil Rights (OCR). Contracts between business associates and business associates that are subcontractors are subject to the same requirements.

The master document is controlled electronically. Printed copies of this document are not controlled. Document users are responsible for ensuring printed copies are valid prior to use.

Business Associate Agreement Policy and Procedure

Procedure #:	HCDCOM106	Effective Date:	10/11/2019
Business Unit:	HCD Shared Policies	Last Review Date:	
Approval Group:	HCD Compliance Policy	Document Owner(s):	

PROCEDURE

The District will maintain a listing of all contracts with vendors and subcontractors. If the business relationship, activity or service involves the use or disclosure of protected health information a business associate agreement (“BAA”) will be obtained. The types of functions or activities that may make a person or entity a business associate include payment or health care operations activities, as well as other functions or activities regulated by the Administrative Simplification Rules. Business associate functions and activities include:

- Claims processing or administration;
- Data analysis, processing or administration;
- Utilization review;
- Quality assurance;
- Billing;
- Benefit management;
- Practice management; and
- Repricing.

Business associate services include legal; actuarial; accounting; consulting; data aggregation; management; administrative; accreditation; and financial.

See the definition of “business associate” at 45 CFR 160.103.

Prior to contracting with any outside vendor whether a person or entity, the Contracts Analyst shall be initially responsible for determining whether a vendor meets the requirements of a business associate of the District. The Chief Compliance Officer and Privacy Officer shall assist in this process as needed.

EXCEPTIONS

Workforce members and healthcare clearinghouses that provide services covered under (TPO) treatment, payment and health care operations

RELATED DOCUMENTS	
Related Policy Document(s)	
Related Forms	
Reference(s)	
Last Revision	
Revision Information/Changes	
Next Review Date	

The master document is controlled electronically. Printed copies of this document are not controlled. Document users are responsible for ensuring printed copies are valid prior to use.

Compliance Hotline

Policy #:	HCDCOM164	Effective Date:	10/14/2019
Business Unit:	HCD Shared Policies	Last Review Date:	
Approval Group:	HCD Compliance Policy	Document Owner(s):	Compliance

Board Approval Date:

SCOPE

This policy applies to all stakeholders and entities of the Health Care District of Palm Beach County (the “District”) and its affiliated entities including, Lakeside Medical Center, Edward J. Healey Center, C.L. Brumback Primary Care Clinics, and School Health.

POLICY

The District shall maintain a compliance (telephone) hotline operated by an independent third party vendor that may be used to report actual or potential violations or questionable conduct. All reports handled in a manner that protects the privacy of the caller. Any report may be made anonymously. Individuals who make a “good faith” report will be protected from retaliation or retribution. All reports will be investigated by Compliance Department under the direction of the Chief Compliance and Privacy Officer.

The master document is controlled electronically. Printed copies of this document are not controlled. Document users are responsible for ensuring printed copies are valid prior to use.

Procedure Name: Compliance Hotline

Procedure #:	HCDCOM164	Effective Date:	10/14/2019
Business Unit:	HCD Shared Policies	Last Review Date:	
Approval Group:	HCD Compliance Policy	Document Owner(s):	Compliance

PROCEDURE

1. The District’s Compliance Hotline is operated by an independent third party vendor to collect and document information provided by any and all callers. Calls will not be recorded and caller ID is not available to the vender. The toll-free Compliance Hotline number 1-866-633-7233 is available 24/7, 365 days a year. A trained operator will request and document the following information from the caller:
 - Name or location of the facility/entity
 - Date of the Call
 - Name and contact information of the caller (unless anonymous)
 - Descriptive information concerning the issue or concern being reported

A case number will be assigned to each caller as well as a severity code. A call back date will be given to the caller.
2. All documented Compliance Hotline calls will be forwarded to the Chief Compliance and Privacy Officer or their designee, who will initiate an investigation within 72 hours of receipt.
3. Employees who report problems and concerns in “good faith” via the Hotline will be protected from any form of retaliation or retribution.
4. The availability of the Compliance Hotline will be communicated at least annually to all District employees and other stakeholders through organizational policies, orientation, newsletters, e-mail communications and other communication vehicles as deemed appropriate.
5. All callers will be informed of their right to remain anonymous. No attempts will be made by the District to identify an anonymous caller. Whenever the caller discloses their identity it will be held in confidence to the fullest extent practical and/or allowable by law.
6. Any matter reported through the Compliance Hotline that is deemed to be potentially unlawful will be referred to legal counsel for advice and guidance.
7. The Chief Compliance and Privacy Officer or designee will:
 - Conduct the appropriate investigation and follow up of issues and concerns reported to the Compliance Hotline. The assistance of other department personnel from such areas as Legal, Human Resources, and Internal Audit will be enlisted if necessary to complete the investigation and/or

determine a course of action Provide feedback to the Compliance Hotline vendor on the status of the investigation and request additional information if needed.

- Maintain security for all calls and related documents involved in ongoing and completed investigations.
- Recommend remedial and/or disciplinary action, if any, based on the results of the investigation.

Potential Conflicts

8. In the event that the Chief Compliance and Privacy Officer (CCPO) is not satisfied that a reported issue or concern has been appropriately addressed and resolved, the CCPO is authorized to take the matter to the Chief Executive Officer and the Chair of the Quality, Patient Safety and Compliance Committee for further evaluation.
9. If a report directly involves the Chief Compliance and Privacy Officer, the hotline vendor will be directed to forward the call to the CEO. The CEO will review the nature of the call and determine validity. Once an issue is validated, the CEO will address the matter promptly with the Chair of the Quality, Patient Safety and Compliance Committee and ensure the appropriate corrective actions are taken.

The Chief Compliance and Privacy Officer will report hotline activity to the Quality, Patient Safety and Compliance Committee on a regular basis. The report will include the number and types of calls received and acted upon as well as general results from hotline operation. In addition the report will include any recommendations for system-wide improvements or corrective actions arising from the results of the operation and related investigations.

EXCEPTIONS

None.

RELATED DOCUMENTS	
Related Policy Document(s)	Compliance Investigations Internal Reporting of Potential Compliance Issues Non-Retaliation Policy
Related Forms	
Reference(s)	
Last Revision	
Revision Information/Changes	
Next Review Date	

The master document is controlled electronically. Printed copies of this document are not controlled. Document users are responsible for ensuring printed copies are valid prior to use.

Compliance Investigation Policy

Policy #:	HCDCOM109	Effective Date:	10/14/2019
Business Unit:	HCD Shared Policies	Last Review Date:	10/14/2019
Approval Group:	HCD Compliance Policy	Document Owner(s):	Compliance

Board Approval Date:

SCOPE

This policy applies to all reports of actual or suspected improper conduct made through any of the established communications mechanisms, of the Health Care District of Palm Beach County (the "District") and its affiliated entities including: Lakeside Medical Center, Edward J. Healey Center, Physician Practice Offices, C.L. Brumback Primary Care Clinics, Pharmacy, School Health, Aeromedical, Trauma and Managed Care.

POLICY

The District and its affiliated entities are fully committed to upholding the highest standards of honesty and ethics and compliance with all relevant laws and regulations. Any and all reports of improper conduct received by the District will be fully documented, investigated and responded to according to the general guidelines provided herein. The Chief Compliance and Privacy Officer (CCPO) has the full authority to and will be responsible for ensuring the timely and independent investigation of each reported matter according to its initial urgency, severity and level of detailed information provided. As necessary, the Legal Department will be included in the appropriate stages of the investigation process.

The master document is controlled electronically. Printed copies of this document are not controlled. Document users are responsible for ensuring printed copies are valid prior to use.

Procedure Name: Compliance Investigation Policy

Procedure #:	HCDCOM109	Effective Date:	10/14/2019
Business Unit:	HCD Shared Policies	Last Review Date:	10/14/2019
Approval Group:	HCD Compliance Policy	Document Owner(s):	Compliance

PROCEDURE

Investigative Procedure

Upon receipt of an employee complaint or other information (including audit results) which suggest the existence of a serious pattern of conduct in violation of applicable laws, rules, regulations, and/or compliance policies, an investigation shall be implemented by the Chief Compliance and Privacy Officer. Steps to be followed in undertaking the investigation shall include, at a minimum:

1. The Chief Compliance and Privacy Officer will notify the Chief Executive Officer and the Board Audit and Compliance Committee Chairman of the nature of the complaint and will obtain a memorandum from external counsel (“Counsel”) authorizing an investigation.
2. The investigation shall be commenced as soon as reasonably possible following the receipt of the complaint or report under the direction of Counsel. The investigation shall include, as applicable, but need not be limited to:
 - An interview of the complainant and other persons who may have knowledge of the alleged problem or process and a review of the applicable laws and regulations which might be relevant to or provide guidance with respect to the appropriateness or inappropriateness of the activity in questions, to determine whether or not a problem actually exists.

If the review results in conclusions or findings that the conduct reported is permitted under applicable laws, regulations or policy; that the act did not occur as alleged; or that it does not otherwise appear to be a compliance violation, the investigation shall be closed.

If the initial investigation concludes that there is improper billing occurring, that practices are occurring which are contrary to applicable laws, rules, and regulations; that inaccurate claims are being submitted, or that additional evidence is necessary, the investigation shall proceed to the next steps:

1. The identification and review of representative bills or claims submitted to the Medicare/Medicaid programs to determine the nature of the problem, the scope of the problem, the frequency of the problem, the durations of the problem, and the potential financial magnitude of the problem.

2. Interviews of the person or persons in the departments who appeared to play a role in the process in which the problem exists. The purpose of the interview will be to determine the facts related to the reported or discovered activity, and may include, but shall not be limited to:
 - Individuals understanding of the Medicare and Medicaid laws, rules and regulations;
 - The identification of persons with supervisory or managerial responsibility in the process;
 - The adequacy of the training of the individuals performing the functions within the process;
 - The extent to which any person knowingly or with reckless disregard or intentional indifference acted contrary to the Medicare or Medicaid laws, rules or regulations;
 - The nature and extent of potential civil or criminal liability of individuals or the District; and
 - Preparation of a summary report which
 - Defines the nature of the problem
 - Summarizes the investigation process
 - Identifies any person whom the investigator believes to have either acted deliberately or with reckless disregard or intentional indifference toward the Medicare/Medicaid laws, rules and policies,
 - If possible, estimates the nature and extent of the resulting overpayment exposure, if any.

DISTRICT RESPONSE

Possible Criminal Activity

In the event the investigation reveals billing or other violations of the law which constitute criminal activity of the law and are the result of intentional or willfully indifferent conduct on the part of any employee or business unit, the District shall undertake the following steps:

1. The facility shall immediately stop all billing related to the problem in the facility/business unit(s) where the problem exists until such time as the offending practices are corrected.
2. The facility management shall initiate appropriate disciplinary action against the person or persons whose conduct appears to have been intentional, willfully indifferent or with reckless disregard for the Medicare and Medicaid laws. Appropriate disciplinary action shall include, at a minimum, the removal of the person from any position with oversight for or impact upon the claims submissions or billing process and may include, in addition, suspension, demotion, and discharge, Where only Medicaid is involved, the (appropriate state agency) and/or the (state) Attorney General shall be notified. In the event that Medicare and Medicaid claims are involved, the District shall notify the programs through the local United States Attorney's Office or the local office of the United States Department of Health and Human Services Office of the Inspector General Division, as Counsel deems appropriate. The District, through its Counsel, shall attempt to negotiate a voluntary disclosure agreement prior to the disclosure.

3. Legal Counsel with the Chief Compliance and Privacy Officer will lead communication with the Board and Audit and Compliance Committee

OTHER NON-COMPLIANCE

In the event the investigation reveals billing or other problems which do not appear to be the result of conduct which is intentional, willfully indifferent, or with reckless disregard for the Medicare and Medicaid laws, the District shall nevertheless undertake the following steps:

1. Improper Payments. In the event the problem results in duplicate payments by Medicare or Medicaid, or payments for services not rendered or provided other than as claimed, it shall:
 - Correct the defective practice or procedure as quickly as possible.
 - Calculate and repay to the appropriate governmental entity duplicate payments or improper payments resulting from the act or omission; Initiate such disciplinary action, if any, as may be appropriate given the facts and circumstances. Appropriate disciplinary action may include, but is not limited to, counseling, demotion, suspension or discharge.
 - Promptly undertake a program of education at the appropriate business unit to prevent future similar problems.
2. No Improper Payment. In the event the problem has or does not result in an overpayment by the Medicare or Medicaid program, the District shall:
 - Correct the defective practice or procedure as quickly as possible.
 - Initiate such disciplinary action, if any, as may be appropriate given the facts and circumstances. Appropriate disciplinary action may include, but is not limited to, counseling, demotion, suspension or discharge.
 - Promptly undertake a program of education at the appropriate business unit to prevent future similar problems.

EXCEPTIONS

None.

RELATED DOCUMENTS	
Related Policy Document(s)	
Related Forms	
Reference(s)	

Last Revision	
Revision Information/Changes	
Next Review Date	

The master document is controlled electronically. Printed copies of this document are not controlled. Document users are responsible for ensuring printed copies are valid prior to use.

False Claims Prevention Policy and Procedure

Policy #:	HCDCOM124	Effective Date:	3/20/2013
Business Unit:	HCD Shared Policies	Last Review Date:	
Approval Group:	HCD Compliance Policy Board Approval	Document Owner(s):	Compliance
Board Approval Date:			

PURPOSE

The purpose of this policy is to inform workforce members about federal and state false claims laws to help detect and prevent fraud, waste and abuse in government funded health care programs.

SCOPE

This policy applies to all workforce members of the Health Care District of Palm Beach County and its Affiliated Entities (“District”), including, Lakeside Medical Center, E.J. Healey Center, School Health, Physician Practice Offices, Primary Care Clinics, Pharmacy, Aeromedical, Trauma and Managed Care. Workforce members include employees, contractors or agents of the District and its affiliated entities.

POLICY

FALSE CLAIMS LAWS

False claims laws permit the government to bring civil actions to recover damages and penalties when a healthcare provider submits a false claim. The purpose of these laws is to combat fraud, waste and abuse in government funded health care programs.

The federal False Claims Act makes it a crime for any person or entity to knowingly submit a false or fraudulent claim for payment of United States Government funds. The fines include a penalty of up to three times the Government’s damages, civil penalties ranging from \$5,500 to \$11,000 per (false) claim, and the costs of the civil action against the entity that submitted the false claim. The False Claims Act applies to any federally funded health care program, including Medicare or Medicaid.

The federal False Claim Act (FCA) provides a “qui tam” provision, commonly referred to as the “whistleblower” provision that permits a private person with knowledge of a false claim to bring a civil action on behalf of the United States Government and share in a portion of the funds recovered.

The FCA also contains a provision that protects whistleblowers from retaliation by their employer. Retaliation includes being discharged, demoted, suspended, threatened, harassed, or otherwise discriminated against for bringing the action forth.

Florida also maintains a false claims act that mirrors the federal FCA. Florida has also adopted several other false claims statutes that are intended to prevent fraud and abuse in any department or agency of the state, including the Florida Medicaid program.

Another federal law, the Program Fraud Civil Remedies Act of 1986 (“PFCRA”) provides administrative remedies for knowingly submitting false claims and statements. A false claim or statement includes submitting a claim or making a written statement that: (1) is for services that were not rendered; (2) asserts a material fact that is false; or (3) omits a material fact. A violation of PFCRA results in a maximum civil penalty of \$5,000 per claim plus an assessment of up to twice the amount of each false or fraudulent claim.

EXCEPTIONS

N/A

The master document is controlled electronically. Printed copies of this document are not controlled. Document users are responsible for ensuring printed copies are valid prior to use.

False Claims Prevention Policy and Procedure

Procedure #:	HCDCOM124	Effective Date:	3/20/2013
Business Unit:	HCD Shared Policies	Last Review Date:	
Approval Group:	HCD Compliance Policy Board Approval	Document Owner(s):	Compliance

PROCEDURE

Detecting and Preventing Fraud, Waste and Abuse in Federal Health Care Programs and other Claims Paid by Federal and State Government.

The District Compliance Program strives to detect and prevents fraud, waste and abuse through regular auditing and monitoring activities as well as through reports of suspicious behavior or potential compliance issues from employees, contractors and agents handling or processing claims. The District has implemented several policies and procedures supporting its efforts to detect and prevent violations of federal and state health care program requirements and the Districts own policies and procedures including the following:

- Standards of Conduct
- Compliance Hotline
- Non-Retaliation Policy
- Compliance Investigations
- Compliance Training and Education
- Government Investigations

Reporting of Potential Compliance Issues:

Any workforce member who has knowledge of or becomes aware of suspicious activity relating to the handling, processing, or payment of claims or any potential compliance issue has a duty to report such activities. Employees, contractors and agents can report their knowledge or suspicions to their immediate supervisor, another member of Management, the Chief Compliance and Privacy Officer or by calling the Compliance Hotline. Anyone making a good faith report (true and correct based on their knowledge and belief) regarding such behavior is protected from any type of retaliation from the District and its affiliated entities (as described above in the provisions of the FCA).

Communication

This policy and procedure will be communicated to all employees and included in compliance training and education and new hire orientation. A copy of this policy and procedure will also be made available to contractors and agents of the District via the organization's public website.

Definitions

Abuse - means provider practices that are inconsistent with sound fiscal, business, or medical practices, and result in an unnecessary cost to the government funded health care programs, or in reimbursement of services that are not medically necessary or that fail to meet professionally recognized standards for health care.

Fraud - is the intentional deception or misrepresentation made by a person with the knowledge that the deception could result in some unauthorized benefit to himself or some other person. It includes any act that constitutes fraud under applicable Federal or State Law.

Agents and Contractors – members of the workforce who act on behalf of the District to furnish, authorize, or monitor Medicare or Medicaid services or who perform billing and coding functions.

Waste – involves the overutilization of services or other practices that, directly or indirectly, result in unnecessary costs to the healthcare system, including the Medicare and Medicaid programs. It is not generally considered to be caused by criminally negligent actions, but by the misuse of resources.

Responsibility

Employee Responsibilities:

1. Do not engage in any behavior that violates the Federal or State False Claims Act.
2. Inform supervisor, Human Resources, the Chief Compliance and Privacy Officer, the Chief Executive Officer or the Compliance Hotline of any actual or suspected violations.
3. Follow the District's and departmental policies and procedures to ensure early detection and prevention of fraud, waste and abuse.

Department Directors/Managers/Supervisors Responsibilities:

1. Notify the Chief Compliance and Privacy Officer of any actual or suspected violations.
2. Create a work environment in which ethical concerns can be raised and openly discussed without fear of retaliation.
3. Ensure that employees follow the District's and departmental policies and procedures to ensure early detection and prevention of fraud, waste and abuse.

Chief Compliance and Privacy Officer Responsibilities:

1. Review and determine appropriateness of those involved in investigation upon receipt of report of possible violation.
2. Resolve the claim by notifying those involved and/or proper authorities.
3. Assist employees and supervisors in education on this policy.

Human Resources Responsibilities:

1. Notify Compliance Department of any claim reported.
2. Review and ensure appropriateness of any recommended employee actions.

RELATED DOCUMENTS	
Related Policy Document(s)	
Related Forms	
Reference(s)	
Last Revision	
Revision Information/Changes	
Next Review Date	

The master document is controlled electronically. Printed copies of this document are not controlled. Document users are responsible for ensuring printed copies are valid prior to use.

Gifts and Gratuities Policy and Procedure

Policy #:	HCDCOM125	Effective Date:	1/16/2013
Business Unit:	HCD Shared Policies	Last Review Date:	
Approval Group:	HCD Compliance Policy	Document Owner(s):	Compliance

Board Approval Date:

PURPOSE

This policy sets forth the standards that must be followed by all employees regarding the acceptance or giving of gifts and other business courtesies and is not intended to override or replace any section of the policy on Non-Monetary Compensation to Physicians or the Conflicts of Interest Policy.

SCOPE

This policy applies to all workforce members of the Health Care District of Palm Beach County and its affiliated entities including Lakeside Medical Center, Edward J. Healey Center, Physician Practice Offices, Primary Care Clinics, School Health, Pharmacy, Aeromedical, Trauma, and Managed Care.

POLICY

Workforce members should never offer, give, solicit or accept anything that would compromise or appear to compromise the recipient's ability to make fair, impartial, and balanced business decisions. Gifts and gratuities are not appropriate if they create an obligation, are given with the intent to inappropriately influence a specific decision or put you in a position where you appear biased. The following guidelines should be adhered to:

1. Accepting or giving cash or cash equivalents (e.g., gift certificates, stocks, bonds, etc.) is never permissible. This prohibition however does not preclude making a donation to a recognized and established charity (i.e., March of Dimes) or participating with others in a fundraising event that may benefit a patient or type of patient that the District serves.
2. Workforce members are prohibited from soliciting or accepting gifts or gratuities that may influence or appear to influence the recipient in the performance of his/her official duties for the purpose of influencing business decisions or the referral of patients/business.
3. Workforce members should not solicit personal gifts or gratuities from any individual or entity outside the District, including physicians, referral sources, service providers, vendors, manufacturer, suppliers, etc.
4. Workforce members shall not solicit or accept gifts from patients or their families. This would not preclude the acceptance of such incidental personal items such as a homemade cookie or a photograph.

5. Acceptance of unsolicited gifts, meals or entertainment from other parties outside of the District that are of nominal value of \$25 per occurrence or \$100 in any one calendar year from any one individual or entity.
6. Workforce members may not provide gifts that exceed \$25.00 in value to allied health professionals.

The master document is controlled electronically. Printed copies of this document are not controlled. Document users are responsible for ensuring printed copies are valid prior to use.

Gifts and Gratuities Policy and Procedure

Procedure #:	HCDCOM125	Effective Date:	1/16/2013
Business Unit:	HCD Shared Policies	Last Review Date:	
Approval Group:	HCD Compliance Policy	Document Owner(s):	Compliance

DEFINITIONS

Allied Health Professional - for the purpose of this policy means a physician assistant or advanced registered nurse practitioner with privileges at Lakeside Medical Center or practicing at E.J. Healey Center.

Workforce Members – employees, volunteers, trainees, contractors or subcontractors and other persons whose conduct in the performance of their assigned duties, is under the direct control of the District, Whether or not they are compensated directly by HCDPBC. This includes medical staff that are also required to comply with the Stark Laws.

Gratuities – includes such items as tips, perquisites, tokens, donations, freebies, benefits, extras, meals, entertainment and the like.

PROCEDURE

1. All workforce members are expected to use good judgment in all interactions with business associates and potential referral sources to insure such actions do not misrepresent [HOSPITAL] or violate ethical business practices. Executives and workforce members are also expected to become familiar with and fully comply with this policy before offering, giving, soliciting or accepting any gifts or gratuities of any type. Any questions or concerns should be immediately directed to your supervisor, the Chief Compliance and Privacy Officer or legal counsel for advice and resolution.
2. If you are offered a gift or gratuity that you feel may be inappropriate or would not comply with this policy, you should decline. If you face a situation where refusing a gift would embarrass or hurt the person offering it, you may accept the gift on behalf of the District and then immediately report it to your manager, the Chief Compliance and Privacy Officer.
3. Advance approval from the Chief Compliance and Privacy Officer or Legal Department is required prior to the initiation of any incentive, reward, contest, or referral program.
4. Gifts and gratuities provided to allied health professionals must be tracked on a log that describes the:
 - a. Name of allied health professional
 - b. Type of gift
 - c. Purpose of gift
 - d. Dollar value of gift

5. Violations of this policy shall be reported to the Chief Compliance and Privacy Officer.
6. All workforce members are expected to become familiar with and to adhere to this policy. Failure to comply may result in disciplinary action up to and including immediate termination, and may subject the individual and the District to legal liability and regulatory actions.

RESPONSIBILITY

All District employees are responsible for ensuring compliance with this policy.

EXCEPTIONS

It is permissible to accept:

1. An unsolicited perishable gift such as flowers or a box of donuts if the gift:
 - a. Cannot be returned or your refusal would embarrass or hurt the person offering it; and/or
 - b. Is not taken home for personal use; and
 - c. Is shared with all staff members at the location from which the workforce member provides services.
2. Unsolicited meals or entertainment of nominal value in situations where the meal or entertainment is provided as part of an educational seminar or training, and the seminar or training relates to the attendee's duties for the District.
3. The occasional offering, acceptance or exchange of promotional items of nominal value (e.g., pens, notebooks, mugs, etc.),
4. Meals and entertainment of modest/nominal value if intended to create goodwill and establish trust in a business relationship and not to influence the referral of business.
5. Items received from family members or friends when it is clear beyond a reasonable doubt that the gift was not made to gain or maintain [business] influence over the recipient.
6. Light refreshments of nominal value may be served to government officials during working meetings (e.g., coffee, juice, pastry, hors d'oeuvres, appetizers, etc.).

RELATED DOCUMENTS	
Related Policy Document(s)	
Related Forms	
Reference(s)	Non-Monetary Compensation to Physicians Conflicts of Interest
Last Revision	
Revision Information/Changes	
Next Review Date	

The master document is controlled electronically. Printed copies of this document are not controlled. Document users are responsible for ensuring printed copies are valid prior to use.

Government Investigation Policy and Procedure

Policy #:	HCDCOM126	Effective Date:	3/20/2013
Business Unit:	HCD Shared Policies	Last Review Date:	
Approval Group:	HCD Compliance Policy	Document Owner(s):	Compliance

Board Approval Date:

SCOPE

This policy applies to all workforce members of the Health Care District of Palm Beach County (“District”) and its affiliated entities including: Lakeside Medical Center, Edward J. Healey Center, Physician Practice Offices, Primary Care Clinics, Pharmacy, School Health, Aeromedical, Trauma and Managed Care.

POLICY

The Healthcare District of Palm Beach County (“District”) and its Affiliated Entities will cooperate with any reasonable demand made pursuant to a valid government investigation, subpoena, and search warrant. It is imperative, however, that the rights of both the District and its personnel are protected by following the procedures described below. If any workforce member receives an inquiry, a subpoena, or other legal document regarding the District’s business, whether at home or in the workplace, from any governmental agency or official, the District’s Legal Counsel and its Chief Compliance and Privacy Officer should be contacted immediately. The District normally arranges for the District’s Legal Counsel to accompany any workforce member being interviewed by a Governmental Agent. Legal Counsel and/or the Chief Compliance and Privacy Officer should be onsite whenever a Governmental Agent is present. The District relies on the common sense and alertness of its employees to inform the Chief Compliance and Privacy Officer regarding the initiation of any governmental investigation. Workforce members should never hide, alter or destroy any District documents, including any electronic information, during an investigation or search even if permitted to do so according to the District’s document management policy.

The master document is controlled electronically. Printed copies of this document are not controlled. Document users are responsible for ensuring printed copies are valid prior to use.

Government Investigation Policy and Procedure

Procedure #:	HCDCOM126	Effective Date:	3/20/2013
Business Unit:	HCD Shared Policies	Last Review Date:	
Approval Group:	HCD Compliance Policy	Document Owner(s):	Compliance

PROCEDURE

GOVERNMENTAL AGENT WITH SUBPOENA (DUCES TECUM):

If a Governmental Agent presents with a subpoena seeking District records at the District office, an Affiliated Entity (i.e. Lakeside Medical Center, Edward J. Healey Center, etc.) or at your home, the following procedure should be followed:

1. The most senior person at the site shall request the Agent display their official identification and request a business card. If the agent does not have a business card, the Agent's name and title should be recorded as soon as practical. Once proper ID has been verified, the senior person will accept service of the subpoena and fax a copy of the subpoena to District Legal Counsel and the Chief Compliance and Privacy Officer as soon as possible.
2. Do not immediately begin providing any documents to the Agent(s) at the time of service, as most subpoenas have a future return date for production of documents. However, if the governmental agent possesses a "forthwith subpoena", obtain a copy and contact District Legal Counsel and the Chief Compliance Officer.
3. The serving of a subpoena does not authorize law enforcement officers to interview employees about their work or District business. Interviews are voluntary. You have the right to refuse to answer any question posed by a Government Agent(s). You have a right to confer with counsel and have counsel present during the interview. While it is your decision to speak to a government agent or not, it is recommended that you do not make statements to the Agent, without legal counsel present.
4. A memorandum to all employees will be prepared and disseminated by Senior Management including the following:
 - a. The specific location that has received a subpoena requiring the production of documents and intent to comply fully with the subpoena;
 - b. The name of Compliance Counsel to assist with the response
 - c. Instruction to employees that no documents should be destroyed;
 - d. Advice to employees that if they are contacted by a governmental agent regarding the subpoenaed documents to obtain the name and telephone number of the Agent and refer the inquiry to District Legal Counsel

5. An independent records custodian will be identified to work with District Legal Counsel and Compliance Department to secure the documents compliance with the subpoena
6. Legal Counsel will review all documents retrieved
7. All documents produced for the government will be date stamped and copied so that a record of what is produced is maintained by District Legal Counsel.

GOVERNMENTAL AGENT WITH SEARCH WARRANT:

If a Government Agent presents at the District Office, an Affiliated Entity or your home with a search warrant, the following procedure should be followed:

1. The most senior person at the location will request that the Government Agent display their official identification and request a business card. If a business card is not available, record the name and the title of the Agent as soon as practical, then request a copy of the warrant and affidavit supporting execution of the search warrant. The affidavit may not be available if it is under seal, but request it anyway;
2. After accepting the warrant you should request time to fax a copy to the Chief Compliance and Privacy Officer and the District's Legal Counsel so they may examine the warrant prior to the commencement of the search. The warrant will include the premises covered; the specific documents, files and/or objects covered; the alleged offenses; and whether the warrant authorizes a search at that time of the day;
3. Identify and determine the Agency of each investigator present and the Agent in Charge and the name and contact information of the government attorney who is referenced in the Search Warrant
4. Senior management cannot direct the District's employees not to speak with investigators; however, they should advise any District's employees present that (a) they have no legal obligation to speak to investigators, (b) in the event an employee desires to speak with an investigator, such employee has the right to be represented by legal counsel prior to speaking with an investigator and may postpone any interview until such employee has retained counsel, (c) the employee may determine the time and location of any interview with investigators, (d) no negative inference shall be attributed to the District or its employees in a court proceeding for refusing to speak with investigators, (e) the District's attorney would prefer to be present during any discussions between the employee and investigators, and (f) the District's legal counsel is available to assist them, if they wish, with the selection of an attorney to represent them.
5. Senior management should advise the District's employees to refrain from engaging in casual conversation with investigators since any statements given by employees to investigators during non-custodial interviews may be used against such employees or the District in a court proceeding, regardless of whether the investigators administered warnings regarding the rights of interviewees and the possible repercussions of their testimony.
6. In the case of a search warrant, if practical, senior management should send home all non-essential employees

7. Senior management should instruct the District's employees not to shred any documents or erase any computer information during the search. You should also suspend any customary daily shredding during the search.
8. District Legal Counsel and the Chief Compliance Officer will come onsite
9. Do not obstruct, impede or interfere with the search as authorized, but do not consent to the search of other areas or documents that are not authorized by the warrant. Agents are entitled to seize only those documents specifically described in the search warrant.
10. Senior management will designate individuals to accompany each Agent, who will keep a detailed list of the areas searched; any questions that are asked and to whom the questions are directed; and any items seized, along with the location, office or file from which the documents came. You should obtain a copy of the agents' seizure inventory. The agents are required to leave with the District a signed inventory list of the seized property (See step 16 below.).
11. Senior management should obtain permission from investigators to copy all records necessary to the continued operation of the District's business prior to their removal from the premises. If the investigators/agents want to remove the computers, you should attempt to ask them to remove computer files or copies of such files only.
12. Direct all inquiries made by the Agent to District Legal Counsel;
13. Direct all requests to sign an affidavit of any kind to District Legal Counsel;
14. Senior management should indicate which documents you believe may be privileged materials and request the investigators or agents to permit you to retain those documents under seal or in the alternative, to seal such documents before releasing them. Examples of privileged materials are (1) attorney-client correspondence, (2) attorney work-product materials, (3) all documents related to the District's Quality Improvement and Risk Management Program.
15. Do not make any statement that indicates you consent or approve of the search. If an agent asks for your consent, inform the agents that you are not authorized to consent to the search and that all such requests should be directed to the District's Legal Counsel.
16. At the end of the search, the Law Enforcement Officers are required to provide you with an inventory of all items they have seized. If counsel has not arrived by the conclusion of the search, request and obtain a copy of the inventory from the agents.

If an employee has concerns about any governmental investigation, the employee may contact his or her manager or the District's Chief Compliance and Privacy Officer.

EXCEPTIONS

N/A

RELATED DOCUMENTS	
Related Policy Document(s)	
Related Forms	Whistleblower Policy and Procedure Standards of Conduct Policy and Procedure
Reference(s)	
Last Revision	
Revision Information/Changes	
Next Review Date	

This policy/procedure is only intended to serve as a general guideline to assist staff in the delivery of patient care; it does not create standard(s) of care or standard(s) of practice. The final decision(s) as to patient management shall be based on the professional judgement of the health care providers(s) involved with the patient, taking into account the circumstances at that time. Any references are to sources, some parts of which were reviewed in connection with formulation of the policy/procedure. The references are not adopted in whole or in part by the hospital(s) or clinic(s) / provider(s).

The master document is controlled electronically. Printed copies of this document are not controlled. Document users are responsible for ensuring printed copies are valid prior to use.

Non-Monetary Compensation to Physicians Policy and Procedure

Policy #:	HCDCOM165	Effective Date:	9/12/2012
Business Unit:	HCD Shared Policies	Last Review Date:	
Approval Group:	HCD Compliance Policy Board Approval	Document Owner(s):	Compliance
Board Approval Date:			

PURPOSE

To ensure compliance with federal and state laws regarding non-monetary compensation and incidental benefits provided to physicians and medical staff. This policy is intended to provide specific guidance regarding restrictions, limits and examples of the types of non-monetary compensation and incidental benefits that are permissible under the Federal “Stark” Laws. Under the Federal Stark Law, if a hospital has a financial relationship with a physician, the physician may not refer to the hospital for the provision of “designated health services” (including inpatient and outpatient hospital services), and the hospital may not bill for such services, unless an exception is met. A “financial relationship” under stark is construed very broadly, which means all remuneration from a hospital to a physician must be considered, including in-kind compensation.

SCOPE

This policy applies to the Health Care District of Palm Beach County (“District’) affiliates that employ physicians and other formal medical staff such as, Lakeside Medical Center, E.J. Healey Center and C L Brumback Clinics.

POLICY

Physicians

In addition to bona fide employment arrangements, a physician will be permitted to receive a limited amount of non-monetary compensation from the District if all of the following conditions are satisfied:

- The compensation does not take into account the volume or value of referrals or other business generated by the referring physician.
- The compensation may not be solicited by the physician or the physician's practice (including employees and staff members).
- The compensation “arrangement” does not violate the Federal anti-kickback statute, section 1128B (b) of the Social Security Act, or any Federal or State law or regulation governing billing or claims submission.

- The annual dollar limit or spending caps currently in place is not knowingly exceeded.

For the 2019 calendar year, the aggregate annual limit has been set at \$416.

Medical Staff

The District also permits providing incidental benefits to medical staff as long as they meet the following criteria:

- Provided to all members of the medical staff practicing in the same specialty (but not necessarily accepted by every member to whom it is offered) without regard to the volume or value of referrals or other business generated between the parties.
- Provided only during periods when the medical staff members are engaged in services or activities that benefit the hospital or its patients (i.e., directly or indirectly related to the delivery of medical services).
- Provided and used by the medical staff members only on the facility's campus including, but not limited to, Internet access, pagers, or two-way radios, used on or away from the campus only to access medical records or information, or to access patients or personnel who are on the campus,
- The value of the benefit is within the current per occurrence limit established.
- The compensation arrangement does not violate the Federal Anti- kickback provision in section 1128B (b) of the Act, or any Federal or State law or regulation governing billing or claims submission.
- Other facilities and healthcare clinics that have bona fide medical staff's may provide compensation under this paragraph on the same terms and conditions applied to hospital.

The 2019 limit for these incidental benefits is \$35 per occurrence.

Medical Staff Appreciation Event

The Stark Law does allow a hospital with a formal medical staff to provide a local staff appreciation event once a year without adhering to the spending caps described above. Any gifts or gratuities provided in connection with the event, however, are subject to the spending cap.

The master document is controlled electronically. Printed copies of this document are not controlled. Document users are responsible for ensuring printed copies are valid prior to use.

Non-Monetary Compensation to Physicians Policy and Procedure

Procedure #:	HCDCOM165	Effective Date:	9/12/2012
Business Unit:	HCD Shared Policies	Last Review Date:	
Approval Group:	HCD Compliance Policy Board Approval	Document Owner(s):	

PROCEDURE

1. The District will implement reasonable mechanisms to track and value the provision of gifts, complimentary items and other benefits to physicians and formal medical staff to ensure non-monetary compensation and incidental benefits do not exceed the established spending limits.
 - a. Non-monetary compensation must be tracked using the attached Physician Function Log (see attached) whereas incidental medical staff benefits that fall within the limits need not be tracked.
2. The hospital CFO or designee and the Healey Center and Clinic Finance Department will be responsible for tracking all non-monetary compensation at their respective facilities.
3. Any questions regarding the applicability or value of non-monetary compensation or incidental benefit should be brought to the attention of the Legal Department and/or the Chief Compliance and Privacy Officer as soon as practical.
4. Annually the District will review all non-monetary compensation and incidental benefits provided to its physicians and medical staff to ensure that established limits have not been exceeded.
5. Where the District has inadvertently provided nonmonetary compensation to a physician in excess of the limit such compensation is deemed to be within the limit if (i) the value of the excess nonmonetary compensation is no more than 50 percent of the limit; and (ii) the physician returns to the District the excess nonmonetary compensation (or an amount equal to the value of the excess nonmonetary compensation) by the end of the calendar year in which the excess nonmonetary compensation was received or within 180 consecutive calendar days following the date the excess nonmonetary compensation was received by the physician, whichever is earlier. The “return” option may be used by an entity only once every three (3) years with respect to the same referring physician.
6. Knowingly and willfully violating this policy will subject the offenders to disciplinary action, up to and including immediate dismissal.

Examples of Non-Monetary Compensation that MUST be tracked:

- Business related meals not furnished in connection with an executed, bona fide personal services arrangement.
- Sporting events or other similar events such as theater and concerts, including the cost of the tickets and a pro rata allocation of the cost of the meal, if applicable.

- Local recreational events, such as fishing, boating, hunting and golfing, including event fees (e.g., admission, equipment rental, greens fees, cart fees, meals, etc.) but excluding the value of any charitable contribution if the event is a charity event.
- CME seminars held off-campus or on-campus if the cost exceeds the per-occurrence limit (e.g. \$35 for 2019).
- Flowers or other gifts provided physicians or their immediate family members to recognize a special event, such as a birthday.
- Room allowances or other financial benefits provided to physician governing board members at a governing board retreat if the benefit is not offered to all governing board members and if they are not covered under a personal services arrangement or listed in his/her appointment letter.
- Prizes and awards given on special days, such as "Doctor's Day".
- Holiday gifts given to governing board members and Chiefs of Staff in recognition of the time and energy expended on behalf of the hospitals and communities they serve.

Examples of Non-Monetary Compensation or Incidental Benefits that need NOT be tracked:

- Free or discounted meals (such as meals served in the physician's lounge), parking and computer/internet access provided in the hospital, so long as they are provided to all members of the medical staff without regard to the volume or value of referrals.
- CME seminars held on campus provided the value of the CME seminar is less than \$35 per invited physician per occurrence, or compliance training held in the local service area where the primary purpose of the seminar is compliance training, regardless of cost.
- Governing board retreats where the hospital pays for travel, food and lodging for all its governing board members and the benefit is included as compensation in the member's appointment letter. In addition, the

hospital may pay for leisure activities of its physician governing board members and the physician's spouse provided the benefit is provided to all governing board members and the benefit is included as compensation in the member's appointment letter.

- Meals provided to an existing member of the medical staff and their spouse where the purpose of the meal is to recruit a physician or other provider to the community and the meal is attended by a District representative, the existing physician member and the recruit and is pursuant to an executed agreement furnished by the Legal Counsel.
- Business related meals where the purpose is to discuss the physician's duties under a services agreement with the hospital where (i) the agreement specifically contemplates such business meals,

and (ii) the meal is modest as judged by local standards and occurs in a venue conducive to conducting a meeting.

- Large donation (i.e., \$1,000) to a local charity in honor of a specific member of the medical staff.
- Retirement present (i.e., \$500 gold watch) given to a physician on the day of his retirement. Physician is no longer a referral source upon retirement (but don't give the gift prior to his/her retirement date).

EXCEPTIONS

N/A

RELATED DOCUMENTS	
Related Policy Document(s)	
Related Forms	
Reference(s)	<ul style="list-style-type: none"> - 42 U.S.C. 1320a-7b; 42 C.F.R. 1001.952(a)-(a) - 42 U.S.C. 1395nn; 42 C.F.R. §§411.350-411.361 (Stark Regulations) - OIG Draft Supplemental Compliance Program Guidance for Hospitals, dated June 8, 2004
Last Revision	
Revision Information/Changes	
Next Review Date	

The master document is controlled electronically. Printed copies of this document are not controlled. Document users are responsible for ensuring printed copies are valid prior to use.

Non-Retaliation Policy and Procedure

Policy #:	HCDCOM134	Effective Date:	1/16/2013
Business Unit:	HCD Shared Policies	Last Review Date:	
Approval Group:	HCD Compliance Policy	Document Owner(s):	Compliance

Board Approval Date:

SCOPE

This procedure applies to the employees of the Health Care District of Palm Beach County (“District”) and its Affiliated Entities, including Lakeside Medical Center, E.J. Healey Center, School Health, Physician Practice Offices, Primary Care Clinics, Pharmacy, Aeromedical, Trauma, and Managed Care.

POLICY

It is the policy of the Health Care District of Palm Beach County (“District”) and its Affiliated Entities that positive employee relations and morale is best achieved and maintained in an environment that promotes ongoing open communication between managers and their employees, including open and candid discussion of employee problems and concerns. The District encourages its employees to express their concerns and opinions regarding improper business conduct and other wrongdoing without fear of retaliation or reprisal.

1. All employees have an affirmative duty and responsibility for reporting perceived misconduct, including actual or potential violations of the laws, regulations, unethical behavior, policies, procedures or the Standards of Conduct.
2. An open door policy shall be maintained by all levels of management to encourage employees to report problems and concerns.
3. Any threats or acts of retaliation or reprisal against an employee who reports a perceived wrongdoing in “good faith” is strictly prohibited. Good faith reporting involves a truthful and honest intent to act without taking an unfair advantage over another person. In other words you believe that what you are reporting is true and correct to the best of your knowledge.
4. Any employee who believes that he or she is being retaliated against by a superior or peer for making a good faith report should immediately notify the Chief Compliance and Privacy Officer and/or a Human Resources representative.
5. Anyone who intentionally makes a false report will be subject to disciplinary action.

Non-Retaliation Policy and Procedure

Procedure #:	HCDCOM134	Effective Date:	1/16/2013
Business Unit:	HCD Shared Policies	Last Review Date:	
Approval Group:	HCD Compliance Policy	Document Owner(s):	Compliance

PROCEDURE

All managers should encourage the reporting of suspected or known wrongdoing and ensure that employees will not be threatened or retaliated against for reporting issues and concerns in good faith.

The following actions will be taken across all operations on a yearly basis:

1. All managers will receive a copy of this policy along with a brief discussion of the spirit, intent and importance of this policy.
2. A copy of this policy will be made available to all employees.
3. A review will be conducted with all managers regarding the proper treatment of employees and the creation of a work environment that permits open communication.

All managers will meet with their employees to discuss this non-retaliation policy.

Every employee must understand that any incident where retaliation or reprisal can be related to an employee raising/reporting a problem regarding business conduct will not be tolerated. Reports of this nature will be reported to and investigated by the Chief Compliance and Privacy Officer with appropriate disciplinary actions taken up to and including termination of employment.

RESPONSIBILITY

EMPLOYEE'S RESPONSIBILITIES:

1. Concerns regarding any suspected or known wrongdoing or other improper business conduct should be reported to the District's management in the following order: (a) immediate supervisor, (b) Senior Management Team
2. If, for any reason, employees feel constrained or uncomfortable reporting any issues or concerns to a member of management should address such concerns to the Director of Human Resources
3. If an employee's concern or problem cannot be satisfactorily resolved through the methods described above, the employee should report the concern to the Chief Compliance and Privacy Officer either directly or through the hotline.

MANAGER'S RESPONSIBILITIES:

1. Promote an “open-door” attitude about Standards of Conduct concerns at all times.
2. Keep Human Resources and/or the Chief Compliance and Privacy Officer informed of all issues and concerns raised by employees.
3. Fully document and discretely investigate the matter in a timely manner (within 7 working days if possible). If a resolution can be reached, inform the employee of the results of the investigation and the resolution.
4. If the investigation cannot be completed or a resolution reached at the local level, refer the matter to the Chief Compliance and Privacy Officer.
5. Ensure the confidentiality of the reporting employee to the extent possible up to the limit of the law.

RELATED DOCUMENTS	
Related Policy Document(s)	
Related Forms	Anti-Discrimination and Harassment Policy False Claims Prevention Policy Standards of Conduct Policy Whistleblower Policy
Reference(s)	
Last Revision	
Revision Information/Changes	
Next Review Date	

The master document is controlled electronically. Printed copies of this document are not controlled. Document users are responsible for ensuring printed copies are valid prior to use.

Overpayments and Refunds Policy and Procedure

Policy #:	HCDCOM147	Effective Date:	1/16/2013
Business Unit:	HCD Shared Policies	Last Review Date:	
Approval Group:	HCD Compliance Policy Board Approval	Document Owner(s):	Compliance
Board Approval Date:			

PURPOSE

The purpose of this policy is to ensure that all credit balances are examined regularly and any overpayments are returned to the appropriate patient(s), guarantor(s) or third-party payer(s) in a timely manner and in accordance with all applicable laws/regulatory requirements. Further, the Health Care District of Palm Beach County (the "District") requires that all overpayment situations be examined to identify trends or recurrent actions that require corrective action to determine preventative measures that may be taken.

SCOPE

This policy applies to all excess payments made to the Health Care District of Palm Beach County (the "District") or its affiliated entities received from any payer source for any reason.

POLICY

The District is committed to conducting timely and thorough investigation of all potential excess payments and returning all bona fide overpayment via refunds, account adjustments or take-backs to the appropriate payer within 60 days after the overpayment has been confirmed and quantified.

DEFINITIONS

Overpayment - a credit balance that results when an improper or excess payment is made to a provider (hospital, clinic, home health, etc.) as a result of patient billing or claims processing errors. Examples of improper or excess payments include instances where a provider is:

- Paid for primary benefits twice.
- Paid for services planned but not performed or for non-covered services.
- Overpaid because of errors made in calculating beneficiary deductible and/or coinsurance amounts.
- Hospital bills and is paid for outpatient services included in a beneficiary's Inpatient claim (e.g., 72-hour rule).
- Paid for services after benefits have been exhausted or where the individual is not otherwise entitled to benefits.

- Paid for services/items that are non-covered, medically unnecessary or custodial care. Paid for services/items that are non-covered, medically unnecessary or custodial care.
- Erroneous information on claims resulting in incorrect DRG codes.
- Inclusion of non-allowable excessive costs in the provider's cost report.
- Services were rendered in a non-participating portion of the facility, or in a bed certified for a type of care other than what was furnished.
- Services were billed and paid by Medicare and the facility later discovers the service was part of a clinical trial and Medicare should not have been billed.
- The facility billed accounts using the wrong provider number i.e., using the Acute Care Provider number when billing patients in the Psychiatric Distinct Part Unit (DPU).
- Overpayments or credit balances would not include proper payments made by Medicare in excess of the provider's charges, such as DRG payments made to hospitals under the Medicare Prospective Payment System.

Identification – an overpayment is considered to be identified when a provider or supplier has or should have, through the exercise of reasonable diligence, determined that it has received an excess payment and quantified the amount of such overpayment. In the Final 60-Day Rule which became effective March 14, 2016, CMS clarified that identification does not occur until both an investigation and quantification of the amount have occurred.

Reasonable Diligence - CMS stated that reasonable diligence is demonstrated through the timely, good faith investigation of credible information which supports a reasonable belief that an overpayment may have been received. The benchmark for timely investigation is "at most 6 months from the receipt of credible information", except in extraordinary circumstances.

Repayment Period – repayment must then be made within 60-days after the reasonable diligence is completed, or the day the provider or supplier received credible information of the potential overpayment if the provider or supplier failed to conduct reasonable diligence. The final rule clarifies that the failure to conduct reasonable diligence, standing alone, does not in and of itself create liability or start the 60-day clock ticking on the requirement to make a repayment, but instead triggers an obligation to exercise reasonable diligence.

Lookback Period – CMS indicated that when a provider or supplier receives credible information of a potential overpayment, such as a RAC finding, they need to review such findings and determine whether they have received overpayments going back six full years. For providers and suppliers reporting and returning overpayments on or after March 14, 2016, even if the overpayments were received prior to that date, the requirements of the final rule apply.

The master document is controlled electronically. Printed copies of this document are not controlled. Document users are responsible for ensuring printed copies are valid prior to use.

Overpayments and Refunds Policy and Procedure

Procedure #:	HCDCOM147	Effective Date:	1/16/2013
Business Unit:	HCD Shared Policies	Last Review Date:	
Approval Group:	HCD Compliance Policy Board Approval	Document Owner(s):	Compliance

PROCEDURE

The following steps will be performed to ensure timely and accurate refunds of overpayments. Patient accounts with credit balances are to be researched for errors such as overpayments, duplicate payment/contractual entries, misapplied charges/credits, and incorrect patient account adjustments, etc. Once researched, all bona fide overpayments must be promptly refunded to the appropriate patient, guarantor, or third-party payor.

1. The District will regularly review all reports and or transactions that identify a credit balance or otherwise may indicate that a duplicate or excess payment has been received for any supply or service that was billed to a commercial or federally funded health care program.
2. The Business Office will analyze and trend overpayments by claim type and cause. Preventative measures will be identified and pursued as appropriate.
3. Individual credit balances or claim types with a high propensity for overpayments will be investigated to determine whether an excess payment has been received. Based on the volume of items, investigations will be scheduled based on the time and amount of the suspected overpayment (i.e., the oldest and largest credit balances will be examined first).
4. Once an overpayment has been identified, the account(s) must be investigated to determine if an overpayment situation requires:
 - a. Filing an adjustment claim;
 - b. Issuing a refund check to the payer; or
 - c. Cancelling the claim and issuing a new one.
5. Generally, overpayments are handled by filing adjustment claims and allowing the payer to recoup their original payment and process the corrected payment. However, it may be necessary to issue a refund check to the payer.
 - a. If adjustment claim can be entered "on line" (or via your electronic billing system), it is not necessary to complete the payer notification form.
 - b. If an adjustment claim cannot be entered on line, it is necessary to complete the payer notification form and the payer must be notified of the overpayment situation within 30 days of identification. If a government payer does not want you to submit the form, you must obtain written notification and fax a copy to the PFS Department as supporting documentation.

6. A log shall be maintained of all overpayments identified and repayments made. This log shall provide a detailed listing of account information which is necessary to identify recurrent errors and trends as well as ensure that corrective action is taken to resolve the problem(s) within 60 days of identification.
7. Quarterly the Overpayments Reporting Log shall be submitted to the Quality, Patient Safety and Compliance Committee for review.

EXCEPTIONS

N/A

Unclaimed Property

In order to comply with state unclaimed property laws, a reasonable effort must be made to locate the party who made the overpayment. The notice must inform the party that the facility is in possession of property belonging to him/her and instruct the party on how to collect the property. This notice must be sent first class mail with a return receipt.

If efforts are not successful to refund the entire amount owed because of the inability to locate the patient, guarantor or third-party payor to whom the refund is due, the credit amount should be recorded to a liability account at the District by Finance and a detailed log should be maintained which supports the balance of the liability account. The log should include, at a minimum, the account number, patient name, party making overpayment, address of party making overpayment, and the date of the overpayment.

Where there is a continued inability to locate the patient, guarantor or the third party to whom the refund is owed, final disposition of the payment must be processed according to the Florida State escheat law by the District's Finance Department.

RELATED DOCUMENTS	
Related Policy Document(s)	
Related Forms	
Reference(s)	42 U.S.C. Section 1395cc(a)(1)(C) 42 C.F.R. Sections 489.20(b), 489.40, 489.41 Medicare Intermediary Manual (Sections 3401, 3401.1, 3401.2, 3401.3) The OIG's Compliance Program Guidance for Hospitals, February 1998. Chap 717 F.S. Disposition of Unclaimed Property
Last Revision	

Revision Information/Changes	
Next Review Date	

The master document is controlled electronically. Printed copies of this document are not controlled. Document users are responsible for ensuring printed copies are valid prior to use.

Physician Employment Policy and Procedure

Policy #:	HCDCOM142	Effective Date:	1/16/2013
Business Unit:	HCD Shared Policies	Last Review Date:	
Approval Group:	HCD Compliance Policy Board Approval	Document Owner(s):	Compliance
Board Approval Date:			

PURPOSE

The purposes of this policy and procedure is to: (1) establish standard procedures for creating physician employment arrangements; (2) ensure compliance with all applicable laws including without limitation, the Stark Laws and Federal and State Anti-kickback Statutes; and (3) promote sound business judgments in connection with all physician arrangements. All physician employment arrangements must be in writing, signed by all parties, and comply with these guidelines.

SCOPE

This policy applies to all affiliates of the Health Care District of Palm Beach County (the "District") that may employ a physician, specifically, Lakeside Medical Center, Physician Practice Offices, Primary Care Clinics, E.J. Healey Center, School Health, Aeromedical, Trauma, and Managed Care.

POLICY

Any arrangements must be undertaken without regard to the value or volume of referrals and must not intend to induce referrals of patients or health care products or services. The District will not enter into any physician arrangement unless the District has an objectively determined, legitimate need for the services contemplated by the arrangement.

All physician arrangements must be approved prior to execution, commencement of services or remuneration by Legal Counsel, District CFO and Chief Compliance and Privacy Officer. For each proposed arrangement, the appropriate Affiliated Entity shall prepare all of the following documentation for submission into the contracts database.

Physician employment arrangements will be pursued only when the District has identified a legitimate need for a physician to provide the type and quantity of services contemplated by the employment arrangement to promote quality, cost-effective care or fulfill other legitimate needs of the District;

- The remuneration paid pursuant to all physician employment arrangements must be commercially reasonable and consistent with regional fair market value⁶ for the services furnished, if available;
- Services furnished pursuant to a physician employment arrangement are appropriately documented by the physician;
- All physician employment arrangements comply with applicable laws and regulations, including the federal Anti-Kickback law and the Stark Laws; and
- Under no circumstance will a physician employment arrangement involve the District paying remuneration to a physician, directly or indirectly, with the intent to induce the physician to refer patients to, or otherwise generate business for any District entity.

EXCEPTIONS

N/A

DEFINITIONS

Physician Arrangement: includes new and renewed contracts with a physician¹ or a group practice. Arrangements shall mean every arrangement or transaction that:

- Involves, directly or indirectly, the offer, payment, solicitation, or receipt of anything of value; and is between the District and any actual or potential source of health care business or referrals to the District. The term “source” shall mean any physician, contractor, vendor, or agent and the term “health care business or referrals” shall be read to include referring, recommending, arranging for, ordering, leasing, or purchasing of any good, facility, item or service for which payment may be made in whole or in part by a federal health care program; or
- Is between the District and a physician (or a physician’s immediate family member (as defined at 42 C.F.R. § 411.351² who makes a referral³ to the District for designated health services.⁴

Contracts Database: means the repository for all contracts at the District. The current repository is Compliance 360.

Physician: means a duly licensed and authorized doctor of medicine, osteopathy, doctor of dental surgery or dental medicine, doctor of podiatric medicine, doctor of optometry, or chiropractor.

Immediate Family Member: refers to a member of a physician’s family including a spouse (i.e., husband or wife); birth or adoptive parent, child, or sibling; stepparent, stepchild, stepbrother, or stepsister; father-in-law, mother-in-law, son-in-law, daughter-in-law, brother-in-law, or sister-in-law; grandparent or grandchild; and spouse of a grandparent or grandchild.

Referrals: are defined as the request by a physician for an item or service, including the request by a physician for a consultation with another physician (and any test or procedure ordered by, or to be performed by (or under the supervision of) that other physician or pursuant to the request or establishment of a plan of care by a physician which includes the provision of the designated health service.

Designated health services: include: clinical laboratory services, physical therapy services; occupational therapy services; radiology services (including magnetic resonance imaging, computerized axial tomography scans, ultrasound services, and nuclear medicine and supplies) ; durable medical equipment and supplies; parenteral and enteral nutrients, equipment, and supplies; prosthetics, orthotics, and prosthetic devices and supplies, home health services; outpatient prescription drugs and inpatient hospital services.

Remuneration: means anything of value including but not limited to, cash, items or services.

Fair Market Value: means the value of an arm’s length transactions, consistent with the compensation that would be included in a services agreement, as the result of a bona fide bargaining between well-informed parties to the agreement who are not otherwise in a position to generate business for the other party at the time of the agreement.

Physician Employment Policy and Procedure

Procedure #:	HCDCOM142	Effective Date:	1/16/2013
Business Unit:	HCD Shared Policies	Last Review Date:	
Approval Group:	HCD Compliance Policy Board Approval	Document Owner(s):	Compliance

PROCEDURE

Implementation:

The District shall ensure that this policy is adhered to by following all of the steps set forth in this policy.

1. Identify the Need for the Services

The District shall obtain appropriate evidence indicating that a physician should be retained to furnish the services contemplated by the physician employment arrangement in order to promote quality, cost-effective care or fulfill other legitimate needs of the District entity. In the case of professional medical services, the District entity shall identify why the physician should be engaged as an employee rather the physician bill payers or patients independently for the service.

2. Project the Number of Hours Required (Part-Time Employment)

Part-time employment should typically be contracted for on an hourly basis (in certain circumstances, "half-day" or "shift"-type arrangements may be appropriate). A District Affiliate may not enter into a part-time physician employment arrangement on an hourly basis unless the District entity has made an objective determination that the number of hours of services contemplated by the physician employment arrangement is reasonable and necessary to accomplish the District entities legitimate needs for the services. The District entity must prepare a written projection of the number of hours reasonably necessary for the physician employee to discharge the services based on:

- a. Any benchmarks referenced by legal authorities, government organizations, provider accreditation bodies, medical education program accreditation bodies,
- b. Independent third party consultants, third party payers, or the entity's medical staff or support board;
- c. Data from time logs; and/or
- d. Other appropriate factors, such as a detailed description of the scope of the services.

3. Demonstrate the Professional Qualifications of the Physician

The District entity may not enter into a physician employment arrangement unless the entity has objectively determined that the physician is qualified and capable of performing the services desired. To demonstrate the physician's qualifications, the entity must:

- a. Verify that the physician is capable of furnishing the services contemplated under the employment arrangement (i.e., the physician must confirm that he/she does not have other preexisting obligations which would limit or restrict the physician from fully performing the services.
- b. Obtain a copy of the physician's curriculum vitae for initial agreements.
- c. Verify that the physician is currently licensed in the State at the Florida Department of

Health website (ww2.doh.state.fl.us).

- d. Verify that the physician is qualified to provide the services (e.g., that the physician possesses relevant training and/or experience in the area); and
- e. Verify, through a search of the U.S. General Services Administration's ("GSA") Lists of Parties Excluded from Federal Procurement and Non procurement Programs and of the OIG's List of Excluded Individuals/Entities, that the physician has no exclusions, suspensions or debarments from participation in any federal health care program,

4. Calculate Fair Market Value

The District entity may not enter into a physician employment arrangement unless the District entity has objectively determined and documented that the compensation being offered to the physician for the services is consistent with fair market value.

- a. For services to be compensated on an hourly basis, in order to ensure that the compensation is consistent with fair market value, the District entity shall derive an hourly rate to be utilized in calculating the compensation by taking the average of the 50th percentile salary for the physician's specialty of the most recent publications of two national salary surveys and dividing the resulting figure by 2,000 hours.

The two national surveys may be selected from any of the following three surveys:

- (1) Sullivan, Cotter & Associates, Inc. -- Physician Compensation and Productivity Survey
- (2) American Medical Group
- (3) Hospital and Healthcare Compensation Services – Physician Salary Survey Report
- (4) Medical Group Management Association – Physician Compensation and Productivity Survey

The District entity shall multiply the hourly rate derived above (or any lesser amount) by the projected number of hours set forth in the physician employment agreement in order to determine the compensation to be offered for the services of the particular physician.

Notwithstanding the foregoing, if the District entity believes that the compensation derived from the above methodology does not represent fair market value (the compensation amount exceeds the fair market value rate determined by the internal methodology) of the physician's services, a written fair market value appraisal by an approved, independent, third party is required for physician employment agreements.. The District entity shall provide all supporting documentation, as well as any other information requested, to the COMPLIANCE 360 package.

- b. For full-time employment services, in order to ensure that the compensation is consistent with fair market value; the District entity shall derive an annual compensation salary equal

to or less than the average of the 50th percentile salary for the physician's specialty of the most recent publications of two national salary surveys. The two national surveys may be selected from any of the following three surveys:

- (1) Sullivan, Cotter & Associates, Inc. -- Physician Compensation and Productivity Survey
- (2) American Medical Group
- (3) Hospital and Healthcare Compensation Services – Physician Salary Survey Report
- (4) Medical Group Management Association – Physician Compensation and Productivity Survey

Notwithstanding the foregoing, if the proposed physician employment agreement includes bonus compensation that has the potential to exceed the average compensation derived from the above.

Methodology, a written fair market value appraisal by an approved, independent, third party is required for personal and administrative services agreements. The District entity shall provide all supporting documentation to Compliance 360.

5. Terms

The term of the physician arrangement must be at least one year. If the physician arrangement is terminated with or without cause, the parties may not enter into the same or substantially same arrangement during the first year of the original term of the arrangement.

6. District Purchasing Policy

All Physician Arrangements must also comply with the Districts Purchasing Policy

PREPARATION:

1. Administrator or designee should prepare and submit a cover memo to the contracts administrator (or designee) via e-mail. The cover memo should contain the following (see Attachment A):
 - a. A detailed description of the services to be provided.
 - b. The reason why the District needs the services.
 - c. The means of calculating fair market value of the remuneration.
 - d. An outline of the terms and conditions of the proposed physician arrangement.
 - e. An outline of all previous, current or anticipated agreements between the District and the physician or immediate family member of the physician.
 - f. A statement/memo of whether any immediate family members of the physician have financial arrangement with the District Entity.
 - g. A statement that the proposed agreement represents the entire agreement with respect to the physician agreement between the District and the physician.
2. Draft agreement template.
3. Copies/folder of all internal and external correspondence (including e-mails, memos, etc) that have been generated in connection with the proposed agreement, as applicable, for

review by CLO or CCO.

4. A copy of the physician's current curriculum vitae (new agreements).
5. A copy of the physician's current professional license verified at ww2.doh.state.fl.us.
6. A criminal background check on the physician.
7. The results of an OIG/GSA search noting no exclusions, suspensions, or debarments of the physician from participating in any federal health care program.
8. Evidence of a National Provider Identifier Number, Medicare and Medicaid Provider Number.
9. All separate arrangements between the facility and physician and/or the physician's immediate family members must incorporate each other by reference or cross-reference.

APPROVAL:

No agreement shall be executed until the District's Legal Counsel, CFO and Chief Compliance and Privacy Officer have reviewed and approved the proposed agreement to ensure compliance with the applicable laws and ensured that all documents relevant to the physician arrangement are set forth in Compliance 360.

EXECUTE:

Once all the approvals have been obtained and documented in the Compliance 360, the District CEO or CFO may execute the agreement on behalf of the District Entity. The Administrator shall inform the physician that they shall not perform any of the designated duties and the District shall not provide any compensation in connection with the agreement until after the agreement and all supporting documents have been executed by both parties. Immediately after execution, the agreement shall be uploaded into Compliance 360.

PAYMENTS:

Request for physician payments will not be processed unless the supporting documentation is included with the check request/payment request. The following will be required prior to processing any physician payments. A current executed contract on file with Finance with effective and expiration date to support the services, documentation of services performed signed by the physician, i.e. time sheet, sign in sheet from meeting, medical directorship log with detailed time and services rendered,, schedule and signed log for on-call,, etc. The documentation of time and services should be carefully reviewed by the appropriate Sr. Manager in the facility to verify that the standards for completion are met. ***Payments may be delayed if the supporting documentation is not included. Manual checks for physician payments are prohibited unless there is written approval from both the District CFO (or designee) and Chief Compliance and Privacy Officer (or designee).***

COMPLIANCE OBLIGATIONS:

All physician arrangements will require the physician to abide by the Health Care District's compliance obligations. Specifically, the physician will be required to have read, understood, and abide by the Health Care District's Standards of Conduct. The parties to the physician arrangement shall comply with the Health Care District's Compliance Program and District policies and procedures related to the Stark Law and the Anti-kickback Statute. A description of the Compliance Program and link to District policies and procedures shall be provided upon request. Further, the

parties to the arrangements shall certify that they will not violate the Stark Law or Anti-kickback Statute. The physician shall complete any required compliance training.

DOCUMENT RETENTION:

All physician arrangement documents will be retained in accordance with the Districts record retention policies.

ENFORCEMENT:

All employees whose responsibilities are affected by these guidelines are expected to be familiar with the basic procedures and responsibilities created in this policy. Failure to comply with these guidelines will be subject to disciplinary action pursuant to all applicable policies and procedures up to and including termination

RELATED DOCUMENTS	
Related Policy Document(s)	
Related Forms	
Reference(s)	<p>Stark Law, 42 U.S.C. § 1395nn, and implementing regulations</p> <p>Employment exception, 42 U.S.C. § 1395nn (e) (2); 42 C.F.R. § 411.357(c). Definition of Immediate Family Member, 42 C.F.R. § 411.351.</p> <p>Anti-Kickback Statute, 42 U.S.C. § 1320a-7b (b): Employment Exception, 42 U.S.C. § 1320a-7b (b) (3) (B).</p>
Last Revision	
Revision Information/Changes	
Next Review Date	

The master document is controlled electronically. Printed copies of this document are not controlled. Document users are responsible for ensuring printed copies are valid prior to use.

Policy Name: Red Flag

Policy #:	HCDCOM146	Effective Date:	1/16/2013
Business Unit:	HCD Shared Policies	Last Review Date:	
Approval Group:	HCD Compliance Policy Board Approval	Document Owner(s):	Compliance
Board Approval Date:			

PURPOSE

This Program was developed in order to comply with the Federal Trade Commission’s Identity Theft Prevention Red Flags Rule (16 CFR § 681.2). This Program has been created in consultation with Patient Billing, Medical Records, and the Legal Department, after conducting an assessment of risk of Identity Theft associated with certain Covered Accounts (as defined in the Procedures) offered by the Health Care District and its Affiliates, including Lakeside Medical Center, Edward J. Healey, Physician Practice Offices, Primary Care Clinics, and Aeromedical services. (The “District”).

SCOPE

Any employee, contractor or agent of the District who obtains or uses patient demographic, insurance or payment information in the performance of their duties.

POLICY

It is the policy of The District to implement and maintain procedures for the prevention, detection and mitigation of identity theft, and to appropriately respond to customer address discrepancies of which it becomes aware.

EXCEPTIONS

N/A

The master document is controlled electronically. Printed copies of this document are not controlled. Document users are responsible for ensuring printed copies are valid prior to use.

Procedure Name: Red Flag

Procedure #:	HCDCOM146	Effective Date:	1/16/2013
Business Unit:	HCD Shared Policies	Last Review Date:	
Approval Group:	HCD Compliance Policy Board Approval	Document Owner(s):	

PROCEDURE

Applicability

This policy is applicable to:

- The District entities and departments that offer or maintain “covered accounts”
- The District entities and departments that use consumer reports obtained from a consumer reporting agency
- Business associates that offer or maintain covered accounts on behalf of The District
- Business associates that use consumer reports obtained from a consumer reporting agency on behalf of The District

Definitions

For purposes of the Program, the following terms are defined as:

“Creditor” means any person who regularly extends, renews or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew or continue credit. Under this definition, a third party debt collector could also be subject to the requirements it if extends, renews or continues credit. The District is a creditor to the extent it offers repayment terms to patients for the settlement of their financial obligations.

“Covered account means”: An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account or savings account; and Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to

the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation or litigation risks.

“Consumer report” means any written, oral, or other communication of any information by a consumer reporting agency (CRA) bearing on a consumer’s credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the patient’s eligibility for – credit or insurance; employment purposes; or any other purpose authorized under the Fair and Accurate Credit Transactions Act.

“Identity Theft” means a fraud committed using the identifying information of another person without authority. It also prescribes duties of users of consumer reports regarding address discrepancies;

“Identifying information” means any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any:

1. Name, social security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number.
2. Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
3. Unique electronic identification number, address or routing code; or
4. Telecommunication identifying information or access device.

“Medical Identity Theft” is a special type of identity theft used to fraudulently obtain health care items or services. Not only may victims suffer financial harm, but they may also receive improper care when incorrect information is entered into existing medical records.

“Red Flag” means a pattern, practice, or specific activity that indicates the possible existence of Identity Theft;

“Service Provider” is a person that performs an activity in connection with a covered account on behalf of the facility (e.g., collection agency, billing company, etc.).

Program Purposes

The purposes of the Program are to:

1. Identify the relevant Red Flags based on the risk factors associated with the District's covered accounts;
2. Institute policies and procedures for detecting Red Flags;
3. Identify steps the District will take to prevent and mitigate Identity Theft; and
4. Create a system for regular updates and administrative oversight to the Program.

Program Administration

The Program must be continually administered through:

1. Involvement of the governing body and senior management;
2. Periodic reports on compliance thru the Audit and Compliance Committee;
3. Staff training;
4. Oversight of service provider arrangements; and
5. Consideration of a set of guidelines and implementing those guidelines that are appropriate.

Identification of Red Flags

The Identity Theft Red Flags Mitigation and Resolution Procedures (Appendix A) identifies the Red Flags that would be most relevant to the District. The Red Flags generally fall within one of the following general types of Red Flags:

1. Suspicious Documents;
2. Suspicious Personal Identifying Information;
3. Suspicious or Unusual Use of Covered Account; and
4. Alerts from Others (e.g. customer, Identity Theft victim, or law enforcement)

Examples of potential Identity Theft indicators include, but are not limited to:

1. A complaint or question from a patient based on the patient's receipt of:
 - a. A bill for another individual;
 - b. A bill for a product or service that the patient denies receiving;
 - c. A bill from a health care provider that the patient never patronized; or
 - d. Notice of insurance benefits (or explanation of benefits) for health care services never received.
2. The demographic information (i.e., address, name, etc.) on the individual's photo identification does not match the demographic information on the proof of insurance card presented.

3. The individual presenting for services does not look like the photo ID.
4. Patient has an insurance number but never produces an insurance card or other physical evidence of insurance.
5. Patient fails to provide identifying information or documents.
6. Information in the patient's medical record is inconsistent with a physical examination or with a medical history as reported by the patient (e.g., patient's age, gender, ethnicity, etc.) Conflicting demographic information presented during registration or treatment.
7. Patient signs a different name on registration forms or signature is inconsistent with previous visits (i.e., signature illegible from previous visits versus legible currently).
8. Documents provided appear to have been altered or damaged and repaired (i.e. torn document is taped);
9. Information on the insurance card is inconsistent with the photo ID provided.
10. A patient complaint about the receipt of a collection notice from a bill collector.
11. Payment denied by insurance because it is improbable or impossible that the insured received the service. (Examples: pregnant male, spleen removed for the second time).
12. Payment denied by insurance because benefits have been depleted or a lifetime cap has been reached.
13. The patient or the patient's representative implies or admits during the process that someone else's identity is being used.
14. A notice or inquiry from an insurance fraud investigator or a law enforcement agency has been received.

Detection of Red Flags

In order to facilitate detection of the Red Flags identified in Appendix A, appropriate staff will take all necessary steps to request, obtain and verify the identity of the person.

1. New Patients/Accounts
 - a. Require identifying information (e.g., full name, date of birth, address, government-issued ID, picture identification, insurance card, etc.) and supporting documentation
 - b. When available, verify information with insurance company's information
2. Existing Accounts
 - a. Verify validity of requests for changes of contact or insurance information (i.e., billing address)
 - b. Verify identification of customers before giving out any personal information

Responding to Red Flags

If an employee detects indications of fraudulent activity that suggests Identity Theft, the District will respond to and investigate the situation, including assessing whether a violation regarding Protected Health Information (PHI) has occurred. Whenever an Identity Theft Red Flag is detected, the employee should:

1. Gather all relevant documentation and report the incident to his or her immediate supervisor and/or the District's Compliance Department;
2. The supervisor or the Compliance Department will make a determination of whether the activity is authentic or potentially fraudulent; and
3. If the activity is determined to indicate it may be fraudulent, then immediate action should be taken which may include the following:
 - a. Cancel the transaction;
 - b. Notify appropriate law enforcement;
 - c. Notify the affected patient;
 - d. Notify affected caregiver's (i.e., physician); and
 - e. Assess the impact to the patient and the organization.
4. Notify law enforcement or encourage the affected patient to file a police report if they have not already done so and complete an ID Theft Affidavit.

The Caregiver shall:

1. Review the affected patient's medical record to confirm whether entries were made to the patient's medical record that comprised inaccurate information;
2. Make a notation in the patient's medical record to indicate Identity Theft may/has occurred; and
3. If necessary, take appropriate action to correct the medical record.

Preventing and Mitigating Identity Theft

In order to prevent and mitigate the effects of Identity Theft, appropriate staff will also follow the steps identified in the attached Identity Theft Red Flags Mitigation and Resolution Procedures (Appendix A).

Service Provider Arrangements

The District will require, by contract, that service providers and business associates that perform activities in connection with Covered Accounts have policies and procedures in place designed to detect, prevent and mitigate the risk of Identity Theft with regard to the Covered Accounts.

Updating of Program

The Quality, Patient Safety and Compliance Committee will periodically review the effectiveness of the Program and update the Program as needed to reflect the addition or removal of Covered Accounts, and changes in risks to patients/covered account holders from Identity Theft.

RELATED DOCUMENTS	
Related Policy Document(s)	
Related Forms	
Reference(s)	
Last Revision	
Revision Information/Changes	
Next Review Date	

The master document is controlled electronically. Printed copies of this document are not controlled. Document users are responsible for ensuring printed copies are valid prior to use.

Honesty. Integrity. Accountability.
It's all in our hands.



Standards of Conduct



To all Employees,

The Health Care District of Palm Beach County is committed to compliance with applicable Federal and State laws, rules and regulations. In order to achieve our goal, we must earn and maintain the trust and credibility of our patients, residents, health plan members, physicians, vendors, and business associates every day. We earn our credibility by keeping our commitments, acting with honesty and integrity and remaining accountable for our actions.

The District has developed this Standards of Conduct booklet to express our commitment to and support for the values of our organization. Honesty, Integrity, and Accountability are more than just concepts at the District; they are the Standards we embrace and demonstrate in our daily work: in our relationships with our patients, residents, health plan members and business partners, and ultimately, in the quality services we provide.

These Standards codify the District's commitment to ethical and lawful conduct and are designed to guide us in upholding our high standards of fair and ethical practices. We encourage you to read these Standards thoroughly and make sure you understand them. We are all responsible for abiding by the Standards. In any case where we believe illegal or unethical conduct may have occurred, we must report it to our supervisors, senior managers, Chief Compliance Officer and Privacy Officer or through the Compliance Hotline. All reports will be taken seriously and properly investigated. Appropriate disciplinary action will be taken if it is determined that anyone has violated District policies or Federal/State laws, rules or regulations.

We must all strive to preserve and strengthen the District's reputation for excellence and integrity. This pursuit of excellence begins with our firm commitment to the organization. Thank you for your enduring commitment to the District's values. Together we will ensure that our commitments and principles continue to be reflected in every aspect of our business activities. Honesty. Integrity. Accountability. It's all in our hands.



Leslie B. Daniels
Chair, Health Care District
Board of Commissioners



Darcy J. Davis
Chair, Health Care District
Board of Commissioners



Deborah J. Hall,
CHC, CRMA, CFSA
VP & Chief Compliance
& Privacy Officer



Honesty. Integrity. Accountability.
It's all in our hands.

Standards of Conduct

November 2019



Honesty. Integrity. Accountability.
It's all in our hands.

Table of Contents

Introduction	1
Mission Statement	1
Core Values	1
Management Obligations	2
Employee Obligations	2
Purpose of the Standards of Conduct	2
Compliance Program.....	3
Quality of Care.....	3
Patient / Resident / Member Rights.....	4
Physicians.....	4
Interactions with Physicians.....	4
Non-Monetary Compensation to Physicians and Potential Referral Sources.....	5
Laws and Regulations	5
EMTALA	5
HIPAA	5
False Claims Act and Deficit Reduction Act	6
Stark Law / Anti-Kickback Statute.....	6
Antitrust Laws	6
Fraud, Waste and Abuse	7
Accreditation and Surveys.....	8
Compliance with Regulatory and Health Plan Requirements.....	8
Contract Performance Standards	8
Environmental Compliance.....	8
Business and Financial Information	9
Cost Reports.....	9
Billing and Coding for Services	9
Documentation and Record Keeping.....	9
Government Reporting	10

Time Sheet Reporting.....	10
Electronic Media	10
Financial Reporting.....	11
Intellectual Property Rights and Obligations.....	11
Workplace Conduct and Employment Practices.....	11
Conflict of Interest.....	11
Ineligible Persons	12
Hiring of Former and Current Government and Fiscal Intermediary Employees.....	12
License and Certification Renewals.....	13
Non-Retaliation	13
No Solicitation.....	13
Relationships among Employees, Patients, Residents and Members	13
Non-Discrimination	13
Harassment	14
Workplace Violence	14
Government Investigations and Search Warrants	14
Gifts and Entertainment	15
Reporting Compliance Concerns	15
Corrective Action	16
Disciplinary Action.....	16
Auditing and Monitoring.....	16
Compliance Hotline.....	16
Compliance Support.....	17
Additional Resources.....	17
Acknowledgement of Receipt and Understanding of the Standards of Conduct.....	18

Introduction

The Health Care District of Palm Beach County (“the District”) and its Affiliated entities (Lakeside Medical Center, Edward J. Healey Rehabilitation and Nursing Center, C. L. Brumback Primary Care Clinics and Dental Services, District Cares, School Health, Pharmacy, Aeromedical, and Trauma) are committed to full compliance with all applicable Federal and State health care program requirements; maintaining the highest ethical standards in the conduct of its business; and maintaining a work environment that promotes and ensures compliance with all applicable laws and regulations.

These Standards of Conduct reflect the District's mission and basic values of honesty, integrity and accountability.

Mission Statement

The mission of the Health Care District of Palm Beach County is to be the health care safety net for Palm Beach County.

We work to accomplish our mission through various programs and services, including:

- Saving lives and providing comprehensive trauma care through our integrated Trauma System
- Covering eligible, uninsured county residents who do not qualify for state or federal care with programs such as Coordinated Care and Maternity Care
- Providing medical services for adults and children through our C. L. Brumback Primary Care Clinics
- Keeping children healthy by staffing registered nurses in our public schools
- Offering skilled nursing care at the Edward J. Healey Rehabilitation and Nursing Center
- Providing acute care in underserved areas through Lakeside Medical Center on the southern shores of Lake Okeechobee

Core Values

The values of the District are demonstrated by:

- **Integrity:** Being committed to honesty, accountability, transparency and ethical standards.
- **Excellence:** Achieving high quality outcomes through innovation, customer service, safety, and continuous improvement.
- **Leadership:** Providing progressive solutions to community health care needs in a cost-effective and efficient manner.
- **Teamwork:** Fostering cooperative and collaborative efforts in the delivery of comprehensive health care services.
- **Respect:** Valuing a culture of inclusion and diversity built on trust, respect, and compassion for all.

Management Obligations

Managers of the District are expected to:

- Set the right ethical tone in work areas
- Answer questions and support employees who raise good faith concerns
- Seek guidance when clarification is needed
- Provide access to information, training and resources needed to comply with all applicable Federal and State laws, regulations and policies
- Create an environment where employees are free to report issues without fear of retaliation
- Stay abreast of any rules and regulations applicable to their department

Employee Obligations

Employees are expected to:

- Become familiar with Federal and State laws and regulations that apply to their position and the delivery and reimbursement of services provided by the District and funded by Federal Health Care programs
- Adhere to Federal and State laws governing Federal Health Care Programs
- Seek guidance from either a supervisor, senior manager or the Chief Compliance Officer if questions arise
- Present no claim for payment or approval that is inaccurate, false, fictitious or fraudulent
- Report activity of any District employee, vendor, physician, contractor, etc. which you believe may violate Federal or State laws, rules, regulations, or the Standards of Conduct to the Chief Compliance and Privacy Officer
- Make no false or misleading reports
- Cooperate with training and investigation efforts

Purpose of the Standards of Conduct

Our Standards of Conduct provide guidance to all workforce members including, board and committee members, employees, vendors and contractors of the Health Care District of Palm Beach County. These standards apply to our relationships with patients, physicians, payers, subcontractors, independent contractors, vendors, consultants and our employees.

The Standards of Conduct establish the general policies and procedures all employees must follow as a condition of employment. In health care, with its many complexities, the Chief Compliance and Privacy Officer may need to provide further guidance and direction to those directly involved in a particular area.

Compliance Program

The District is committed to maintaining an organizational and accountability structure to assure compliance with governmental laws, rules and regulations, organizational policy and procedures. The Compliance Program supports the District's ethical standards, Standards of Conduct and a zero tolerance for fraud, waste and abuse.

The Compliance Program demonstrates the commitment of the District and the Board of Commissioners to meet the highest standards of compliance. The overall accountability for the District's Compliance Program rests with the Board of Commissioners.

The Chief Compliance and Privacy Officer serves as the focal point for compliance activities within the District and reports directly to the Quality, Patient Safety & Compliance Committee of the Board of Commissioners. The Chief Compliance Officer has direct access to the Chief Executive Officer and Board of Commissioners.

Quality of Care

Our goal is to provide high quality, cost-effective health care to all of our patients. To that end, we are committed to the delivery of safe, effective, efficient, compassionate and satisfying patient care. Every workforce member must at all times remain committed to the District's obligations to promote the delivery of high quality care to patients, residents and health plan members. The mission of the District is to be the health care safety net for Palm Beach County and our vision is meeting changes in health care to keep our community healthy. We shall uphold sound standards of professional practice in all District facilities and programs.

The District maintains a comprehensive program to promote the quality objectives of the organization. In promoting high quality care, District facilities are focused on the attentiveness and dedication of service to patients; the utilization of evolving technology to ensure quality and patient safety; and creating an overall culture that makes patient safety paramount. As a general principle, the District aspires to a standard of excellence for all caregivers within its facilities, including the entire facility team, which is committed to the delivery of safe, effective, efficient, compassionate and satisfying care and services. We shall treat our patients, residents and members with respect and dignity and provide care that is both necessary and appropriate. We make no distinction in the availability of services; the admission, transfer or discharge of patients; or in the care we provide based on age, gender, disability, race, color, religion or national origin or any other characteristic protected by law.

There are increasingly numerous measures that relate in some way to the quality of patient care. These include, for example, the Conditions of Participation of the Centers for Medicare and Medicaid Services (CMS) and the standards and surveys of The Joint Commission, the Florida Agency for Health Care Administration (AHCA), and the U. S. Department of Health and Human Services Health Resources and Services Administration (HRSA). The District is attentive to all of these standards and seeks to establish systems that reflect the best practices required or intended by these various standard-setting efforts.

This commitment to quality of care and patient safety is an obligation of every District workforce member. Accordingly, it is a fundamental principle of being part of the District that each person dedicates himself or herself to achieving the goals described here. In addition, in any circumstance where a District workforce member has a question about whether the quality or patient safety commitments set forth herein are being fully met, that individual is obligated to raise this concern through appropriate channels until it is satisfactorily addressed and resolved. Such channels include those established at the facility and

beyond, including the Compliance Hotline. In addition to the facility and District channels, the District workforce is provided resources and guidance as to how to solicit intervention or review by external quality partners including the Joint Commission, state survey agencies or state quality improvement organizations.

Patient / Resident / Member Rights

We make no distinction in the availability of services; the admission, transfer, or discharge of patients; or in the care we provide based on age, gender, disability, race, color, religion, sex, sexual orientation, gender identity, or national origin. We recognize and respect the diverse backgrounds and cultures of our patients and make every effort to equip our caregivers with the knowledge and resources to respect each patient's cultural needs.

Each patient, resident and health plan member has access to a written statement of his or her rights along with a Notice of Privacy Practices. These statements include their rights to:

- Make decisions regarding their medical care
- Refuse or accept treatment
- Make informed decisions
- Maintain their health information

Physicians

Interactions with Physicians

There are both Federal and State laws and regulations which govern the relationship between health care providers and physicians who refer patients to their facilities. The applicable laws and regulations include, but are not limited to, the Stark Law and the Anti-Kickback Statute. It is important that employees who interact with physicians, particularly those responsible for making payments to physicians for services rendered, providing space or services to physicians, recruiting physicians to the community, and arranging for physicians to serve in leadership positions are aware of the requirements of the laws, regulations and policies that address these relationships.

Relationships must be appropriately structured, and diligently administered to ensure that any and all arrangements comply with the law. An arrangement with a physician must be structured to ensure compliance with legal requirements, our policies and procedures, and with any operational guidance that has been issued. Arrangements must be in writing, approved by Legal Counsel and reviewed by the Compliance Department. Failure to meet all requirements of these laws and regulations can result in serious consequences for the organization. It is important to remember the following:

- We do not accept payments for referrals we make. No District employee or anyone acting on behalf of the organization is permitted to solicit or receive anything of value, directly or indirectly, in exchange for the referrals of patients. Similarly, when making patient referrals to another health care provider, we do not take into account the volume or value of referrals that the provider has made (or may make to us).
- We do not pay for referrals. We accept patient referrals and admissions based solely on the patient's medical needs and our ability to render the needed services. We do not pay or offer to pay anyone, be it employees, physicians, or other persons or entities for patient referrals.

Non-Monetary Compensation to Physicians and Potential Referral Sources

Any entertainment, gift or token of appreciation involving physicians or other persons who are in a position to refer patients to the District or any of its affiliated entities can only be offered or accepted in accordance with District compliance policies which have been developed consistent with Federal laws, regulations, and rules regarding these practices. Employees must consult our policies and procedures prior to offering or accepting any business courtesy or token of appreciation to or from a potential referral source. See also “*Business Courtesies to Physicians and Immediate Family Members Procedure*” on the Compliance page on SharePoint.

Laws and Regulations

EMTALA

At Lakeside Medical Center ("the Hospital"), we follow the Emergency Medical Treatment and Active Labor Act (EMTALA) in providing an emergency screening examination and/or necessary stabilization to all patients, regardless of ability to pay. Provided we have the capacity and capability, any person presenting with an emergency medical condition including active labor will receive medical screening and necessary stabilizing treatment without delay to seek financial and demographic information. We do not admit, discharge or transfer patients with emergency medical conditions simply based on their ability or inability to pay or any other discriminatory factor.

Patients with emergent medical conditions are only transferred to another facility at the patient's request or if the patient's medical needs cannot be met at the Hospital and appropriate care is knowingly available at another facility. Patients are only transferred in strict compliance with State and Federal EMTALA regulatory and statutory requirements.

HIPAA

We collect information about a patient's medical condition, history, medication and family illness to provide quality care. The Health Insurance Portability and Accountability Act (HIPAA) of 1996, also known as the Privacy Rule, provides Federal protection of personally identifiable health information held by covered entities and gives patients an array of rights with respect to that information. In following the HIPAA privacy regulations, we do not use, disclose or discuss patient-specific information with others unless it is necessary to serve the patient, resident and health plan member or is required by law. District employees should never use or disclose confidential information that violates the privacy rights of patients, residents or health plan members. Should you have additional questions, contact the District's Chief Compliance and Privacy Officer at 561-659-1270 ext. 295524.

False Claims Act and Deficit Reduction Act

The Federal False Claims Act (FCA) and Deficit Reduction Act protect government programs including Medicare, Medicaid and TRICARE from fraud and abuse. The government enacted the FCA to prohibit knowingly submitting false or fraudulent claims to Federally-funded government programs including Medicare. In addition, the Florida False Claims Act prohibits persons from knowingly causing or assisting in causing the State government to pay claims that are false or fraudulent. It provides remedies including civil monetary penalties and treble damages when money is obtained from the State government by reason of a false or fraudulent claim. The District complies with these laws and maintains policies to detect, report and prevent waste, fraud and abuse. The District encourages its employees, vendors, and contractors to report suspected improper conduct and provides protection for whistleblowers.

Stark Law / Anti-Kickback Statute

All business arrangements with a physician or family member (extends beyond immediate family members) of a physician must be in writing and compliant with all applicable laws, rules, regulations and District policies. All of these arrangements must be reviewed and approved in advance by the Compliance and Legal Departments.

The District does not offer or pay for referrals. We accept patient referrals and admissions based solely on the patient's medical needs and our ability to render the needed service(s). We do not pay or offer to pay anyone; e.g., physicians or other persons or entities for referring patients.

We also do not solicit or accept payments for referrals we make. No District employee or person acting on behalf of the District is permitted to solicit or receive anything of value, directly or indirectly, in cash or in kind, in exchange for the referral of patients. Also, when making patient referrals, no employee or person acting on behalf of the District is allowed to receive any payment in cash or in kind, directly or indirectly, for the patient referral.

Antitrust Laws

Antitrust laws are designed to create a level playing field in the marketplace and to promote fair competition. These laws could be violated by discussing the District's business with a competitor, such as how prices are set, or disclosing the terms of vendor relationships. Employees need to be mindful, particularly at outside meetings, not to participate in discussions regarding prohibited subjects such as pricing, labor costs, etc. Contact the Compliance Department for further information.

The District will comply with all applicable laws and regulations, including Florida Statutes, Chapter 112, that ensures that public officials and employees: conduct themselves independently and impartially; not use their offices or positions for private gain other than remuneration provided by law; and to avoid conflicts between public duties and private interests.

No District employee:

- Shall solicit or accept anything of value - including a gift, loan, and reward, promise of future employment, favor, or service - that is based on any understanding that the vote, official action or judgment of the employee would be influenced by such gift. Sec.112.313(2), Florida Statutes.
- Acting as purchasing agent or acting in his/her official capacity shall, directly or indirectly, purchase, rent, or lease any realty, goods or services for the District from a business entity in which the employee, his/her spouse, or child is an officer, partner, director or proprietor, or in which the

employee, his/her spouse, or child (or any combination of them) has a material interest. Nor shall a public employee, acting in a private capacity, rent, lease, or sell any realty, goods or services to his/her own agency. Sec. 112.313(3), Florida Statutes.

- Or his/her spouse or minor child shall accept any compensation, payment, or thing of value which, with the exercise of reasonable care, is known or should be known to influence the official action of such employee. Sec. 112.313(4), Florida Statutes.
- Shall corruptly use or attempt to use his/her official position or any property or resource within his/her trust, or perform his/her official duties, to obtain a special privilege, benefit or exemption for himself/herself or others. Sec. 112.313(6), Florida Statutes.
- Shall disclose or use information not available to the general public and gained by reason of his/her public position for his/her personal gain or benefit or the gain or benefit of others. Sec. 112.313(8), Florida Statutes.

Fraud, Waste and Abuse

We have an obligation under the law to conform to the requirements of the Medicare, Medicaid and other governmental programs (“Programs”). Fraud, waste and abuse committed against these Programs will not be tolerated by the District and may be prosecuted under various provisions of the United States Criminal Code, which could result in the imposition of restitution, fines, and in some instances, imprisonment. In addition, there is also a range of administrative sanctions (such as exclusion from participation in Medicare, Medicaid and other government programs) and civil monetary penalties that may be imposed.

While not an exhaustive list, the following are examples of fraud, waste, or abuse:

- Forging or changing patient-billing related items, such as making false claims, or billing for services or supplies not rendered, not medically necessary, or not documented
- Misrepresenting or otherwise falsifying a diagnosis or procedure code in order to obtain payment or payment at a higher rate of reimbursement permitted for the actual diagnosis or service provided
- Alteration or forgery of checks
- Any misuse or theft of funds
- Any irregularity in the handling or reporting of financial transactions
- Any irregularities of giving or receiving payment in connection with business transactions and the giving or obtaining of contracts
- Falsifying or altering any record or report, such as an employment application, payroll or time record, expense account, medical record or patient record
- Falsely reporting costs

The District is committed to conducting routine audits, monitoring and reviews along with implementing a system of internal controls to prevent and detect fraud, waste and abuse. Please do not ignore these types of activities. If you know or suspect activity of this nature, report it immediately. If you are uncertain if any activity is fraudulent, abusive or wasteful, contact the Chief Compliance and Privacy Officer for guidance.

Accreditation and Surveys

In preparation, during or after surveys, District employees are expected to deal with all accrediting agencies, such as The Joint Commission, HRSA, and Accreditation Association for Ambulatory Health Care, in a direct, open and honest manner. When government agencies and other accrediting bodies conduct surveys, we must respond with openness and accurate information. In preparation for or during surveys and inspections, employees must never conceal, destroy, or alter documents, lie or make misleading statements to agency representatives. Employees must never attempt to cause another employee to fail to provide accurate information or obstruct, mislead or delay the communication of information or records relating to a possible violation of any applicable law or regulation.

Compliance with Regulatory and Health Plan Requirements

The District will comply with all Federal, State and local laws and regulations that apply to our business, as well as the terms of all contracts with Federal or State agencies covering our health plans. We will not pursue any business initiative or opportunity that requires us to act illegally or in violation of our contractual obligations.

Employees are expected to know the basic laws, regulations and contract requirements that apply to his or her job. Employees are also expected to know and follow District policies and procedures and compliance-related processes and systems. Suspected violations of health plan contracts or District policy must be promptly reported to a supervisor, senior manager or the Chief Compliance Officer.

Contract Performance Standards

The District's health plan contracts include a number of specific performance standards related to network adequacy, permissible forms of marketing activities, quality of care, and responsiveness to member rights including enrollee concerns or complaints. Meeting these standards is consistent with the District's commitment to integrity and responsiveness to addressing the health needs of health plan populations and failure to do so may subject the District to financial or other penalties. The District has developed a system of internal controls to promote and monitor compliance with these standards.

Environmental Compliance

The District is committed to providing a safe and secure environment for patients, residents, family members, employees, providers, visitors and customers. We comply with established safety and infection control laws and regulations, which are intended to prevent job-related hazards. We are consistent with ergonomic standards and maintain a safe work environment.

We are respectful of the environment and conserve natural resources. We exercise our policies and procedures with regard to the environment and use District buildings, property, laboratory processes and medical products in accordance with Federal, State and accreditation standards. We comply with permit requirements that allow for the safe discharge of pollutants into the air, sewage systems, water or land.

We comply with all laws and regulations governing the handling, storage, use and disposal of hazardous materials, other pollutants and infectious wastes.

Business and Financial Information

Cost Reports

The District is required by Federal and State laws and regulations to submit reports regarding our operating costs and statistics. We will comply with all laws and regulations relating to all cost reports including the methodologies to claim reimbursement for the cost of services provided to Federal Program beneficiaries. All issues related to the preparation, submission and settlement of cost reports must be performed or coordinated with the District's Finance Department.

Billing and Coding for Services

The District maintains comprehensive policies and systems to facilitate accurate billing to government payers, commercial insurers and patients. These policies conform to pertinent Federal and State laws and regulations. All District employees and contractors are prohibited from knowingly causing or submitting false or misleading claims for approval or payment. All medical records that support billings must be accurate and timely.

Documentation and Record Keeping

All records and documents created by District employees should be honestly and accurately prepared. Examples include medical records (e.g., X-rays, provider notes, lab results, etc.), financial records, e-mails, hard copy correspondence, reports and presentations. The following rules apply to all types of documentation:

- We never falsify facts or knowingly create false or misleading records
- We do not sign someone else's name to any document
- We never document as someone else
- We strive to only create records that are necessary and required to perform our duties
- We only give records and information to people who have a legal "need to know" or right to review
- We always secure documents and records, preserve patient confidentiality and respect our patients' privacy rights

All employees must follow the District's policy on retention of records. Each of us is responsible for the integrity and accuracy of documents and records. Records must never be destroyed in an effort to hide or deny access to anyone with a legal right to view the record such as a patient, governmental authority, payor or legal representative.

The District has established policies and procedures regarding the storage and destruction of records. All records shall be kept for the legally required minimum timeframe. Once that timeframe has expired, records will be destroyed in a timely and appropriate manner. For more details regarding the retention periods and the destruction procedures of records, consult the Records Department at 561-659-1270 ext. 295781.

Government Reporting

All required filings and reports to Federal, State, and local government authorities must be made accurately and in a timely manner. False statements contained in a government filing or report could subject the District, and the responsible individual(s) to civil and/or criminal penalties. Employees responsible for creating or accumulating information for a report or filing that is submitted to a more senior manager for approval or signature are accountable for ensuring the accuracy of the information provided. They are also responsible for affirmatively disclosing any problems or concerns with the process or content of the report before it is submitted. Documentation and work papers used to prepare or support information contained in a government report or filing must be retained in accordance with District record retention policies.

Time Sheet Reporting

Employees who submit time reports must do so in a complete, accurate and timely manner. Employees must also ensure that hours worked and costs incurred are applied to the appropriate account for which the effort was required. The signature (manual or electronic) on a time report is a representation that the time accurately reflects the number of hours worked. The supervisor's signature on a time report or expense report is a representation that appropriate steps have been taken to verify the validity of the hours or expenses recorded. Omission or falsification of time records is grounds for dismissal.

Electronic Media

All communication systems, including but not limited to computers, electronic mail, Intranet/ Internet records / access, telephones and voice mail, are the property of the organization to be used primarily for business purposes in accordance with the District's electronic communications policies and standards. Users of computer and telephonic systems should presume no expectation of privacy in anything they create, store, send or receive on District computer and telephone systems. The District reserves the right to monitor and/or access communication usage and content consistent with established District policies and procedures.

Employees may not use internal communication channels or access to the internet at work to post, store, transmit, download or distribute any threatening materials: knowingly, recklessly, or maliciously false materials; obscene materials; or anything constituting or encouraging a criminal offense, giving rise to civil liability or otherwise violating any laws. In addition, these channels of communication may not be used to send chain letters, personal broadcast messages or copyrighted documents that are not authorized for reproduction; nor are they to be used to conduct a job search or any other use that would violate District Equal Employment Opportunity policies. Employees who abuse our communication systems' policies or use these systems excessively for non-business purposes, may lose these privileges and be subject to disciplinary action in accordance with Human Resources' policies and procedures.

Employees must comply with the District's security policies governing the use of information systems. Only assigned user IDs and strong passwords shall be used. Employees will be required to periodically change their passwords according to District policy. Passwords must never be shared with or disclosed to anyone. The use of tools or techniques to break or exploit District information security measures is strictly prohibited. District information systems shall not be used to access inappropriate or prohibited websites.

Great care should be taken when any employee receives an attachment or communication from an unknown or untrusted source to employ appropriate measures to prevent the spread of a virus or any other type of “cyber” attack that may compromise the integrity of electronic systems or data.

Financial Reporting

All financial information must reflect actual transactions and conform to Generally Accepted Accounting Principles. All funds or assets must be properly recorded in the books and records of the District. The District maintains a system of internal accounting controls to provide reasonable assurances that all transactions are executed in accordance with senior management’s authorization and are recorded in a proper manner so as to maintain accountability of the organization’s assets.

Intellectual Property Rights and Obligations

Any work product authored, invented, or otherwise developed including any patent, trademark, copyright or trade secret by an employee during the scope of his or her employment with the District shall be considered the intellectual property of the District. The following factors will be considered in determining whether something is created during employment:

- The nature of the employee’s work
- Whether the intellectual property developed is related to the District’s business
- Whether the employee was directed to produce the intellectual property as part of his or her work duties
- Whether the employee utilized the District’s property or resources to develop the intellectual property and
- Whether the employee created the intellectual property while being paid by the District

If any work product created is eligible for copyright, it will be considered “Work for Hire” under the United States Copyright Act, with the District identified as the author and owner of such work.

Workplace Conduct and Employment Practices

Conflict of Interest

Every employee who is in a position of influence or has control over the affairs, decisions or assets of the District, has an explicit duty to protect the interest of the Health Care District when entering into any transaction or arrangement that may potentially benefit the private interest of that employee or a related party. A conflict of interest occurs when a person is in a position to derive personal benefit from actions or decisions made in their official capacity as an employee of the District. A conflict may exist even if the situation is not resolved in the favor of the employee or a related party, such as a family member. Further, the appearance of a conflict may be just as damaging to the employee and/or the District as an actual conflict.

The District recognizes the right of employees to engage in activities outside of their District employment. These activities are a concern to the District when they conflict with the employee’s official duties and responsibilities at the District. A conflict of interest may occur if outside activities or personal interests influence or appear to influence the ability to make objective decisions in fulfilling the employee’s job responsibilities.

A conflict of interest may also exist if the demands of any outside activities hinder or distract an employee from his or her job performance or cause the use of District resources for non-District purposes. Any questions an employee has as to whether an outside activity might be or appear to be a conflict of interest should be directed to his or her supervisor, Human Resources or the Chief Compliance Officer. A policy of full disclosure must be followed to assess and prevent potential conflicts of interest from arising.

The Health Care District will not allow employees to engage in secondary employment where a conflict of interest exists. Upon hire and annually thereafter, all employees will complete a Conflict of Interest Statement. If during the year a conflict or potential conflict of interest occurs, the employee should discuss it with his or her supervisor and complete an updated Conflict of Interest Statement. The Chief Compliance and Privacy Officer shall review all Conflict of Interest Statements annually and make recommendations regarding mitigation.

Examples of Conflict of Interest:

- An employee or family member owns a company or service that does or wants to do business with the District
- Outside employment or activities which use the equipment, personnel or other resources of the District
- Acceptance of gifts, payments (in cash or in kind) or services from those seeking to do business with the District
- Outside activities (consulting, employment, management or other contractual relationships) with a person or entity, or financial interests in an entity, that does business with or competes with the District, particularly when the employee may influence a District decision involving that business
- If an employee's spouse or other family member is engaged in a business similar in nature to the District or under contract with the District, or employed by an organization under contract with the District

Ineligible Persons

It is the policy of the District not to contract with, employ or bill for services rendered by an individual or entity that is excluded or ineligible to participate in Federal health care programs; suspended or debarred from Federal government contracts; or has been convicted of a criminal offense related to the provision of health care items or services. These individuals, companies or groups are not eligible to do business with or be employed by the District.

The District verifies that individuals and entities employed by or doing business with the District are not excluded by the Office of the Inspector General (OIG) or General Service Administration (GSA). These checks are performed upon hiring or contracting and monthly thereafter.

Hiring of Former and Current Government and Fiscal Intermediary Employees

The recruitment and/or employment of former or current U.S. government employees may be impacted by regulations concerning conflicts of interest. Hiring employees directly from a fiscal intermediary requires certain regulatory notifications. Employees should consult with the Compliance, Legal and Human Resources Departments regarding such recruitment and hiring.

License and Certification Renewals

Employees and other individuals in positions that require professional licenses, certifications, or other credentials are responsible for the ongoing maintenance of their credentials and shall comply at all times with Federal and State requirements applicable to their respective disciplines. Additionally, if an employee becomes aware of someone whose license has been restricted or suspended in any manner, he or she has a duty to report that restriction or suspension to their supervisor, Human Resources or the Chief Compliance and Privacy Officer. To ensure compliance, the District may require evidence of the individual's current license or active credentials. The District will not allow any employee, independent contractor or privileged practitioner to work without a valid license or credentials required for their position.

Non-Retaliation

The Health Care District is committed to protecting employees from retaliation or reprisal when they report allegations in "good faith" of a violation of law or regulation, unethical behavior or other prohibited act that has or may occur. Good faith reporting involves a truthful and honest intent to act without taking an unfair advantage over another person. In other words, you believe that what you are reporting is true and correct to the best of your knowledge. Any employee who believes that he or she is being retaliated against by a superior or peer for making a good faith report should immediately notify the Chief Compliance and Privacy Officer and/or a Human Resources representative. If you have any questions regarding retaliation, contact the Compliance Department or refer to the "*Non-Retaliation Policy*" on the Compliance page on SharePoint. Anyone who intentionally makes a false report may be subject to disciplinary action.

No Solicitation

It is District policy to limit the solicitation and distribution of literature to employees during working hours and in working areas by all persons and organizations. This policy applies to employees and non-employees while on any District premises. No employee should ever be compelled or made to feel compelled to participate in a District or District business unit fundraising endeavor to support charitable organizations such as the United Way. Parties with a legitimate contractual agreement with the District may be allowed to provide information where appropriate, for the purpose of delivery of health care, efficient business practices or to provide professional development. Such persons shall not engage in sales solicitation directed at employees, patients or visitors.

Relationships Among Employees, Patients, Residents and Members

Employees must remember to keep relationships professional at all times with other employees, patients in the hospital, residents at the Edward J. Healey Rehabilitation and Nursing Center or members of our programs. We are prohibited from purchasing gifts for our patients, residents and members as well as accepting gifts from them. If ever in doubt about a relationship, employees should consult with their supervisor, Human Resources or the Chief Compliance and Privacy Officer. Refer to the "*Gift Policy*" on the Compliance page on SharePoint for more information on the subject.

Non-Discrimination

Our employees have the right to work in an environment free from discrimination. The Health Care District does not discriminate against any person regardless of race, color, national origin, disability, age, sex (including pregnancy and sex stereotyping), sexual orientation, gender identity and/or expression, religion, or creed, and/or any other legally protected classification. This applies to excluding or denying benefits,

admission to, participation in, or receipt of the services and benefits under any of its programs and activities (operated directly by the District or through an approved contractor), and in staff and employee assignments. Any employees with knowledge or reasonable suspicions of discrimination should report their observations to Human Resources. If you have any questions regarding discrimination, contact the Compliance Department or refer to the “*Non-Discrimination Policy*” on the Compliance page on SharePoint for more information.

Harassment

Each employee of the Health Care District and its Affiliates, District Clinic Holdings, dba C. L. Brumback Clinics and District Hospital Holdings dba Lakeside Medical Center has the right to work in an environment free of harassment and disruptive behavior, including behaviors that undermine a culture of safety. Harassment includes degrading or humiliating jokes, slurs, intimidation or any conduct that creates a hostile work environment. Sexual harassment is also prohibited, including unwanted sexual advances and verbal or physical contact of a sexual nature that creates an intimidating, hostile or offensive work environment.

Workplace Violence

Workplace violence is any act or threat of physical violence, menacing, intimidation or other threatening or disruptive behavior that occurs at or off the worksite and adversely impacts work-related activities. It may be intentional or unintentional and it may affect and involve employees, clients, residents, patients, physicians, contractors, suppliers and visitors. If you observe or experience any form of workplace violence, you should report the incident to your supervisor, the Human Resource Department, a member of management, the Facility Administrator, or the Compliance Department.

Government Investigations and Search Warrants

The District will cooperate fully with government investigations and other requests for information. If a government investigator contacts you regarding your work, or affiliation and/or knowledge of the District, do not feel pressured to talk to the investigator without first contacting the District’s Legal Counsel and the Chief Compliance and Privacy Officer. As an employee, you have the right to:

- Speak with the investigator or decline to speak to the investigator
- Request that the interview take place at a time and place that is convenient to you
- Have Legal Counsel present
- Terminate the interview at any time
- Refuse to answer any questions

If you do speak with the investigator, the District expects you to be truthful and to avoid speculation on your part in your responses. It is important to remember that interviews with government investigators may have a substantial legal effect that may impact your legal rights and those of the District. You should always be polite and request the following:

- The business cards of all investigators or to view their photo identification
- The reason for their visit
- Ask whether there is a subpoena or warrant for any requested documents or records

If you are presented with a subpoena, search warrant or court order, it is expected that you immediately notify your supervisor, Legal Counsel and the Compliance Department. District employees are expected to respond with openness and accurate information. Employees must never conceal, destroy or alter any documents.

Gifts and Entertainment

Our services and business relationships are intended to promote the best interests of the District and its patients, residents and health plan members. We cannot offer or accept anything of value in exchange for referrals or business. Employees are prohibited from accepting gifts, payments, fees for services, discounts, valuable privileges or other favors, which would or might appear to influence them in the performance of their official duties. Gifts must never be offered, given to, solicited or received from a referral source with the intent of inducing referrals or in a manner that could give the appearance of intending to induce referrals. A referral source is defined as an entity or individual that does or might in the future direct patients or other medically-related activities to the District.

These restrictions also apply any time we are in active negotiations or in a Request for Qualifications/Request for Proposal (RFQ/RFP) process with a potential vendor.

Whenever a gift is offered that is not allowed by policy, the gift should be graciously refused or returned to the donor, and reported to the Chief Compliance and Privacy Officer. If after explaining our gift policy, the donor refuses to take the gift back, or would be offended by your refusal, you should contact the Compliance Department immediately for further direction.

A gift is any item of value, including, but not limited to, marketing items (such as t-shirts, food, flowers, etc.) if the recipient is not expected to pay for the item. Cash, gift cards, traveler's checks, money orders, honorariums or other cash equivalents received from patients, vendors, customers, physicians, or government officials are strictly prohibited. Perishable items (such as food, popcorn, etc.) may be accepted during special occasions (e.g., holiday season) as long as they are of reasonable value (not extravagant), appropriate for the occasion and shared among the entire department staff.

Reporting Compliance Concerns

Employees are expected to report any suspected or known violations of law, regulation and District policies including those described in the Standards of Conduct and other supporting policies and procedures. Examples include, but are not limited to, incidents of fraud, waste or abuse, harassment, etc. Issues or incidents can be reported to your supervisor, Human Resources, the Chief Compliance and Privacy Officer or the Compliance Hotline. Remember the District is committed to protecting employees from retaliation or reprisal for making a "good faith" report. It is also important to: provide as much relevant information as possible regarding the issue or incident reported; cooperate with any compliance investigation; and only disclose information to those who have a need to know. Indiscriminately disclosing information regarding confidential compliance investigations may inhibit or corrupt the investigation, and as a result, may subject you to disciplinary action up to and including termination. For additional information on reporting compliance concerns, refer to "Internal Reporting of Potential Compliance Issues Policy" on the Compliance page on SharePoint.

Corrective Action

When an internal investigation determines a violation occurred, the Compliance Department will initiate appropriate corrective action. Possible corrective actions include, but are not limited to, refunds of any overpayment(s) received, employee disciplinary action up to and including termination and reporting the incident to the appropriate Federal or State authorities.

Disciplinary Action

Failure to comply with the Standards of Conduct, District policies and procedures or any applicable laws and/or regulations may result in disciplinary action up to and including termination of employment and/or criminal or civil sanctions including fines, imprisonment and exclusion from participation in government programs. Violations of laws and/or regulations may also result in the imposition of penalties on the District up to and including exclusion from contracting with Federal and State agencies. Similar corrective actions may be applied in those instances in which an individual and/or the District fail to report suspected or identified noncompliance.

Auditing and Monitoring

The District is committed to the aggressive monitoring of compliance with its policies and applicable laws and regulations. In addition to its ongoing monitoring efforts, the District will ensure that compliance audits are conducted of areas and activities with the greatest risk identified by a formal risk assessment and or investigation. These audits may be scheduled or unannounced and may be expanded based in the initial findings.

Compliance Hotline 1-866-633-7233

The Compliance Hotline is managed by an independent third party. All callers have the option of remaining anonymous and are issued a report number so they can follow up on actions taken. The Compliance Hotline operators do not have caller identification and are unable to trace calls. When a call is made, the caller is encouraged to provide enough details to investigate the caller's concerns, including the business unit and department. A caller's anonymity will be protected to the full extent allowed by law. Information regarding each call will be forwarded to the Compliance department in order to facilitate investigation and corrective action.

All reports should be made in good faith. There will be no retaliation for expressing concerns or passing along information about situations that seem questionable to you as long as they are made in good faith.

Compliance Support

The Health Care District's Compliance Program promotes open identification, discussion, reporting and resolution of compliance issues without fear of retaliation. The Health Care District's Compliance Department is led by the Chief Compliance and Privacy Officer.

For more information on the District's Compliance Program and policies, visit SharePoint.

Issues can be reported several ways - by email (visit the Compliance Department site on SharePoint), phone, fax, mail, interoffice mail, or in person: Health Care District of Palm Beach County Compliance Department:

1515 N. Flagler Drive, Suite 101
West Palm Beach, FL 33401-3429
Attn.: Chief Compliance and Privacy Officer
Phone: 561-804-5786

Additional Resources

Compliance Hotline	1-866-633-7233
HIPAA Privacy	Phone: 561-804-5600 ext. 295893 or ext. 295617 Privacy@hcdpbc.org
Human Resources	561-804-5982
Legal Department	561-804-5955

Acknowledgement of Receipt and Understanding of the Standards of Conduct

I acknowledge that I have received and reviewed these Standards of Conduct. I agree to comply with the Standards of Conduct and all related policies and procedures. I also acknowledge that the Standards of Conduct are only a statement of principles of individual and business conduct, and do not constitute an employment contract.

I will promptly report any identified or potential violation of which I become aware to my supervisor, Human Resources, the Chief Compliance and Privacy Officer or another member of the Compliance Department. I understand that any violation of the Standards of Conduct or any Compliance Policy or Procedure is grounds for disciplinary action, up to and including termination. Because the information and policies described in the standards, policies and procedures are subject to change as needed, I acknowledge that revisions to the policies and procedures may occur without prior notice. Any such changes will be communicated as soon as possible after the change is instituted. I also understand that the revised information may supersede, modify or eliminate existing policies.

Signature: _____

Print Name: _____

Date: _____

Department: _____

- Location: Health Care District (West Palm Beach)
- Edward J. Healey Rehabilitation and Nursing Center
- Lakeside Medical Center
- C. L. Brumback Primary Care Clinics and Dental Services
- Trauma Hawk Aeromedical Hangar Facility
- School Health Program
- Other (specify):



Published by the Compliance Department
Health Care District of Palm Beach County
1515 N. Flagler Drive, Suite 101
West Palm Beach, FL 33401-3429
561-804-5600



DISTRICT CLINIC HOLDINGS, INC.
BOARD OF DIRECTORS
December 11, 2019

1. Description: IT Policies Adoption

2. Summary:

Clinic Administration would like to retire the Clinic IT Policies from 2013 and instead adopt the Health Care District of Palm Beach County IT Policies.

3. Substantive Analysis:

Attached you will find the policies staff are recommending be retired:

- 400-13 Access Control
- 401-13 Contingency Plan
- 402-13 Device and Media Control
- 403-13 Facility Security
- 404-13 Information Access Management
- 405-13 Password Protection
- 406-13 Person or Entity Authentication
- 407-13 Risk Analysis and Management
- 408-13 Termination or Transfer Employee
- 409-13 Transmission Security
- 410-13 Workforce Clearance
- 411-13 Workstation Security
- 412-13 Workstation Use

Attached you will also find the policies staff are recommending be adopted:

- Acceptable Use
- Backups
- Change Control
- Email
- Encryption
- Guest Access
- Incident Reporting
- Information Security Governance
- Instant Messaging
- Network Access and Authentication
- Network Security
- Passwords
- Physical Security
- Remote Access
- Removable Media
- Security Awareness Program
- Termination and Transfer
- Third Party Connection

DISTRICT CLINIC HOLDINGS, INC.
BOARD OF DIRECTORS
December 11, 2019

Two-Factor Authentication
 User Access Review
 VPN
 Wireless Access

4. Fiscal Analysis & Economic Impact Statement:

	Amount	Budget
Capital Requirements	N/A	Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>
Annual Net Revenue	N/A	Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>
Annual Expenditures	N/A	Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>

Reviewed for financial accuracy and compliance with purchasing procedure:

N/A

 Joel Snook
 VP & Chief Financial Officer

5. Reviewed/Approved by Committee:

N/A

 Committee Name

 Date Approved

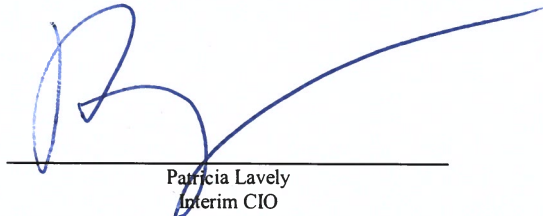
6. Recommendation:

Staff recommends the Board approve the retirement of Clinic IT Policies and the adoption of the Health Care District IT Policies.

Approved for Legal sufficiency:



 Valerie Shahriari
 VP & General Counsel



 Patricia Lavelly
 Interim CIO



 Dr. Belma Andric
 Chief Medical Officer, VP & Executive Director
 of Clinic Services

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Acceptable Use**

Effective Date: January 14, 2015

Department: **Information Technology**

Policy Number: N/A

POLICY

The Health Care District of Palm Beach County is hereinafter referred to as "the company."

Though there are a number of reasons to provide a user network access, by far the most common is granting access to employees for performance of their job functions. This access carries certain responsibilities and obligations as to what constitutes acceptable use of the corporate network. This policy explains how corporate information technology resources are to be used and specifies what actions are prohibited. While this policy is as complete as possible, no policy can cover every situation, and thus the user is asked additionally to use common sense when using company resources. Questions on what constitutes acceptable use should be directed to the user's supervisor.

Since inappropriate use of corporate systems exposes the company to risk, it is important to specify exactly what is permitted and what is prohibited. The purpose of this policy is to detail the acceptable use of corporate information technology resources for the protection of all parties involved.

APPLICABILITY

The scope of this policy includes any and all use of corporate IT resources, including but not limited to, computer systems, email, the network, and the corporate Internet connection.

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Acceptable Use**

Effective Date: January 14, 2015

Department: **Information Technology**

Policy Number: N/A

DEFINITIONS

Blogging - The process of writing or updating a "blog," which is an online, user-created journal (short for "web log").

Instant Messaging - A text-based computer application that allows two or more Internet-connected users to "chat" in real time.

Peer-to-Peer (P2P) File Sharing - A distributed network of users who share files by directly connecting to the users' computers over the Internet rather than through a central server.

Remote Desktop Access - Remote control software that allows users to connect to, interact with, and control a computer over the Internet just as if they were sitting in front of that computer.

Streaming Media - Information, typically audio and/or video, that can be heard or viewed as it is being delivered, which allows the user to start playing a clip before the entire download has completed.

PROCEDURE

- Detailed information about the use of email is covered in the company's Email Policy.
- Confidential data must not be A) shared or disclosed in any manner to non-employees of the company, B) should not be posted on the Internet or any publicly accessible systems, and C) should not be transferred in any insecure manner. Please note that this is only a brief overview of how to handle confidential information, and that other policies may refer to the proper use of this information in more detail.
- The user should take reasonable efforts to avoid accessing network data, files, and information that are not directly related to his or her job function. Existence of access capabilities does not imply permission to use this access.

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Acceptable Use**

Effective Date: January 14, 2015

Department: **Information Technology**

Policy Number: N/A

- The following actions shall constitute unacceptable use of the corporate network. This list is not exhaustive, but is included to provide a frame of reference for types of activities that are deemed unacceptable. The user may not use the corporate network and/or systems to:
 - Engage in activity that is illegal under local, state, federal, or international law.
 - Engage in any activities that may cause embarrassment, loss of reputation, or other harm to the company.
 - Disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, annoying, insulting, threatening, obscene or otherwise inappropriate messages or media.
 - Engage in activities that cause an invasion of privacy.
 - Engage in activities that cause disruption to the workplace environment or create a hostile workplace.
 - Make fraudulent offers for products or services.
 - Perform any of the following: port scanning, security scanning, network traffic sniffing, data monitoring, keystroke logging, password capture, or other IT information gathering techniques when not part of employee's job function.
 - Install or distribute unlicensed or "pirated" software.
 - Log into or attempt to log into systems or assets that the user does not have explicit rights to do so.
 - Engaging in denial of service or "hacking" activities of internal or external systems.
 - Any form of online gambling.
 - Reveal personal or network passwords to others, including family, friends, or other members of the household when working from home or remote locations.
 - Install unauthorized or unapproved software or hardware

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Acceptable Use**

Effective Date: January 14, 2015

Department: **Information Technology**

Policy Number: N/A

- Blogging and social networking by selected employees are subject to the terms of this policy, whether performed from the corporate network or from personal systems. Blogging and social networking are allowed from the corporate computer network provided that A) it is done in a professional and responsible manner, B) confidential data is not disclosed, C) no information detrimental to the company is published and D) it is only performed by authorized employees on behalf of the company's official business.
- Instant Messaging software that operates outside the corporate network is not permitted for any purpose. These include AOL, Yahoo, Facebook, etc. instant messengers. Company provided instant messaging software is authorized for use by personnel deemed appropriate by Business Unit Managers and with the proper written approval.
- Actions detrimental to the computer network or other corporate resources, or that negatively affect job performance are not permitted.
- The Internet is a network of interconnected computers of which the company has very little control. The user should recognize this when using the Internet for job related purposes, and understand that it is a public domain and he or she can come into contact with information, even inadvertently, that he or she may find offensive, sexually explicit, or inappropriate. The user must use the Internet for job related purposes at his or her own risk. The company is specifically not responsible for any information that the user views, reads, or downloads from the Internet.

The company's computer systems and networks must not be used to download, upload, or otherwise handle illegal and/or unauthorized copyrighted content. Any of the following activities constitute violations of acceptable use policy, if done without permission of the copyright owner: A) copying and sharing images, music, movies, or other copyrighted material using P2P file sharing or unlicensed CD's and DVD's; B) posting or plagiarizing copyrighted material; and C) downloading copyrighted files which employee has not already legally procured. This list is not meant to be exhaustive, copyright law applies to a wide variety of works and applies to much more than is listed above.

- Peer-to-Peer (P2P) networking is not allowed on the corporate network under any circumstance.
- Streaming media can use a great deal of network resources and thus must be used carefully. Streaming media is allowed for job-related functions only.
- Users should expect no privacy when using the corporate network or company resources. Such use may include but is not limited to: transmission and storage of files, data, and messages. The company reserves the right to monitor any and all use of the computer network. To ensure compliance with company policies this may include the interception and review of any emails, or other messages sent

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Acceptable Use**

Effective Date: January 14, 2015

Department: **Information Technology**

Policy Number: N/A

or received, inspection of data stored on personal file directories, hard disks, and removable media.

- Excessive use of company bandwidth or other computer resources is not permitted. Large file downloads or other bandwidth-intensive tasks that may degrade network capacity or performance must be performed during times of low company-wide usage.
- Personal usage of company computer systems is prohibited.
- Use of remote desktop software and/or services is allowable as long as it is provided by the company. Remote access to the network must conform to the company's Remote Access Policy.
- Using company-owned or company-provided computer systems to circumvent any security systems, authentication systems, user-based systems, electronic security policies, technical controls, or escalating privileges is expressly prohibited. Knowingly taking any actions to bypass or circumvent security is expressly prohibited. This includes but is not limited to accessing guest wireless networks to bypass security controls.
- No company-owned or company-provided computer systems may be knowingly used for activities that are considered illegal under local, state, federal, or international law. Such actions may include, but are not limited to, the following:
 - Unauthorized Port Scanning
 - Unauthorized Network Hacking
 - Unauthorized Packet Sniffing
 - Unauthorized Packet Spoofing
 - Unauthorized Denial of Service
 - Unauthorized Wireless Hacking
 - Any act that may be considered an attempt to gain unauthorized access to or escalate privileges on a computer or other electronic system
 - Acts of Terrorism

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Acceptable Use**

Effective Date: January 14, 2015

Department: **Information Technology**

Policy Number: N/A

- Identity Theft
- Spying
- Downloading, storing, or distributing violent, perverse, obscene, lewd, or offensive material as deemed by applicable statutes
- Downloading, storing, or distributing copyrighted material

The company will take all necessary steps to report and prosecute any violations of this policy.

- Non-company-provided equipment is expressly prohibited on the company's corporate network (does not include any wired and/or wireless guest networks).
- Personal storage devices represent a serious threat to data security and are expressly prohibited on the company's network.
- Installation of non-company-supplied programs is prohibited. Numerous security threats can masquerade as innocuous software - malware, spyware, and Trojans can all be installed inadvertently through games or other programs. Alternatively, software can cause conflicts or have a negative impact on system performance.
- If a security incident or breach of any security policies is discovered or suspected, the user must immediately notify his or her supervisor and IT personnel and/or follow any applicable guidelines as detailed in the corporate Incident Response Policy. Examples of incidents that require notification include:
 - Suspected compromise of login credentials (username, password, etc.).
 - Suspected ransomware/virus/malware/Trojan infection.
 - Loss or theft of any device that contains company information.
 - Loss or theft of ID badge or keycard.
 - Any attempt by any person to obtain a user's password over the telephone or by email.
 - Any other suspicious event that may impact the company's information security.

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Acceptable Use**

Effective Date: January 14, 2015

Department: **Information Technology**

Policy Number: N/A

- Users must treat a suspected security incident as confidential information, and report the incident only to his or her supervisor and IT personnel. Users must not withhold information relating to a security incident or interfere with an investigation.
- This document is part of the company's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

RESPONSIBILITY

This policy will be enforced by the Chief Information Officer and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

CROSS-REFERENCES

N/A

ADDENDA

N/A

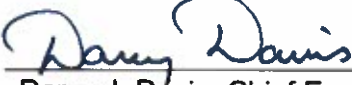
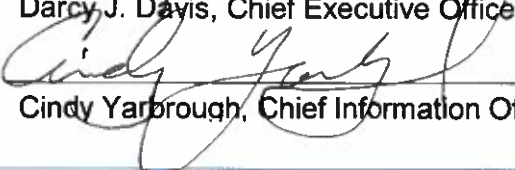
DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Acceptable Use**

Effective Date: January 14, 2015

Department: **Information Technology**

Policy Number: N/A

APPROVED BY	DATE
 Darcy J. Davis, Chief Executive Officer	
 Cindy Yarbrough, Chief Information Officer	9/27/18

PROCEDURE REVISION OR REVIEWED HISTORY

Original Procedure Date	Revisions	
March 12, 2014	1/14/2015 TFS	"[Next Revised Procedure Date]"
	9/27/2018 CY	"[Next Revised Procedure Date]"
	"[Next Revised Procedure Date]"	"[Next Revised Procedure Date]"
	"[Next Revised Procedure Date]"	"[Next Revised Procedure Date]"

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Backups**

Effective Date: January 14, 2015

Department: **Information Technology**

Policy Number: N/A

POLICY

The Health Care District of Palm Beach County is hereinafter referred to as "the company."

A backup policy is similar to an insurance policy - it provides the last line of defense against data loss and is sometimes the only way to recover from a hardware failure, data corruption, or a security incident. A backup policy is related closely to a disaster recovery policy, but since it protects against events that are relatively likely to occur, in practice it will be used more frequently than a contingency planning document. A company's backup policy is among its most important policies.

The purpose of this policy is to provide a consistent framework to apply to the backup process. The policy will provide specific information to ensure backups are available and useful when needed - whether to simply recover a specific file or when a larger-scale recovery effort is needed.

APPLICABILITY

This policy applies to all staff and contractors working on behalf of the Health Care District of Palm Beach County (HCD) and computer systems that access the Health Care District of Palm Beach County's Information Resources.

DEFINITIONS

Backup	To copy data to a second location, solely for the purpose of safe keeping of that data
Backup Media	Any storage devices that are used to maintain data for backup purposes. These are often magnetic tapes, CDs, DVDs, or hard drives.
Full Backup	A backup that makes a complete copy of the target data.
Incremental Backup	A backup that only backs up files that have changed in a designated time period, typically since the last backup was run.
Restoration	Also called "recovery." The process of restoring the data from its backup-up state to its normal state so that it can be used and accessed in a regular manner.

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Backups**

Effective Date: January 14, 2015

Department: **Information Technology**

Policy Number: N/A

PROCEDURE

- The company must identify what data is most critical to its organization. This can be done through a formal data classification process or through an informal review of information assets. Regardless of the method, critical data should be identified so that it can be given the highest priority during the backup process.
- A backup policy must balance the importance of the data to be backed up with the burden such backups place on the users, network resources, and the backup administrator. Data to be backed up will include:
 - All data determined to be critical to company operation and/or employee job function. This includes but is not limited to: health management and information systems, directory services, e-mail, network infrastructure, financial data, claims and eligibility data.
 - All information stored on the corporate file server(s) and email server(s). It is the user's responsibility to ensure any data of importance is moved to the file server.
 - All information stored on network servers, which may include web servers, database servers, domain controllers, firewalls, and remote access servers, etc.
 - Users should not have an expectation of data stored locally (C drive, My Documents, etc.) to be backed up. Users are highly encouraged to store all data on network storage share drives. Users should never store confidential company data on local drives.
- Backup frequency is critical to successful data recovery. The company has determined that the following backup schedule will allow for sufficient data recovery in the event of an incident, while avoiding an undue burden on the users, network, and backup administrator.

Incremental: every day

Full: every 7 days

Network infrastructure devices should be backed up after any change takes place in their configuration, or on a monthly basis, whichever occurs first. Automated backup mechanisms are highly suggested to take the burden off administrators every time a change occurs.

- When utilizing off-site storage solutions, all backup tapes, media, etc. will be encrypted unless the data, operating system, or backup method does not permit the encryption of the data. Back up encryption keys will be changed on per annum basis.
- Geographic separation from the backups must be maintained, to some degree, in order to protect from fire, flood, or other regional or large-scale catastrophes. Offsite storage must be balanced with the time required to recover the data, which must meet the company's uptime requirements. Storage of backups is a serious issue and one that requires careful consideration. Since backups contain critical, and often

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Backups**

Effective Date: January 14, 2015

Department: **Information Technology**

Policy Number: N/A

confidential, company data, precautions must be taken that are commensurate to the type of data being stored. The company has set the following guidelines for backup storage.

When stored onsite, backups should be kept in an environmentally secure container within an access-controlled area. When shipped off-site, a hardened facility (i.e., commercial backup service or safe deposit box) that uses accepted methods of environmental controls, including fire suppression, and security processes must be used to ensure the integrity of the backup media.

- When determining the time required for backup retention, the company must determine what number of stored copies of backup-up data is sufficient to effectively mitigate risk while preserving required data. The company has determined that the following will meet all requirements (note that the backup retention policy must confirm to the company's data retention policy and any industry regulations, if applicable):

Incremental Backups must be saved for at least one month.

Full Backups must be saved for at least one month.

- The data restoration procedures must be tested and documented. Documentation should include exactly who is responsible for the restore, how it is performed, under what circumstances it is to be performed, and how long it should take from request to restoration. It is extremely important that the procedures are clear and concise such that they are not A) misinterpreted by readers other than the backup administrator, and B) confusing during a time of crisis.
- Since a backup policy does no good if the restoration process fails it is important to periodically test the restore procedures to eliminate potential problems.

Backup restores must be tested when any change is made that may affect the backup system, as well as at least once per year.

- Certain types of backup media, such as magnetic tapes, have a limited functional lifespan. After a certain time in service the media can no longer be considered dependable. When backup media is put into service the date must be recorded on the media. The media must then be retired from service after its time in use exceeds manufacturer specifications.

RESPONSIBILITY

This policy will be enforced by the Chief Information Officer and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Backups**

Effective Date: January 14, 2015

Department: **Information Technology**

Policy Number: N/A

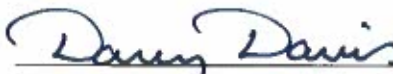
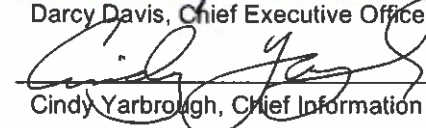
including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities

CROSS-REFERENCES

N/A

ADDENDA

N/A

APPROVED BY	DATE
 _____ Darcy Davis, Chief Executive Officer	_____
 _____ Cindy Yarbrough, Chief Information Officer	9/26/18 _____

PROCEDURE REVISION OR REVIEWED HISTORY

Original Procedure Date	Reviewed or Revised	
March 12, 2014	1/14/2015 TFS	"[Next Revised Procedure Date]"
	9/14/2018 CY	"[Next Revised Procedure Date]"
	"[Next Revised Procedure Date]"	"[Next Revised Procedure Date]"
	"[Next Revised Procedure Date]"	"[Next Revised Procedure Date]"

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Change Control**

Effective Date: January 14, 2015

Department: **Information Technology**

Policy Number: N/A

POLICY

The Health Care District of Palm Beach County is hereinafter referred to as "the company."

A well structured configuration management and change control process must be in place to aid staff members through many different types of changes to the environment. Without this policy in place, people can make changes that others do not know about and have not been approved. This can result in the risk of confusion, or at the worst, the disruption of operations and services. These risks can be mitigated with a sound Change Management and Control Policy.

The purpose of this policy is to state the standards for change management and control to the company's network. Configuration management and system changes can be done safely if certain steps are taken to mitigate known risks. This policy outlines the steps the company wishes to take to secure its change management procedures.

APPLICABILITY

This policy covers anyone who makes changes to company production data or systems, to include vendors and Business Associates. Business Units wishing to make purchases of technology related equipment, software, applications, and services are encouraged to seek the advice and consultation of the IT Department before purchase. This will help alleviate any technological barriers that may be encountered after purchase.

DEFINITIONS

N/A

PROCEDURE

- Change requests must be submitted to IT management and to affected Business Unit management for approval. The requestor is responsible for overseeing the activities that take place until completion.
- The individual or group requesting the change must justify the reasons and clearly show the benefits and

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Change Control**

Effective Date: January 14, 2015

Department: **Information Technology**

Policy Number: N/A

possible pitfalls of the change. More research and information may be required at this stage.

- When emergency or immediate changes are required to bring a system back on line, step 4.1 and 4.2 will be accomplished as soon as possible. After the system has been stabilized, steps 4.3 and 4.6 will be accomplished.
- Once the change is approved, it should be entered into the change tracking application. The application must be updated as progress continues until completion.
- The change must be fully tested to uncover any unforeseen results. Depending on the severity of the change, it may need to be presented to the affected business unit to show purpose, outcome, and possible ramifications of the change. The test plan and final results must be documented in the change management application.
- Once the change has been fully tested and reviewed, a schedule will be developed that outlines the projected phases of the change being implemented and the necessary milestones. The steps should be fully documented and progress will be monitored. In addition to an implementation plan, a “back out” plan will be incorporated in case the change goes awry and a return to a pre-change state is necessary.
- A summary of the change will be documented in the change management software.

RESPONSIBILITY

This policy will be enforced by the Chief Information Officer and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

CROSS-REFERENCES

N/A

ADDENDA

N/A


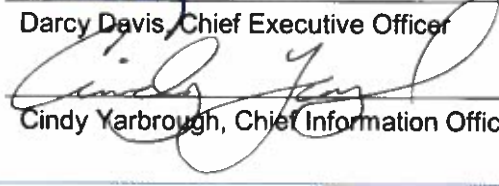
DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Change Control**

Effective Date: January 14, 2015

Department: **Information Technology**

Policy Number: N/A

APPROVED BY	DATE
 _____ Darcy Davis, Chief Executive Officer	_____ _____ 9/27/18
 _____ Cindy Yarbrough, Chief Information Officer	

PROCEDURE REVISION OR REVIEWED HISTORY

Original Procedure Date	Reviewed or Revised	
March 12, 2014	1/14/2015 TFS	"[Next Revised Procedure Date]"
	9/27/2018 CY	"[Next Revised Procedure Date]"
	"[Next Revised Procedure Date]"	"[Next Revised Procedure Date]"
	"[Next Revised Procedure Date]"	"[Next Revised Procedure Date]"

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title:	Email	Effective Date:	January 14, 2015
Department:	Information Technology	Policy Number:	N/A

POLICY

The Health Care District of Palm Beach County is hereinafter referred to as "the company."

Email is an essential component of business communication; however it presents a particular set of challenges due to its potential to introduce a security threat to the network. Email can also have an effect on the company's liability by providing a written record of communications, so having a well thought out policy is essential. This policy outlines expectations for appropriate, safe, and effective email use.

The purpose of this policy is to detail the company's usage guidelines for the email system. This policy will help the company reduce risk of an email-related security incident, foster good business communications both internal and external to the company, and provide for consistent and professional application of the company's email principles.

APPLICABILITY

The scope of this policy includes the company's email system in its entirety, including desktop and/or web-based email applications, server-side applications, email relays, and associated hardware. It covers all electronic mail sent from the system, as well as any external email accounts accessed from the company network regardless of employment status (full time, part time, contractor, consultant, or vendor).

DEFINITIONS

Auto Responder	An email function that sends a predetermined response to anyone who sends an email to a certain address. Often used by employees who will not have access to email for an extended period of time in order to notify senders of their absence.
Certificate	Also called a "Digital Certificate." A file that confirms the identity of an entity, such as a company or person. Often used in VPN and encryption management to establish trust of the remote entity.
Data Leakage	Also called Data Loss, data leakage refers to data or intellectual property that is pilfered in small amounts or otherwise removed from the network or computer systems. Data leakage is sometimes malicious and sometimes inadvertent by users with good intentions.
Email	Short for electronic mail, email refers to electronic letters and other communication sent between networked computer users, either within a company or between companies.

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Email** Effective Date: January 14, 2015

Department: **Information Technology** Policy Number: N/A

Encryption	The process of encoding data with an algorithm so that it is unintelligible and secure without the key. Used to protect data during transmission or while stored.
Mobile Devices	A portable device that can be used for certain applications and data storage. Examples are PDAs or smartphones.
Password	A sequence of characters that is used to authenticate a user to a file, computer, network, or other device. Also known as a passphrase or passcode.
Spam	Unsolicited bulk email. Spam often includes advertisements, but can include malware, links to infected websites, or other malicious or objectionable content.
Smartphone	A mobile telephone that offers additional applications, such as PDA functions and email.
Two Factor Authentications	A means of authenticating a user that utilizes two methods: something the user has, and something the user knows. Examples are smart cards, tokens, or biometrics, in combination with a password.

PROCEDURE

- Users are asked to exercise common sense when sending or receiving email from company accounts. Additionally, the following applies to the proper use of the company email system.
- When using a company email account, email must be addressed and sent carefully. Users should keep in mind that the company loses any control of email once it is sent external to the company network. Users must take extreme care when typing in addresses, particularly when email address auto-complete features are enabled; using the "reply all" function; or using distribution lists in order to avoid inadvertent information disclosure to an unintended recipient. Careful use of email will help the company avoid the unintentional disclosure of sensitive or non-public information.
- Personal Use and General Guidelines
 - The following is never permitted: spamming, harassment, communicating threats, solicitations, chain letters, personal financial gain, or pyramid schemes. This list is not exhaustive, but is included to provide a frame of reference for types of activities that are prohibited.
 - Emails of a personal nature sent and received on company email systems will be limited in nature.
 - The user is prohibited from forging email header information or attempting to impersonate another

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Email** Effective Date: January 14, 2015

Department: **Information Technology** Policy Number: N/A

person.

- Users are prohibited from intercepting or otherwise reading email belonging to another user or group that he or she is not authorized to view.
- Email is an insecure method of communication, and thus information that is considered confidential or proprietary to the company may not be sent via email, regardless of the recipient, without proper encryption.
- It is company policy not to open email attachments from unknown senders, or when such attachments are unexpected.
- Email systems were not designed to transfer large files and as such emails should not contain attachments of excessive file size.
- Company e-mail accounts are not to be used to subscribe to personal or commercial distribution lists of a non-business related nature.
- Please note that the topics above may be covered in more detail in other sections of this policy.
- The company uses email as an important communication medium for business operations. Users of the corporate email system are expected to check and respond to email in a consistent and timely manner during business hours.

Additionally, users are asked to recognize that email sent from a company account reflects on the company, and, as such, email must be used with professionalism and courtesy.

- Email signatures (contact information appended to the bottom of each outgoing email) may or may not be used, at the discretion of management or the individual user. Users are asked to keep any email signatures professional in nature; however the company does not place any restrictions on email signature content.
- The company recommends the use of an auto-responder (if the email system is equipped with such a feature) if the user will be out of the office for an entire business day or more. The auto-response should notify the sender that the user is out of the office, the date of the user's return, and who the sender should contact if immediate assistance is required.
- The company makes the distinction between the sending of mass emails and the sending of unsolicited email (spam). Mass emails may be useful for company purposes (such as when communicating with the company's employees or customer base), and is allowed as the situation dictates. The sending of spam, on the other hand, is strictly prohibited.

Due to the nature and capability of mass e-mail, the ability to mass email is limited to a select few

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Email** Effective Date: January 14, 2015
Department: **Information Technology** Policy Number: N/A

employees.

- Users must use care when opening email attachments. Viruses, Trojans, and other malware can be easily delivered as an email attachment. Users should:
 - Never open unexpected email attachments.
 - Never open email attachments from unknown sources.
 - Never click links within email messages unless he or she is certain of the link's safety. It is often best to copy and paste the link into your web browser, or retype the URL, as specially-formatted emails can hide a malicious URL.

The company may use methods to block what it considers to be dangerous or emails or strip potentially harmful email attachments as it deems necessary.

- Users should expect no privacy when using the corporate network or company resources. Such use may include but is not limited to: transmission and storage of files, data, and messages. The company reserves the right to monitor any and all use of the computer network. To ensure compliance with Federal and State statutes and company policies this may include the long term storage, interception and review of any emails, or other messages sent or received, inspection of data stored on personal file directories, hard disks, and removable media.

Furthermore, email, files, and data transmitted via corporate networks are subject to retention and long term storage by the company.

- Users should be advised that the company owns and maintains all legal rights to its email systems and network, and thus any email passing through these systems is owned by the company and it may be subject to use for purposes not be anticipated by the user. Keep in mind that email may be backed up, otherwise copied, retained, or used for legal, disciplinary, or other reasons. Additionally, the user should be advised that email sent to or from certain public or governmental entities may be considered public record.
- Users must understand that the company has little control over the contents of inbound email, and that this email may contain material that the user finds offensive. If unsolicited email becomes a problem, the company may attempt to reduce the amount of this email that the users receive, however no solution will be 100 percent effective. The best course of action is to not open emails that, in the user's opinion, seem suspicious. If the user is particularly concerned about an email, or believes that it contains illegal content, he or she should notify his or her supervisor.
- Many mobile phones or other mobile devices, often called smartphones or tablets, provide the capability to send and receive email. This can present a number of security issues, particularly relating to the storage of email, which may contain sensitive data, on the device. Users are not to access, or attempt to access, the

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title:	Email	Effective Date:	January 14, 2015
Department:	Information Technology	Policy Number:	N/A

company's email system from a mobile device without the permission of his or her supervisor.

Currently, the company only allows mobile device e-mail access to salaried employees.

Note that this section does not apply if the company provides the phone and mobile email access as part of its remote access plan. In this case, permission is implied. Refer to the Mobile Device Policy for more information.

- Any specific regulations (industry, governmental, legal, etc.) relating to the company's use or retention of email communications are listed in separate data retention policies.
- The company recognizes that users may have personal email accounts in addition to their company-provided account. The following sections apply to non-company provided email accounts:
- Users must use the corporate email system for all business-related email. Users are prohibited from sending business email from a non-company-provided email account. Users are prohibited from sending or forwarding business email to a personal account for convenience or in an effort to bypass existing security mechanisms.
- Users are prohibited from accessing external or personal email accounts from the corporate network. Exceptions may be made on a case by case basis pending department manager approval.
- Users are required to use a non-company-provided (personal) email account for all non-business communications. The corporate email system is for corporate communications only.
- As with any company passwords, passwords used to access email accounts must be kept confidential and used in adherence with the Password Policy. At the discretion of the Chief Information Officer, the company may further secure email with certificates, two factor authentication, or another security mechanism.
- Email is an insecure means of communication. Users should think of email as they would a postcard, which, like email, can be intercepted and read on the way to its intended recipient. Users must exercise care when addressing, replying (to all) and forwarding email that may contain sensitive information.

Sensitive information may include proprietary company information, information not publicly available, protected health information (HIPAA), financial information, Payment Card Industry (PCI) data, Personal Identification Information, and any other data that if released to unauthorized individuals, could cause harm to the company or its customer base.

The company requires that any email containing sensitive information be encrypted using company provided email encryption methods. If the e-mail itself is unencrypted then any attachment(s) within the email containing sensitive information must be encrypted. Please refer to the company's Encryption Policy

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Email**

Effective Date: January 14, 2015

Department: **Information Technology**

Policy Number: N/A

for more detailed guidance.

Further guidance on the treatment of confidential information exists in the company's Confidential Data Policy. If information contained in the Confidential Data Policy conflicts with this policy, the Confidential Data Policy will apply.

- The company will use its best effort to administer the company's email system in a manner that allows the user to both be productive while working as well as reduce the risk of an email-related security incident.
- A good way to mitigate risk from email is to filter it before it reaches the user so that the user receives only safe, business-related messages. For this reason, the company will filter email at the Internet gateway and/or the mail server, in an attempt to filter out spam, viruses, or other messages that may be deemed A) contrary to this policy, or B) a potential risk to the company's IT security. No method of email filtering is 100 percent effective, so the user is asked additionally to be cognizant of this policy and use common sense when opening emails.

Additionally, many email and/or anti-malware programs will identify and quarantine emails that it deems suspicious. This functionality may or may not be used at the discretion of the Chief Information Officer.

- The use of an email disclaimer, usually text appended to the end of every outgoing email message, is an important component in the company's risk reduction efforts. The company requires the use of email disclaimers on every outgoing email, which must contain the following notices:
 - The email is for the intended recipient only
 - The email may contain private information
 - If the email is received in error, the sender should be notified and any copies of the email destroyed
- Any unauthorized review, use, or disclosure of the contents is prohibited

An example of such a disclaimer is:

NOTE: This email message and any attachments are for the sole use of the intended recipient(s) and may contain confidential and/or privileged information. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by replying to this email, and destroy all copies of the original message.

The company should review any applicable regulations relating to its electronic communication to ensure that its email disclaimer includes all required information.

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Email** Effective Date: January 14, 2015

Department: **Information Technology** Policy Number: N/A

- Users are encouraged to delete email periodically when the email is no longer needed for regulatory or business purposes. The goal of this policy is to keep the size of the user's email account manageable, and reduce the burden on the company to store and backup unnecessary email messages.

However, users are strictly forbidden from deleting email in an attempt to hide a violation of this or another company policy. Further, email must not be deleted when there is an active investigation or litigation where that email may be relevant.

- Email must be retained and backed up in accordance with the applicable federal and state statutes, laws, and company policies, which may include but are not limited to the: Data Classification Policy, Confidential Data Policy, Backup Policy, and Retention Policy.

Unless otherwise indicated, for the purposes of backup and retention, email should be considered operational data.

- Email addresses must be constructed in a standard format in order to maintain consistency across the company. The company can choose virtually any format, as long as it can be applied consistently throughout the organization. The intent of this policy is to simplify email communication as well as provide a professional appearance.
- Often the use of an email alias, which is a generic address that forwards email to a user account, is a good idea when the email address needs to be in the public domain, such as on the Internet. Aliases reduce the exposure of unnecessary information, such as the address format for company email, as well as (often) the names of company employees who handle certain functions. Keeping this information private can decrease risk by reducing the chances of a social engineering attack.

The company may or may not use email aliases, as deemed appropriate by the Chief Information Officer and/or executive team. Aliases may be used inconsistently, meaning: the company may decide that aliases are appropriate in some situations but not others depending on the perceived level of risk.

- Email accounts will be set up for each user determined to have a business need to send and receive company email. Accounts will be set up at the time a new hire starts with the company, or when a promotion or change in work responsibilities for an existing employee creates the need to send and receive email.

At times, email accounts may be given to non-employees, contractors, or other individuals authorized to conduct certain aspects of the company's business. In these cases, the company may designate the temporary or non-employee status of the account in the account name.

All account activations will be initiated after the proper request documentation has been completed, i.e.

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Email**

Effective Date: January 14, 2015

Department: **Information Technology**

Policy Number: N/A

User Registration Form.

- When a user leaves the company, or his or her email access is officially terminated for another reason, the company will disable the user's access to the account by password change, disabling the account, or another method. The company is under no obligation to block the account from receiving email, and may continue to forward inbound email sent to that account to another user, or set up an auto-response to notify the sender that the user is no longer employed by the company. In certain circumstances, another user may need long term full access to the former employee's account. The manager of the affected department's approval is required in these instances.
- As part of the email service, email storage may be provided on company servers or other devices. The email account storage size must be limited to what is reasonable for each employee, at the determination of the Chief Information Officer. Storage limits may vary by employee or position within the company.
- The following actions shall constitute unacceptable use of the corporate email system. This list is not exhaustive, but is included to provide a frame of reference for types of activities that are deemed unacceptable. The user may not use the corporate email system to:
 - Send any information that is illegal under applicable laws.
 - Using a corporate email address to subscribed to non-company related distribution lists, i.e. local restaurants, coupon suppliers, clothing merchants, etc.
 - Access another user's email account without A) the knowledge or permission of that user - which should only occur in extreme circumstances, or B) the approval of company executives in the case of an investigation, or C) when such access constitutes a function of the employee's normal job responsibilities.
 - Send any emails that may cause embarrassment, damage to reputation, or other harm to the company.
 - Disseminate defamatory, discriminatory, vilifying, sexist, racist, abusive, rude, harassing, annoying, insulting, threatening, obscene or otherwise inappropriate messages or media.
 - Send emails that cause disruption to the workplace environment or create a hostile workplace. This includes sending emails that are intentionally inflammatory, or that include information not conducive to a professional working atmosphere.
 - Make fraudulent offers for products or services.
 - Attempt to impersonate another person or forge an email header.
 - Send spam, letter bombs, solicitations, chain letters, or pyramid schemes.

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Email**

Effective Date: January 14, 2015

Department: **Information Technology**

Policy Number: N/A

- Knowingly misrepresent the company's capabilities, business practices, warranties, pricing, or policies.
- Conduct non-company-related business.
- Knowingly engaging in activity designed to deny the availability of email services, also known as denial of service.

The company may take steps to report and prosecute violations of this policy, in accordance with company standards and applicable laws.

- Data can leave the network in a number of ways. Often this occurs unintentionally by a user with good intentions. For this reason, email poses a particular challenge to the company's control of its data.

Unauthorized emailing of company data, confidential or otherwise, to external email accounts for the purpose of saving this data external to company systems is prohibited. If a user needs access to information from external systems (such as from home or while traveling), that user should notify his or her supervisor rather than emailing the data to a personal account or otherwise removing it from company systems.

The company may employ data loss prevention techniques to protect against leakage of confidential data at the discretion of the Chief Information Officer.

- Email systems were not designed to transfer large files and as such emails should not contain attachments of excessive file size. The company requires that the user limit email attachments to 50Mb or less.

The user is further asked to recognize the additive effect of large email attachments when sent to multiple recipients, and use restraint when sending large files to more than one person.

- This document is part of the company's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.
- This policy will be enforced by the Chief Information Officer and/or executive team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities are suspected, the company may report such activities to the applicable authorities. If any provision of this policy is found to be unenforceable or voided for any reason, such invalidation will not affect any remaining provisions, which will remain in force.
- This policy will be reviewed and edited if applicable at a minimum per annum or when changes are required that affect how this policy is applied and enforced. All modifications will be recorded in the Change Log at the end of this document.

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Email**

Effective Date: January 14, 2015

Department: **Information Technology**

Policy Number: N/A

RESPONSIBILITY

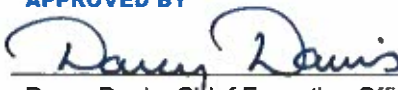
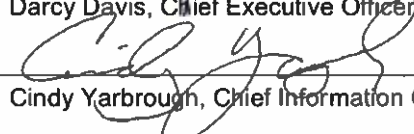
This policy will be enforced by the Chief Information Officer and/or executive team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities are suspected, the company may report such activities to the applicable authorities. If any provision of this policy is found to be unenforceable or voided for any reason, such invalidation will not affect any remaining provisions, which will remain in force.

CROSS-REFERENCES

N/A

ADDENDA

N/A

APPROVED BY	DATE
 Darcy Davis, Chief Executive Officer	
 Cindy Yarbrough, Chief Information Officer	9/27/18

PROCEDURE REVISION OR REVIEWED HISTORY

Original Procedure Date	Reviewed or Revised	
March 12, 2014	1/14/2015 TFS	"[Next Revised Procedure Date]"
	9/27/2018 CY	"[Next Revised Procedure Date]"
	"[Next Revised Procedure Date]"	"[Next Revised Procedure Date]"
	"[Next Revised Procedure Date]"	"[Next Revised Procedure Date]"

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title:	Encryption Policy	Effective Date:	January 14, 2015
Department:	Information Technology	Policy Number:	N/A

POLICY

The Health Care District of Palm Beach County is hereinafter referred to as "the company."

1.0 Overview

Encryption, also known as cryptography, can be used to secure data while it is stored or being transmitted. It is a powerful tool when applied and managed correctly. As the amount of data the company must store digitally increases, the use of encryption must be defined and consistently implemented in order ensure that the security potential of this technology is realized.

2.0 Purpose

The purpose of this policy is to outline the company's standards for the use of encryption technology so that it is used securely and managed appropriately. This policy not only covers what data is to be encrypted, but also how encryption is to be implemented and controlled.

3.0 Scope

This policy covers all data stored on or transmitted across corporate systems.

4.0 Policy

4.1 Applicability of Encryption

While it is best practice to encrypt all company data, this may not be practical given the amount of data on company owned systems. Examples may include publicly releasable information stored on local shares.

At a minimum, all sensitive data, whether stored at rest on company systems or transmitted to and from company systems, must be encrypted. This may include proprietary company information, information not publicly available, protected health information (HIPAA), financial information, Payment Card Industry (PCI) data, Personal Identification Information, and any other data that if released to unauthorized individuals, could cause harm to the company or its customer base.

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Encryption Policy** Effective Date: January 14, 2015

Department: **Information Technology** Policy Number: N/A

1. Data while stored: This includes data located on company-owned or company-provided systems, devices, media, personally owned devices that access company data, etc. One of following examples of encryption options for stored data will be used on the devices listed above:

- Whole disk encryption (workstations, laptops, mobile devices, etc.)
- Encryption of partitions/files
- Encryption of disk drives
- Encryption of storage media/USB drives, if authorized.
- Encryption of backups
- Encryption of data generated by applications

2. Data while transmitted: This includes any data sent across the company network, or any data sent to or from a company-owned or company-provided system. Encryption will be used on all sensitive data being transmitted within, to, or from company systems. Types of transmitted data that will be encrypted include:

- VPN tunnels
- Remote access sessions
- Web applications
- An entire email message with or without attachments containing sensitive information outlined in 4.1, paragraph 2.
- An encrypted attachment containing sensitive information outlined in 4.1, paragraph 2 sent within an unencrypted email.
- Remote desktop access
- Communications with applications/databases, both internal and external to the company.

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: Encryption Policy	Effective Date: January 14, 2015
Department: Information Technology	Policy Number: N/A

- Files transmitted via any file transfer protocol, i.e. FTP, SFTP, etc.
- Scan-to-email communications.

4.2 Encryption Key Management

Key management is critical to the success of an implementation of encryption technology. The following guidelines apply to the company's encryption keys, encryption passwords, encryption passphrases, and key management:

- Management of keys must ensure that data is available for decryption when needed.
- Keys must be backed up.
- Keys must be locked up.
- Keys must never be transmitted in clear text.
- Keys are confidential data.
- Keys must not be shared.
- Keys must be used and changed at least annually, semi-annually is preferred.
- Management of keys is restricted to the IT Security official (does not apply to user passwords, passphrases, etc.)

4.3 Acceptable Encryption Algorithms

45 CFR § 164.312 requires the implementation of encryption mechanisms to protect sensitive data. In order to comply with this requirement, only the strongest types of generally-accepted, non-proprietary encryption algorithms are allowed that conform to current FIPS standards. Acceptable algorithms should be reevaluated as encryption technology changes.

Use of company proprietary encryption is specifically forbidden since it has not been subjected to public

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: Encryption Policy	Effective Date: January 14, 2015
Department: Information Technology	Policy Number: N/A

inspection and its security cannot be assured.

4.4 Legal Use

Some governments have regulations applying to the use and import/export of encryption technology. The company must conform to encryption regulations of the local or applicable government.

The company specifically forbids the use of encryption to hide illegal, immoral, or unethical acts. Anyone doing so is in violation of this policy and will face immediate consequences per the Enforcement section of this document.

4.5 Applicability of Other Policies

This document is part of the company's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

5.0 Enforcement

This policy will be enforced by Chief Information Officer and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

6.0 Review and/or Revisions

This policy will be reviewed and edited if applicable at a minimum per annum or when changes are required that affect how this policy is applied and enforced. All modifications will be recorded in the Change Log at the end of this document.

7.0 Definitions

Encryption - The process of encoding data with an algorithm so that there is a low probability of assigning meaning to the data without possessing the key originally used to encode the data. Used to protect data during transmission or while stored.

Encryption Key - An alphanumeric series of characters that enables data to be encrypted and decrypted

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: Encryption Policy	Effective Date: January 14, 2015
Department: Information Technology	Policy Number: N/A

utilizing a pre-existing algorithm.

FIPS – Federal Information Processing Standards. Standards developed by the U.S. federal government for use in computer systems, but more significantly encryption standards such as *FIPS PUB 197 Advance Encryption Standard (AES)*.

Mobile Storage Media - Any data storage device used to store information. Examples are: external hard drive, USB thumb drive, compact flash card, CD/DVD, magnetic tape, floppy disk, etc.


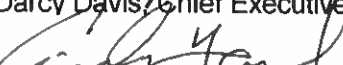
Password - A sequence of characters that is used to authenticate a user to a file, computer, or network. Also known as a passphrase or passcode.

Remote Access - The act of communicating with a computer or network from an off-site location. Often performed by home-based or traveling users to access documents, email, or other resources at a main site.

Remote Desktop Access - Remote control software that allows users to connect to, interact with, and control a computer over the Internet just as if they were sitting in front of that computer.

Virtual Private Network (VPN) - A secure network implemented over an insecure medium, created by using encrypted tunnels for communication between endpoints.

Whole Disk Encryption - A method of encryption that encrypts all data on a particular drive or volume, including swap space and temporary files.

APPROVED BY	DATE
 _____ Darcy Davis, Chief Executive Officer	10-29-18 _____
 _____ Cindy Yarbrough, Chief Information Officer	10/18/18 _____

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Encryption Policy** Effective Date: January 14, 2015

Department: **Information Technology** Policy Number: N/A

PROCEDURE REVISION OR REVIEWED HISTORY

Original Procedure Date	Reviewed or Revised	
March 14, 2014	1/14/2015 TFS	"[Next Revised Procedure Date]"
	10/12/2018 CY	"[Next Revised Procedure Date]"
	"[Next Revised Procedure Date]"	"[Next Revised Procedure Date]"
	"[Next Revised Procedure Date]"	"[Next Revised Procedure Date]"
	"[Next Revised Procedure Date]"	"[Next Revised Procedure Date]"

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Guest Access**

Effective Date: January 14, 2015

Department: **Information Technology**

Policy Number: N/A

POLICY

The Health Care District of Palm Beach County is hereinafter referred to as "the company."

Guest access to the company's network is often necessary for customers, consultants, or vendors who are visiting the company's offices. This can be simply in the form of outbound Internet access, or the guest may require access to specific resources on the company's network. Guest access to the company's network must be tightly controlled.

The company may wish to provide network access as a courtesy to guests wishing to access the Internet, or by necessity to visitors with a business need to access the company's resources. This policy outlines the company's procedures for securing guest access.

APPLICABILITY

The scope of this policy includes any visitor to the company wishing to access the network or Internet through the company's infrastructure, and covers both wired and wireless connections. This scope excludes guests accessing wireless broadband accounts directly through a cellular carrier or third party where the traffic does not traverse the company's network.

DEFINITIONS

Account A combination of username and password that allows access to computer or network resources.

Guest A visitor to the company premises who is not an employee.

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Guest Access**

Effective Date: January 14, 2015

Department: **Information Technology**

Policy Number: N/A

PROCEDURE

- Guest access will be provided on a case-by-case basis to any person who can demonstrate a reasonable business need to access the network, or access the Internet from the company network. All account activations will be initiated after the proper request documentation has been completed, i.e. User Registration Form. Guest accounts will be automatically disabled after 90 days from activation unless otherwise noted for longer term guests.
- Guests must agree to and sign the company's Acceptable Use Policy (AUP) before being granted access.
- Guest need for access will be evaluated and provided on a case-by-case basis. This should involve management approval if the request is non-standard.
- Guest accounts, if offered, are only to be used by guests. Users with network accounts must use their accounts for network access. Guest accounts must be set up for each guest accessing the company's network. Guest accounts must have specific expiration dates that correlate to the business need for the individual guest's access. The account expiration date is not to exceed the time period required by the guest for access which is currently 90 days unless need requires it to be longer. A proper user access request form is required.
- Guests are expected to be responsible for maintaining the security of his or her machine, and to ensure that it is free of viruses, Trojans, malware, etc. The company reserves the right to inspect the machine if a security problem is suspected, but will not inspect each guest's system prior to accessing the network.
- Best practices dictate that guest access be kept separate, either logically or physically, from the corporate network, since guests have typically not undergone the same amount of scrutiny as the company's employees. This must be weighed, however, with the costs and technical issues that come with providing such separation. Guest access should be provided prudently and monitored for appropriateness of use.
- Guests requiring public internet access only will be directed to one of the company's public wireless networks.
- Guest access will be restricted to the minimum amount necessary. Depending on the guest needing access, this can often be limited to outbound Internet access only. The company will evaluate the need of each guest and provide further access if there is a business need to do so.

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Guest Access**

Effective Date: January 14, 2015

Department: **Information Technology**

Policy Number: N/A

- Since guests are not employees of the company they are not considered trusted users. As such, the company will monitor guest access to ensure that the company's interests are protected and the Acceptable Use Policy is being adhered to.
- This document is part of the company's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.
- This policy will be enforced by the IT Manager and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.
- This policy will be reviewed and edited if applicable at a minimum per annum or when changes are required that affect how this policy is applied and enforced. All modifications will be recorded in the Change Log at the end of this document.

RESPONSIBILITY

This policy will be enforced by the Chief Information Officer and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

CROSS-REFERENCES

N/A

ADDENDA

N/A


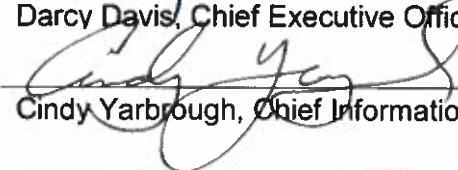
DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Guest Access**

Effective Date: January 14, 2015

Department: **Information Technology**

Policy Number: N/A

APPROVED BY	DATE
 Darcy Davis, Chief Executive Officer	
 Cindy Yarbrough, Chief Information Officer	9/24/18

PROCEDURE REVISION OR REVIEWED HISTORY

Original Procedure Date

January 14, 2015

Reviewed or Revised

1/14/2015 TFS	"[Next Revised Procedure Date]"
9/26/2018 CY	"[Next Revised Procedure Date]"
"[Next Revised Procedure Date]"	"[Next Revised Procedure Date]"
"[Next Revised Procedure Date]"	"[Next Revised Procedure Date]"
"[Next Revised Procedure Date]"	"[Next Revised Procedure Date]"

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Incident Reporting**

Effective Date: 09/25/2018

Department: **Information Technology**

Policy Number: N/A

POLICY

The Health Care District of Palm Beach County is hereinafter referred to as "the company."

The purpose of this policy is to promptly report, investigate, and resolve all incidents that are not part of normal operations that disrupt business processes.

APPLICABILITY

This policy applies to all Information Technology department employees.

DEFINITIONS

Incident An unplanned interruption to an IT service or reduction in the quality, including reliability and availability, of an IT service or any component part of that service.

Major Incident An event which has significant impact or urgency, which demands a response beyond the routine Incident Management process. This will include, but not limited to, any incident that involves loss of confidential information, such as PHI or PII, ransomware attacks or phishing emails.

PROCEDURE

- Employees should respond quickly to reports of any incident and take immediate action to contain the incident, prevent its reoccurrence and further degradation of services.
- Employees will need to determine whether the incident should be handled individually or reported to the Chief Information Officer and Security Analyst.

If the incident is not classified as major, the IT support staff should repair the system, restore services and log evidence in the incident reporting software.

If the incident is classified as major, the Health Care District Incident Response Plan will be followed and evidence of the event will be logged in the reporting software.

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Incident Reporting**

Effective Date: 09/25/2018

Department: **Information Technology**

Policy Number: N/A

RESPONSIBILITY

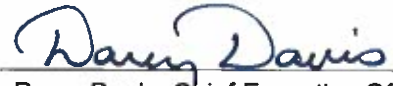
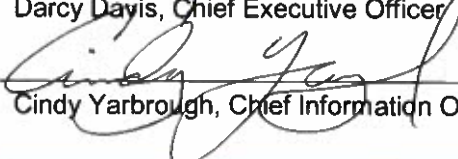
This policy will be enforced by the Chief Information Officer and/or executive team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities are suspected, the company may report such activities to the applicable authorities. If any provision of this policy is found to be unenforceable or voided for any reason, such invalidation will not affect any remaining provisions, which will remain in force.

CROSS-REFERENCES

N/A

ADDENDA

N/A

APPROVED BY	DATE
 _____ Darcy Davis, Chief Executive Officer	_____
 _____ Cindy Yarbrough, Chief Information Officer	9/27/18 _____

PROCEDURE REVISION OR REVIEWED HISTORY

Original Procedure Date	Reviewed or Revised	
September 25, 2018	"[Next Revised Procedure Date]"	"[Next Revised Procedure Date]"
	"[Next Revised Procedure Date]"	"[Next Revised Procedure Date]"
	"[Next Revised Procedure Date]"	"[Next Revised Procedure Date]"
	"[Next Revised Procedure Date]"	"[Next Revised Procedure Date]"

POLICY

Policy Title: **Information Security Governance Policy**

Effective Date: September 13, 2017

Department: **Information Technology and Compliance**

Policy Number: IS1000

POLICY

The Health Care District of Palm Beach County (the "District") Information Security Management Policy (ISMP) provides definitive information on the measures used to establish and enforce the Information Security Management Program at the District.

SCOPE

This policy and program applies to all employees and workforce members of the Health Care District of Palm Beach County and its Affiliated Entities ("District"), including, Lakeside Medical Center, E.J. Healey Center, School Health, C. L. Brumback Clinics, Pharmacy, Aeromedical, and Trauma.

PURPOSE

The purpose of the Information Security Management Policy (ISMP) is to provide a framework for:

- Implementing an Information Security Management Program.
- Protecting the confidentiality, integrity, and availability of all District data and systems.
- Ensuring the effectiveness of security controls over data and systems that support District's operations.
- Providing effective District-wide management and oversight of information security risks.
- Providing for the development, review, and maintenance of security controls required to protect the District's data and systems.

The key factor driving the formation of the Information Security Management Program is risk. This program sets the ground rules under which the District operates and safeguards its data and systems to both reduce risk and minimize the impact of potential incidents.

The procedures resulting from this policy—including their related standards, and guidelines—are necessary to support the management of information security risks in daily operations. The development of policies provides due care to ensure that the District users understand their day-to-day security responsibilities and the threats that could impact the District.

Implementing consistent security controls across the District will help the District comply with current and future compliance obligations as well as ensure long-term due diligence in protecting the confidentiality, integrity, and availability of the District data.

POLICY

Policy Title: **Information Security Governance Policy**

Effective Date: September 13, 2017

Department: **Information Technology and Compliance**

Policy Number: IS1000

1.1. APPLICABILITY

This policy applies to all District data, systems, activities, and assets owned, leased, controlled, or used by the District, its agents, contractors, or other business partners on behalf of the District. This policy applies to all District employees, as well as contractors, consultants, and their respective facilities supporting the District business operations, wherever District data are stored or processed, including any third party contracted by the District to handle, process, transmit, store, or dispose of the District data.

Protecting company data and the systems that collect, process, and maintain this information is of critical importance. Consequently, the security of systems must:

- Include controls and safeguards to offset possible threats.
- Ensure accountability, availability, integrity and confidentiality of data.
- Guard against unauthorized access, alteration, disclosure or destruction of data and systems.
- Guard against accidental loss or destruction.

The District Information Security Management Program is committed to protecting information and information assets across the enterprise. Effective information security is a team effort involving participation and support of every District employee and contractor who interacts with data and systems. Therefore, it is the responsibility of every user to read and adhere to this policy and the procedures.

1.2. Definitions

- **Control:** A term describing any management, operational, or technical method that is used to manage risk.
- **Event:** An information security incident.
- **Information:** A definable piece of communication or representation of knowledge that has value to the organization. Examples of information include, but are not limited to the following: databases, data files, reports, documents, contracts, agreements, system documentation, research information, user manuals, training material, procedures, business continuity plans, audit trails, archived information, strategic plans or business implementation roadmaps.

POLICY


Policy Title: **Information Security Governance Policy**

Effective Date: September 13, 2017

Department: **Information Technology and Compliance**

Policy Number: IS1000

- **Information owner:** The party or parties accountable for ensuring the appropriate use of information—the person in the business that requires this information system. The information owner must be a District employee. (Compare to "information system owner".)
- **Information security:** A term that covers the protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional. Focus is on the confidentiality, integrity, and availability of data.
- **Information security incident:** Any incident that:
 - Compromises the confidentiality, integrity or availability of information.
 - Creates a potential threat for loss or disruption to business operations, reputation or assets.
 - Is a violation of security policies or general security practices.
- **Information system:** A discrete set of technology resources organized for the creation, storage, processing, transmission, use or disposal of information.
- **Information system owner:** The person in IT responsible for the information system architecture. (Compare to "information owner".)
- **Threats:** A threat is any circumstance or event with the potential to create loss. A threat can be a natural occurrence, technology, or physical failure, a person with intent to harm, or a person who unintentionally causes harm.
- **Vulnerabilities:** A vulnerability is a weakness in an information system, system security procedure, internal control, or implementation that could be exploited by a threat source. A technical vulnerability can be a flaw in hardware, firmware, or software that leaves an information system open to potential exploitation.

APPROVED BY	DATE
 _____ Darcy J. Davis, Chief Executive Officer	_____ 9-13-17 September 13, 2017
Committee: N/A _____	_____ N/A
Health Care District Board: _____	_____ September 13, 2017

POLICY

Policy Title: **Information Security Governance Policy**

Effective Date: September 13, 2017

Department: **Information Technology and Compliance**

Policy Number: IS1000

POLICY REVISION HISTORY

Original Policy Date

September 13, 2017

Revisions

"[Next Revised Policy Date]"	"[Next Revised Policy Date]"
"[Next Revised Policy Date]"	"[Next Revised Policy Date]"
"[Next Revised Policy Date]"	"[Next Revised Policy Date]"
"[Next Revised Policy Date]"	"[Next Revised Policy Date]"

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Instant Messaging**

Effective Date: 10/03/2018

Department: **Information Technology**

Policy Number: N/A

POLICY

The purpose of this policy is to prevent improper instant messaging communications and to avoid abuse and inappropriate use. Detailed information is presented to assist the organization's staff, provide guidelines for proper instant messaging and review penalties for improper use.

APPLICABILITY

This policy applies to all staff and contractors working on behalf of the Health Care District of Palm Beach County (HCD) and computer systems that access the Health Care District of Palm Beach County's Information Resources.

DEFINITIONS

- | | |
|------------------------|---|
| Instant Messaging (IM) | A type of online chat that offers real-time text transmission over the Internet or Intranet. Short messages are typically transmitted between two parties when each user chooses to complete a thought and select "send". |
| Cisco Jabber | Provides access presence, instant messaging (IM), voice, video, voice messaging, desktop sharing, and conferencing. |

PROCEDURE

Approved Messaging Application

The Health Care District of Palm Beach County Information Technology Department approves the use of only one specific instant messaging application, Cisco Jabber. The IT Department will install the instant messaging application on all applicable systems. The installation and use of any unauthorized instant messaging application are prohibited. All users, regardless of organization role, must obtain departmental approval prior to requesting any IM software or using an IM application on any HCD provided equipment.

Security

IM data should never be considered secure. If any user believes their instant messaging account is compromised, the user should cease using the account immediately and notify the IT department. The Information Technology department will assist users to determine whether an account is corrupt and properly secure the account for future use.

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Instant Messaging**

Effective Date: 10/03/2018

Department: **Information Technology**

Policy Number: N/A

Monitoring

Instant messaging offers an opportunity for non-authorized users to view or access HCD information, including proprietary, sensitive and confidential data. In order to properly audit and secure its network, systems, computers, and data, HCD may monitor and will archive instant messaging use. Users should have no expectation of privacy when using HCD owned devices or HCD provided instant messaging services.

Ownership

As a productivity enhancement tool, all instant messages (including backup and archive copies) sent or received using HCD provided systems become the Health Care District of Palm Beach County's property. If requested, employees must surrender all instant messages material in a timely manner and discontinue use of the HCD based accounts immediately upon request.

RESPONSIBILITY

Authorized Use

The organization's instant messaging systems should be used only for fulfilling business operations and job responsibilities. Under no circumstances should illegal, offensive, objectionable or inappropriate information or images be exchanged using organization-provided computers, instant messaging accounts or systems, networks, smartphones or text-messaging applications.

When using instant messaging services, all users should follow these guidelines:

- Do not discuss confidential, proprietary or sensitive organizational information.
- Do not open or accept attachments from any unauthorized user.
- Do not open or accept any suspicious or unexpected attachments.
- Never share patient's Protected Health Information (PHI) or Personally Identifiable Information (PII), credit card, financial, banking or similar information within an instant message.

Violations and Penalties

Violations of the Instant Messaging Policy could result in disciplinary action leading up to and including termination of employment and civil and/or criminal prosecution under federal and/or state laws.

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Instant Messaging**

Effective Date: 10/03/2018

Department: **Information Technology**

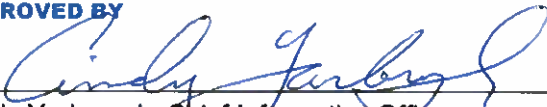

Policy Number: N/A

CROSS-REFERENCES

N/A

ADDENDA

N/A

APPROVED BY	DATE
 _____ Cindy Yarbrough, Chief Information Officer	10/3/18 _____
 _____ Darcy Davis, Chief Executive Officer	10-8-18 _____

PROCEDURE REVISION HISTORY

Original Procedure Date

10/03/2018

Revisions

Procedure Revision Date	Description of Changes

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Network Access and Authentication**

Effective Date: January 14, 2015

Department: **Information Technology**

Policy Number: N/A

POLICY

The Health Care District of Palm Beach County is hereinafter referred to as "the company."

Consistent standards for network access and authentication are critical to the company's information security and are often required by regulations or third-party agreements. Any user accessing the company's computer systems has the ability to affect the security of all users of the network. An appropriate Network Access and Authentication Policy reduces risk of a security incident by requiring consistent application of authentication and access standards across the network.

The purpose of this policy is to describe what steps must be taken to ensure that users connecting to the corporate network are authenticated in an appropriate manner, in compliance with company standards, and are given the least amount of access required to perform their job function. This policy specifies what constitutes appropriate use of network accounts and authentication standards.

APPLICABILITY

The scope of this policy includes all users who have access to company-owned or company-provided computers or require access to the corporate network and/or systems. This policy applies not only to employees, but also to guests, contractors, and anyone requiring access to the corporate network. Public access to the company's externally-reachable systems, such as its corporate website or public web applications, are specifically excluded from this policy.

DEFINITIONS

Antivirus Software	An application used to protect a computer from viruses, typically through real time defenses and periodic scanning. Antivirus software has evolved to cover other threats, including Trojans, spyware, and other malware.
Authentication	A security method used to verify the identity of a user and authorize access to a system or network.
Biometrics	The process of using a person's unique physical characteristics to prove that person's identity. Commonly used are fingerprints, retinal patterns, and hand geometry.
Encryption	The process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission or while stored.
Password	A sequence of characters that is used to authenticate a user to a file, computer, or network.

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title:	Network Access and Authentication	Effective Date:	January 14, 2015
Department:	Information Technology	Policy Number:	N/A

Also known as a passphrase or passcode.

Smart Card	A plastic card containing a computer chip capable of storing information, typically to prove the identity of the user. A card-reader is required to access the information.
Token	A small hardware device used to access a computer or network. Tokens are typically in the form of an electronic card or key fob with a regularly changing code on its display.

PROCEDURE

- During initial account setup, certain checks must be performed in order to ensure the integrity of the process. The following policies apply to account setup:
 - Positive ID and coordination with Human Resources is required.
 - Account creation and access rights granted will be documented and approved through official channels.
 - Users will be granted the least amount of network access required to perform his or her job function.
 - Users will be granted access only if he or she accepts the Acceptable Use Policy.
 - Access to the network will be granted in accordance with the Acceptable Use Policy.
 - Department Managers are ultimately responsible for determining access level and amount of access to information systems and data. This determination will be annotated in the appropriate form, i.e. URF, when creating new accounts

- Network accounts must be implemented in a standard fashion and utilized consistently across the organization. The following policies apply to account use:

- Accounts must be created using a standard format consisting of first initial- last name equaling eight characters total.

Accounts must be password protected (refer to the Password Policy for more detailed information).

- Accounts must be for individuals only. Account sharing is not permitted. Group accounts may be approved on a case by case basis.
- Generic logon IDs are not normally authorized. If they are required for network or system functionality, they will be kept to an absolute minimum.
- User accounts must not be given administrator or 'root' access unless this is necessary to perform his or her job function.

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Network Access and Authentication**

Effective Date: January 14, 2015

Department: **Information Technology**

Policy Number: N/A

- Occasionally guests will have a legitimate business need for access to the corporate network. When a reasonable need is demonstrated, temporary guest access is allowed. This access, however, must be severely restricted to only those resources that the guest needs at that time and disabled when the guest's work is completed. Guest account activations will be initiated after the proper request documentation has been completed, i.e. User Registration Form. Guest accounts will be automatically disabled after 90 days from activation unless otherwise noted for longer term guests.
- Individuals requiring access to confidential data must have an individual, distinct account. This account may be subject to additional monitoring or auditing at the discretion of the Chief Information Officer or executive team, or as required by applicable regulations or third-party agreements.
- When managing network and user accounts, it is important to stay in communication with the Human Resources department so that when an employee no longer works at the company, or has been transferred within the company, immediate actions can be taken. Human Resources must create a process to notify the IT Department in the event of a staffing change, which includes employment termination, employment suspension, or a change of job function (promotion, demotion, suspension, etc.). Access to account(s) must be modified, suspended, or disabled accordingly and immediately to ensure the confidentiality and integrity of the data the employee had previous access to. See the Termination and Transfer Procedure for detailed guidance.
- User machines must be configured to request authentication against the domain at startup. If the domain is not available or authentication for some reason cannot occur, then the machine should not be permitted to access the network.
- When accessing the network locally, username and password is an acceptable means of authentication. Usernames must be consistent with the requirements set forth in this document, and passwords must conform to the company's Password Policy.
- Remote access to the network can be provided for convenience to users but this comes with risk to security. For that reason, the company encourages additional scrutiny of users remotely accessing the network. The company's standards dictate that username and password is an acceptable means of authentication as long as appropriate policies are followed. Remote access must adhere to the Remote Access Policy.
- Screen lock out passwords offer an easy way to strengthen security by removing the opportunity for a malicious user, curious employee, or intruder to access network resources through an idle computer. For this reason screen lock outs are required to be activated after 20 minutes of inactivity. Some clinical applications may have custom policies approved by Senior Management on a case by case basis.

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Network Access and Authentication**

Effective Date: January 14, 2015

Department: **Information Technology**

Policy Number: N/A

Regardless of inactivity timeout, re-authentication to the domain with a password and/or ID badge is required to unlock the screen.

- If a user will not be using a system for a long period of time, i.e. several hours, overnight, or a weekend, they should consider logging out of the system completely but leaving the system powered on.
- Any system connecting to the network can have a serious impact on the security of the entire network. A vulnerability, virus, or other malware may be inadvertently introduced in this manner. For this reason, users must strictly adhere to corporate standards with regard to antivirus software and patch levels on their machines. Users must not be permitted network access if these standards are not met. This policy will be enforced with products that provide network admission control.
- Industry best practices state that username and password combinations must never be sent as plain text. If this information were intercepted, it could result in a serious security incident. Therefore, authentication credentials must be encrypted during transmission across any network, whether the transmission occurs internal to the company network or across a public network such as the Internet.
- Repeated logon failures can indicate an attempt to 'crack' a password and surreptitiously access a network account. In order to guard against password-guessing and brute-force attempts, the company must lock a user's account after 3 unsuccessful logins.

In order to protect against account guessing, when logon failures occur the error message transmitted to the user must not indicate specifically whether the account name or password were incorrect. The error can be as simple as "the username and/or password you supplied were incorrect."

- While some security can be gained by removing account access capabilities during non-business hours, the company does not mandate time-of-day lockouts. This may be either to encourage working remotely, or because the company's business requires all-hours access.
- This document is part of the company's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed

RESPONSIBILITY

This policy will be enforced by the Chief Information Officer and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Network Access and Authentication**

Effective Date: January 14, 2015

Department: **Information Technology**


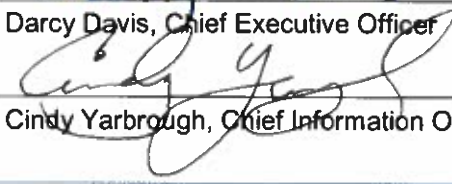
Policy Number: N/A

CROSS-REFERENCES

N/A

ADDENDA

N/A

APPROVED BY	DATE
 _____ Darcy Davis, Chief Executive Officer	_____
 _____ Cindy Yarbrough, Chief Information Officer	9/27/18

PROCEDURE REVISION OR REVIEWED HISTORY

Original Procedure Date	Reviewed or Revised	
March 12, 2014	1/14/2015 TFS	
	9/27/2018 CY	

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Network Security**

Effective Date: January 14, 2015

Department: **Information Technology**

Policy Number: N/A

POLICY

The Health Care District of Palm Beach County is hereinafter referred to as "the company."

The company wishes to provide a secure network infrastructure in order to protect the integrity of corporate data and mitigate risk of a security incident. While security policies typically avoid providing overly technical guidelines, this policy is necessarily a more technical document than most.

The purpose of this policy is to establish the technical guidelines for IT security, and to communicate the controls necessary for a secure network infrastructure. The network security policy will provide the practical mechanisms to support the company's comprehensive set of security policies. However, this policy purposely avoids being overly-specific in order to provide some latitude in implementation and management strategies.

APPLICABILITY

This policy covers all IT systems and devices that comprise the corporate network or that are otherwise controlled by the company.

DEFINITIONS

- ACL** A list that defines the permissions for use of, and restricts access to, network resources. This is typically done by port and IP address.
- Antivirus** An application used to protect a computer from viruses, typically through real time defenses and periodic scanning. Antivirus software has evolved to cover other threats, including Trojans, spyware, and other malware.
- Firewall** A security system that secures the network by enforcing boundaries between secure and insecure areas. Firewalls are often implemented at the network perimeter as well as in high-security or high-risk areas.
- IDS** Stands for Intrusion Detection System. A network monitoring system that detects and alerts to suspicious activities.
- IPS** Stands for Intrusion Prevention System. A networking monitoring system that detects and automatically blocks suspicious activities.

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Network Security** Effective Date: January 14, 2015
Department: **Information Technology** Policy Number: N/A

NTP	Stands for Network Time Protocol. A protocol used to synchronize the clocks on networked devices.
Password	A sequence of characters that is used to authenticate a user to a file, computer, network, or other device. Also known as a passphrase or passcode.
RAID	Stands for Redundant Array of Inexpensive Disks. A storage system that spreads data across multiple hard drives, reducing or eliminating the impact of the failure of any one drive.
Switch	A network device that is used to connect devices together on a network. Differs from a hub by segmenting computers and sending data to only the device for which that data was intended.
VLAN	Stands for Virtual LAN (Local Area Network). A logical grouping of devices within a network that act as if they are on the same physical LAN segment.
Virus	Also called a "Computer Virus." A replicating application that attaches itself to other data, infecting files similar to how a virus infects cells. Viruses can be spread through email or via network-connected computers and file systems.

PROCEDURE

- A compromised password on a network device could have devastating, network-wide consequences. Passwords that are used to secure these devices, such as routers, switches, and servers, must be held to higher standards than standard user-level or desktop system passwords. Accounts and passwords should be controlled from a central device, i.e. RADIUS, TACACS, LDAP, Directory services, etc. as much as possible.
- The following statements apply to the construction of passwords for network devices:
 - Passwords will be at least 12 characters
 - Passwords should be comprised of a mix of letters, numbers and special characters (punctuation marks and symbols)
 - Passwords must be comprised of a mix of upper and lower case characters
 - Passwords should not be comprised of, or otherwise utilize, words that can be found in a dictionary
 - Passwords should not be comprised of an obvious keyboard sequence (i.e., qwerty)
 - Passwords should not include "guessable" data such as personal information like birthdays, addresses, phone numbers, locations, etc.
- Repeated logon failures can indicate an attempt to 'crack' a password and surreptitiously access a network account. In order to guard against password-guessing and brute-force attempts, the company must lock a

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Network Security**

Effective Date: January 14, 2015

Department: **Information Technology**

Policy Number: N/A

user's account after 3 unsuccessful logins. This can be implemented as a time-based lockout or require a manual reset, at the discretion of the IT Manager.

In order to protect against account guessing, when logon failures occur the error message transmitted to the user must not indicate specifically whether the account name or password were incorrect. The error can be as simple as "the username and/or password you supplied were incorrect."

- Passwords must be changed according to the company's Password Policy. Additionally, the following requirements apply to changing network device passwords:
- If any network device password is suspected to have been compromised, all network device passwords must be changed immediately.
- If a company network or system administrator leaves the company, all passwords to which the administrator could have had access must be changed immediately. This statement also applies to any consultant or contractor who has access to administrative passwords.
- Vendor default passwords must be changed when new devices are put into service.

Passwords not controlled by a central device that are used on domain assets, stand-alone devices, and local accounts will be changed at least annually, semi-annually is preferred. This includes, but is not limited to:

- SNMP
 - Network infrastructure devices
 - Local administrator accounts
 - Service accounts
 - Wireless access devices
-
- Where passwords are used an application must be implemented that enforces the company's password policies on construction, changes, re-use, and lockout, i.e. RADIUS, TACACS, LDAP, Directory services, etc.
 - As a general rule, administrative (also known as "root") access to systems should be limited to only those who have a legitimate business need for this type of access. This is particularly important for network devices, since administrative changes can have a major effect on the network, and, as such, network security. All default root passwords must be changed from default. Additionally, administrative access to these systems must be logged.

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Network Security**

Effective Date: January 14, 2015

Department: **Information Technology**

Policy Number: N/A

- The logging of certain events is an important component of good network management practices. Logging needs vary depending on the type of network system, and the type of data the system holds. The following sections detail the company's requirements for logging and log review.
- Logs from application servers are of interest since these servers often allow connections from a large number of internal and/or external sources. These devices are often integral to smooth business operations.

Examples: Web, email, database servers, and health management systems.

Requirement: Logging must be enabled to the fullest degree possible. No passwords should be contained in logs.

- Logs from network devices are of interest since these devices control all network traffic, and can have a huge impact on the company's security.

Examples: Firewalls, network switches, routers, IDS, and IPS.

Requirement: Logging must be enabled to the fullest degree possible. No passwords should be contained in logs.

- Critical devices are any systems that are critically important to business operations. These systems may also fall under other categories above - in any cases where this occurs, this section shall supersede.

Examples: File servers, lab or manufacturing machines, systems storing intellectual property, and domain controllers.

Requirements: Logging must be enabled to the fullest degree possible. No passwords should be contained in logs.

- While logging is important to the company's network security, log management can become burdensome if not implemented appropriately. As logs grow, so does the time required to review the logs. For this reason, the company requires that a central log management application be utilized, i.e. a SIEM.
- Device logs do little good if they are not reviewed on a regular basis. Central log management applications can assist in highlighting important events, however, a member of the company's IT team must still review the logs at least once per week, daily is preferred.
- Device logs should be retained for a minimum of one year or longer if required for forensic investigation purposes. Unless otherwise determined by the IT manager, logs should be considered operational data.

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Network Security**

Effective Date: January 14, 2015

Department: **Information Technology**

Policy Number: N/A

- Firewalls are arguably the most important component of a sound security strategy. Internet connections and other unsecured networks must be separated from the company network through the use of a firewall.
- The following statements apply to the company's implementation of firewall technology:
 - Firewalls must provide secure administrative access (through the use of encryption) with management access limited to only networks where management connections would be expected to originate, i.e. internal LANs.
 - No unnecessary services or applications should be enabled on firewalls. The company should use 'hardened' systems for firewall platforms, or appliances.
 - Clocks on firewalls should be synchronized with the company's other networking hardware using NTP or another means. Among other benefits, this will aid in problem resolution and security incident investigation.
 - The firewall ruleset must be documented and audited quarterly. Audits must cover each rule, what it is for, if it is still necessary, and if it can be improved. If a rule is deemed no longer necessary or in use, it will either be disabled or deleted. If a rule allows more access than necessary, it will be strangled to the minimum necessary.
 - For its own protection, the firewall ruleset must include a "stealth rule," which forbids connections to the firewall itself.
 - The firewall must log dropped or rejected packets.
- Firewalls are often configured to block only inbound connections from external sources; however, by filtering outbound connections from the network, security can be greatly improved. This practice is also referred to as "Egress Traffic Filtering."

Blocking outbound traffic prevents users from accessing unnecessary, and many times, dangerous services. By specifying exactly what outbound traffic to allow, all other outbound traffic is blocked. This type of filtering could block root kits, viruses, and other malicious tools if a host were to become compromised.

The company requires that normal outbound traffic be limited to only known "good" services, examples of which are the following ports: 25, 53, 80, and 443. All other outbound traffic must be blocked at the firewall unless an exception is granted based on legitimate business purposes.

- Networking hardware, such as routers, switches, and access points, should be implemented in a consistent manner. The following statements apply to the company's implementation of networking hardware:
 - Networking hardware must provide secure administrative access (through the use of encryption)

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Network Security**

Effective Date: January 14, 2015

Department: **Information Technology**

Policy Number: N/A

with management access limited to only networks where management connections would be expected to originate, i.e. internal LANs.

- Clocks on all network hardware should be synchronized using NTP or another means. Among other benefits, this will aid in problem resolution and security incident investigation.
- If possible for the application, switches are required over hubs. When using switches the company should use VLANs to separate networks if it is reasonable and possible to do so.
- Access control lists must be implemented on network devices that prohibit direct connections to the devices. Connections to the router should be limited to the greatest extent possible. Exceptions to this are management connections that can be limited to known sources.
- Unused services and ports must be disabled on networking hardware.
- Access to administrative ports on networking hardware must be restricted to known management hosts and otherwise blocked with a firewall or access control list.
- When deploying networking hardware, a standardized hardening script will be followed to ensure consistent, secured devices across the environment.
- Vulnerability scanning of any new device before being placed into production is highly encouraged. Any major vulnerabilities discovered shall be remediated prior to the server being placed into production.
- Servers typically accept connections from a number of sources, both internal and external. As a general rule, the more sources that connect to a system, the more risk that is associated with that system, so it is particularly important to secure network servers. The following statements apply to the company's use of network servers:
 - Unnecessary files, services, and ports should be removed or blocked. If possible, follow a server-hardening guide, which is available from the leading operating system manufacturers.
 - Network servers, even those meant to accept public connections, must be protected by a firewall or access control list.
 - A standard, hardened installation process will be utilized for the company's network servers. This will provide consistency across servers no matter what employee or contractor handles the installation.
 - Clocks on network servers should be synchronized with the company's other networking hardware using NTP or another means. Among other benefits, this will aid in problem resolution and security

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Network Security**

Effective Date: January 14, 2015

Department: **Information Technology**

Policy Number: N/A

incident investigation.

- Vulnerability scanning of any new server before being placed into production is highly encouraged. Any major vulnerabilities discovered shall be remediated prior to the server being placed into production.
- Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) technology can be useful in network monitoring and security. The tools differ in that an IDS alerts to suspicious activity whereas an IPS blocks the activity. When tuned correctly, IDSs are useful but can generate a large amount of data that must be evaluated for the system to be of any use. IPSs automatically take action when they see suspicious events, which can be both good and bad, since legitimate network traffic can be blocked along with malicious traffic.

The company requires the use of an IDS and/or IPS on critical or high-risk network segments. If an IDS is used, procedures must be implemented to review and act on the alerts expediently. If an IPS is used, procedures must be implemented that provide a mechanism for emergency unblocking if the IPS obstructs legitimate traffic. Also, if an IPS is used, it should be audited and documented according to the standards detailed in the "Firewalls" section of this document.

- Security testing, also known as a vulnerability assessment, a security audit, or penetration testing, is an important part of maintaining the company's network security. Security testing can be provided by IT Staff members, but is often more effective when performed by a third party with no connection to the company's day-to-day Information Technology activities. The following sections detail the company's requirements for security testing.
- Internal security testing does not necessarily refer to testing of the internal network, but rather testing performed by members of the company's IT team. Internal testing should not replace external testing; however, when external testing is not practical for any reason, or as a supplement to external testing, internal testing can be helpful in assessing the security of the network.

Internal security testing is allowable, but only by employees whose job functions are to assess security, and only with permission of the IT Security Analyst and/or Chief Information Officer. Internal testing should have no measurable negative impact on the company's systems or network performance.

See the IT Security Internal Testing Procedure for further guidance.

- External security testing, which is testing by a third party entity, is an excellent way to audit the company's security controls. The IT Security Analyst and/or Chief Information Officer must determine to what extent this testing should be performed with regulatory compliance being a driving factor.

External testing must not negatively affect network performance or network security at any time.

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Network Security**

Effective Date: January 14, 2015

Department: **Information Technology**

Policy Number: N/A

As a rule, "penetration testing," which is the active exploitation of company vulnerabilities must not negatively impact company systems or data.

The company requires external security testing bi-annually at a minimum, annually is preferred, or after major system changes have occurred since the risk posture has changed. Furthermore, it is highly encouraged to contract a third party risk assessment / security test after a security event or incident.

- IT assets often contain sensitive data about the company's network which may include proprietary company information, information not publicly available, protected health information (HIPAA), financial information, Payment Card Industry (PCI) data, Personal Identification Information, and any other data that if released to unauthorized individuals, could cause harm to the company or its customer base. When such assets and the data they may contain are no longer needed the following guidelines must be followed:
 - Protecting devices containing sensitive data awaiting destruction, disposal, or reuse is of the utmost importance. Devices awaiting destruction, disposal, or reuse must be stored in locked rooms i.e., data centers, communication rooms, etc.
 - Any asset tags or stickers that identify the company must be removed before disposal.
 - Any configuration information must be removed by deletion or, if applicable, resetting the device to factory defaults.
 - Hard drives will be removed and disposed of properly or destroyed. See 4.8.1
 - At a minimum, data wiping must be used. Simply reformatting a drive or deleting data does not make the data unrecoverable. If wiping is used, the company must use the most secure commercially-available methods for data wiping. Alternatively, the company has the option of physically destroying the data storage mechanism from the device (such as its hard drive or solid state memory) or contracting with a third party to perform destruction.
 - In the case of rented or leased assets that are capable of data storage, i.e. copiers, scanners and printers, sanitization of the data storage mechanism must be ensured prior to returning the asset to the owner.
 - If an asset is damaged beyond repair, it must be assumed that the data on any storage mechanism may still be recoverable. The guidelines listed above still apply even though it may seem the asset is inoperable.
 - The company specifically directs users not to destroy data in violation of this policy. Particularly forbidden is destroying data that a user may feel is harmful to himself or herself, or destroying data

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Network Security**

Effective Date: January 14, 2015

Department: **Information Technology**

Policy Number: N/A

in an attempt to cover up a violation of law or company policy.

- Data storage media often contains sensitive company data which may include proprietary company information, information not publicly available, protected health information (HIPAA), financial information, Payment Card Industry (PCI) data, Personal Identification Information, and any other data that if released to unauthorized individuals, could cause harm to the company or its customer base. When such assets are to be reused, disposed of, or damaged beyond repair, the following guidelines must be followed:
 - Protecting storage media containing sensitive data awaiting destruction, disposal, or reuse is of the utmost importance. Devices awaiting destruction, disposal, or reuse must be stored in locked areas i.e., data centers, communication rooms, or lockable cabinets in the IT Department.
 - If locked, third party destruction specific containers are provided, they will be utilized for the destruction of storage media and the storage requirement above no longer applies. A log entry will be kept for every item of storage media slated for destruction or disposal to include date, type of media (model, etc.) serial number of the media, and by whom.
 - Hard drives, CDs, DVDs, floppy drives, magnetic tapes and flash drives will be physically destroyed, degaussed or properly disposed of utilizing authorized disposal methods when the media is no longer needed.
 - Hard drives, floppy drives, magnetic tapes and flash drives will be data wiped using the most secure commercially-available methods for data wiping if the media is intended to be reused or reimaged in the case of a workstation or laptop. Department of Defense standards of data wiping are recommended.
 - Only under extreme circumstances may a hard drive or other media storage device be sent to a third party for repair, data recovery, or an investigation. In such a case, the vendor must sign a non-disclosure agreement and the original media will be returned to the company.
 - The company specifically directs users not to destroy data in violation of this policy. Particularly forbidden is destroying data that a user may feel is harmful to himself or herself, or destroying data in an attempt to cover up a violation of law or company policy.
- Some data or assets must be retained in order to protect the company's interests, preserve evidence, and generally conform to good business practices. Some reasons for data retention include:
 - Litigation
 - Accident investigation

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Network Security**

Effective Date: January 14, 2015

Department: **Information Technology**

Policy Number: N/A

- Security incident investigation
- Regulatory requirements
- Intellectual property preservation
- Patient medical records preservation

If any of the above criteria apply, the storage requirements outlined in 4.8.1 will apply.

- IT must maintain a tracking record of the movements of hardware and electronic media. This record must include the name of the person responsible for the item (Dept. Manager), the location of the item, and any future movement of the item.
- Good network design is integral to network security. By implementing network compartmentalization, which is separating the network into different segments, the company will reduce its network-wide risk from an attack or virus outbreak. Further, security can be increased if traffic must traverse additional enforcement/inspection points. The company requires the following with regard to network compartmentalization:

- Higher Risk Network: Examples: Guest network, wireless network.

Requirements: Segmentation of higher risk networks from the company's internal network is highly encouraged but not required.

- Externally-Accessible Systems: Examples: Email servers, web servers.

Requirements: Segmentation of externally-accessible systems from the company's internal network is highly encouraged but not required.

- Internal Networks: Examples: Sales, Finance, Human Resources.

Requirements: Segmentation of internal networks from one another can improve security as well as reduce chances that a user will access data that he or she has no right to access. The company encourages, but does not require, such segmentation.

- Network documentation, specifically as it relates to security, is important for efficient and successful network management. Further, the process of regularly documenting the network ensures that the company's IT Staff has a firm understanding of the network architecture at any given time. The intangible benefits of this are immeasurable.

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Network Security**

Effective Date: January 14, 2015

Department: **Information Technology**

Policy Number: N/A

At a minimum, network documentation must include:

- Network diagram(s)
- System configurations
- Firewall ruleset
- IP Addresses
- Access Control Lists

The company requires that network documentation be performed and updated on a quarterly basis or as network changes take place.

- Computer viruses and malware are pressing concerns in today's threat landscape. If a machine or network is not properly protected, a virus outbreak can have devastating effects on the machine, the network, and the entire company. The company provides the following guidelines on the use of antivirus/anti-malware software:
 - All company-provided user workstations, servers, and mobile devices must have antivirus/anti-malware software installed.
 - Installed software must maintain a current "subscription" to receive patches and virus signature/definition file updates. Automatic or real time scanning should be enabled.
 - Antivirus signature file updates must be installed in a timely manner, either automatically or manually.
 - In addition to the workstation requirements, virus and malware scanning must be implemented at the Internet gateway to protect the entire network from inbound threats.
 - Users must not be able to disable malware software.
- Software applications can create risk in a number of ways, and thus certain aspects of software use must be covered by this policy. The company provides the following requirements for the use of software applications:
 - All software downloads, purchases, acquisitions, etc., will be vetted and approved by IT management.
 - Only legally licensed software may be used. Licenses for the company's software must be stored in a secure location.

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Network Security**

Effective Date: January 14, 2015

Department: **Information Technology**

Policy Number: N/A

- Open source and/or public domain software can only be used with the permission of the IT Manager.
- Software should be kept reasonably up-to-date by installing new patches and releases from the manufacturer.
- Vulnerability alerts should be monitored for all software products that the company uses. Any patches that fix vulnerabilities or security holes must be installed expediently.
- Certain tasks require that network devices be taken offline, either for a simple re-boot, an upgrade, or other maintenance. When this occurs, the IT Staff should perform the tasks before and after normal business hours. Tasks that are deemed "emergency support," as determined by the IT Manager, can be performed at any time.
- Out of date operating systems and third party software installed on those systems present one of the greatest dangers to technology security today. Many security vulnerabilities are taken advantage of and exploited by malicious actors because they are well known in the hacking community. By promptly patching systems and software when the patches are released by the manufacturers, the threat exposure can be greatly reduced.

Frequent patching of operating system software as well as third party installed software is required, preferably on a weekly basis, but required on a monthly basis at a minimum. IT management reserves the right to push critical or emergency patches outside of regularly scheduled patching as deemed appropriate.

Automated patching is highly encouraged as it takes the burden off administrators, however critical devices such as servers, databases, network devices, etc. should be manually patched since their functionality may be degraded by a patch that was not fully tested in a given unique environment. Manual patching of critical devices shall either take place on a monthly basis or as patches are released for individual operating systems.

- Documenting changes to network devices is a good management practice and can help speed resolution in the event of an incident. The IT Staff must document hardware and/or configuration changes to network devices in a "change log." Network devices must bear a sticker or tag indicating essential information, such as the device name, IP address, MAC address, asset information, and any additional data that may be helpful, such as information about cabling. See the Change Management Policy for further guidance.
- When a security incident is suspected that may impact a network device, the IT Staff should refer to the company's Incident Response Policy for guidance.

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Network Security**

Effective Date: January 14, 2015

Department: **Information Technology**

Policy Number: N/A

- Redundancy can be implemented on many levels, from redundancy of individual components to full site-redundancy. As a general rule, the more redundancy implemented, the higher the availability of the device or network, and the higher the associated cost. The company wishes to provide the IT Manager with latitude to determine the appropriate level of redundancy for critical systems and network devices. Redundancy should be implemented where it is needed, and should include some or all of the following:

- Hard drive redundancy, such as mirroring or RAID
- Server level redundancy, such as clustering or high availability
- Component level redundancy, such as redundant power supplies or redundant NICs
- Keeping hot or cold spares onsite
- Redundant WAN and LAN links

- Outdated products can result in a serious security breach. When purchasing critical hardware or software, the company must purchase a maintenance plan, support agreement, or software subscription that will allow the company to receive updates to the software and/or firmware for a specified period of time. The plan must meet the following minimum requirements:

Hardware: The arrangement must allow for repair/replacement of the device within an acceptable time period, as determined by the IT Manager, as well as firmware or embedded software updates.

Software: The arrangement must allow for updates, upgrades, and hotfixes for a specified period of time.

- It is the company's intention to comply with this policy not just on paper but in its everyday processes as well. With that goal in mind the company requires the following:
- The IT Security Analyst will be responsible for the company's compliance with this security policy and any applicable security regulations. This employee must be responsible for A) the initial implementation of the security policies, B) ensuring that the policies are disseminated to employees, C) training and retraining of employees on the company's information security program (as detailed below), D) any ongoing testing or analysis of the company's security in compliance with this policy, E) updating the policy as needed to adhere with applicable regulations and the changing information security landscape.
- A training program must be implemented that will detail the company's information security program to all users and/or employees covered by the policy, as well as the importance of data security. Employees must sign off on the receipt of, and in agreement to, the user-oriented policies. Re-training should be

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Network Security**

Effective Date: January 14, 2015

Department: **Information Technology**

Policy Number: N/A

performed at least quarterly.

- The company's security policies should be reviewed at least annually. Additionally, the policies should be reviewed when there is an information security incident or a material change to the company's security policies. As part of this evaluation the company should review:
 - Any applicable regulations for changes that would affect the company's compliance or the effectiveness of any deployed security controls.
 - If the company's deployed security controls are still capable of performing their intended functions.
 - If technology or other changes may have an effect on the company's security strategy.
 - If any changes need to be made to accommodate future IT security needs.
- This document is part of the company's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

RESPONSIBILITY


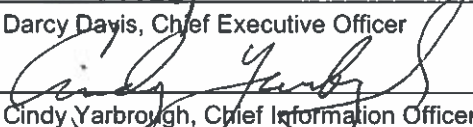
This policy will be enforced by the Chief Information Officer and/or executive team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities are suspected, the company may report such activities to the applicable authorities.

CROSS-REFERENCES

N/A

ADDENDA

N/A

APPROVED BY	DATE
 _____ Darcy Davis, Chief Executive Officer	_____
 _____ Cindy Yarbrough, Chief Information Officer	9/27/18 _____

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Network Security**

Effective Date: January 14, 2015

Department: **Information Technology**

Policy Number: N/A

PROCEDURE REVISION OR REVIEWED HISTORY

Original Procedure Date

Reviewed or Revised

March 12, 2014

1/14/2015 TFS	"[Next Revised Procedure Date]"
9/27/2018 CY	"[Next Revised Procedure Date]"
"[Next Revised Procedure Date]"	"[Next Revised Procedure Date]"
"[Next Revised Procedure Date]"	"[Next Revised Procedure Date]"

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Passwords**

Effective Date: January 14, 2015

Department: **Information Technology**

Policy Number: N/A

POLICY

The Health Care District of Palm Beach County is hereinafter referred to as "the company."

A solid password policy is perhaps the most important security control an organization can employ. Since the responsibility for choosing good passwords falls on the users, a detailed and easy-to-understand policy is essential.

The purpose of this policy is to specify guidelines for use of passwords. Most importantly, this policy will help users understand why strong passwords are a necessity, and help them create passwords that are both secure and useable. Lastly, this policy will educate users on the secure use of passwords.

APPLICABILITY

This policy applies to any person who is provided an account on the organization's network or systems, including: employees, guests, contractors, partners, vendors, etc.

DEFINITIONS

Authentication	A security method used to verify the identity of a user and authorize access to a system or network
Password	A sequence of characters that is used to authenticate user to a file, computer, network, or other device. Also known as a passphrase or passcode.
PIN	Personally Identifiable Number
SNMP	Simple Network Management Protocol
SSO	Single Sign-On
Two Factor Authentication	A means of authenticating a user that utilizes two methods: something the user has, and something the user knows. Examples are smart cards, tokens, badge taps, or biometrics, in combination with a password.

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Passwords**

Effective Date: January 14, 2015

Department: **Information Technology**

Policy Number: N/A

PROCEDURE

- The best security against a password incident is simple: following a sound password construction strategy. The organization mandates that users adhere to the following guidelines on password construction:
 - Passwords will be at least 12 characters, unless specific software doesn't support the District's password complexity methodology.
 - Passwords will be comprised of a mix of letters, numbers and special characters (punctuation marks and symbols).
 - Passwords will be comprised of a mix of upper and lower case characters.
 - Passwords should not be comprised of, or otherwise utilize, words that can be found in any dictionary.
 - Passwords should not be comprised of an obvious keyboard sequence (i.e., qwerty).
 - Passwords should not include "guessable" data such as personal information about yourself, your spouse or partner, your pet, your children, birthdays, addresses, phone numbers, locations, etc.
 - PIN length and complexity will be determined by the individual application or operating system.

Creating and remembering strong passwords does not have to be difficult. Substituting numbers for letters is a common way to introduce extra characters - a '3' can be used for an 'E,' a '4' can be used for an 'A,' or a '0' for an 'O.' Symbols can be introduced this way as well, for example an 'i' can be changed to a '!'

Another way to create an easy-to-remember strong password is to think of a sentence, and then use the first letter of each word as a password. The sentence: 'The quick brown fox jumps over the lazy dog!' easily becomes the password 'Tqbfjotld!' Of course, users may need to add additional characters and symbols required by the Password Policy, but this technique will help make strong passwords easier for users to remember.

- Passwords and PINs should be considered confidential data and treated with the same discretion as any of the organization's proprietary information. The following guidelines apply to the confidentiality of organization passwords and PINs:

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Passwords**

Effective Date: January 14, 2015

Department: **Information Technology**

Policy Number: N/A

- Users will not disclose their passwords or PINs to anyone.
 - Users will not share their passwords or PINs with others (co-workers, supervisors, family, etc.).
 - Users must not write down their passwords or PINs and leave them unsecured.
 - Users must not check the "save password" or "save PIN" box when authenticating to applications.
 - Users must not use the same password or PIN for different systems and/or accounts.
 - Users must not send passwords or PINs via email.
 - Users must not re-use passwords or PINs.
- In order to maintain good security, passwords should be periodically changed. This limits the damage an attacker can do as well as helps to frustrate brute force attempts. At a minimum, users must change passwords every 90 days. The organization may use software that enforces this policy by expiring users' passwords after this time period.
 - In the event that a user can't reset his or her password or unlock their account utilizing the SSO password reset function and contacts IT for a password reset or account unlock, the user's identity will be verified by IT personnel.
 - Since compromise of a single password can have a catastrophic impact on network security, it is the user's responsibility to immediately report any suspicious activity involving his or her passwords to the Help Desk. Any request for passwords over the phone or email, whether the request came from organization personnel or not, should be expediently reported. When a password is suspected to have been compromised the IT Manager will request that the user, or users, change all his or her passwords.
 - This document is part of the organization's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

RESPONSIBILITY

This policy will be enforced by the Chief Information Officer and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Passwords**

Effective Date: January 14, 2015

Department: **Information Technology**


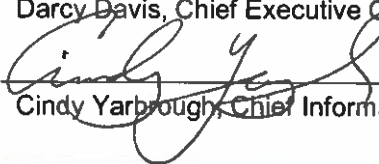
Policy Number: N/A

CROSS-REFERENCES

N/A

ADDENDA

N/A

APPROVED BY	DATE
 Darcy Davis, Chief Executive Officer	
 Cindy Yarbrough, Chief Information Officer	9/27/18

PROCEDURE REVISION OR REVIEWED HISTORY

Original Procedure Date	Reviewed or Revised	
March 12, 2014	1/14/2015 TFS	"[Next Revised Procedure Date]"
	9/27/2018 CY	"[Next Revised Procedure Date]"
	"[Next Revised Procedure Date]"	"[Next Revised Procedure Date]"
	"[Next Revised Procedure Date]"	"[Next Revised Procedure Date]"

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title:	Physical Security Policy	Effective Date:	January 14, 2015
Department:	Information Technology	Policy Number:	N/A

POLICY

The Health Care District of Palm Beach County is hereinafter referred to as "the company."

1.0 Overview

Information assets are necessarily associated with the physical devices on which they reside. Information is stored on workstations and servers and transmitted on the company's physical network infrastructure. In order to secure the company data, thought must be given to the security of the company's physical Information Technology (IT) resources to ensure that they are protected from standard risks.

2.0 Purpose

The purpose of this policy is to protect the company's physical information systems by setting standards for secure operations.

3.0 Scope

This policy applies to the physical security of the company's information systems, including, but not limited to, all company-owned or company-provided network devices, servers, personal computers, mobile devices, and storage media. Additionally, any person working in or visiting the company's office is covered by this policy.

Please note that this policy covers the physical security of the company's Information Technology infrastructure, and does not cover the security of non-IT items or the topic of employee security. While there will always be overlap, care must be taken to ensure that this policy is consistent with any existing physical security policies.

4.0 Policy

4.1 Access Controls

Access controls are necessary to restrict entry to the company data centers and communications areas to only approved persons. There are several standard ways to do this, which are outlined in this section, along with the company's guidelines for their use.

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title:	Physical Security Policy	Effective Date:	January 14, 2015
Department:	Information Technology	Policy Number:	N/A

4.1.1 Keys & Keypads

The use of keys and keypads is acceptable, as long as keys are marked "do not duplicate" and their distribution is limited. These security mechanisms are the most inexpensive and are the most familiar to users. The disadvantage is that the company has no control, aside from changing the locks or codes, over how and when the access is used. Keys can be copied and keypad codes can be shared or seen during input. However, used in conjunction with another security strategy, such as an alarm system, good security can be obtained with keys and keypads.

4.1.2 Keycards & Biometrics

Keycards and biometrics are allowable forms of access controls. At a minimum, all data centers will utilize keycard badge access with logging of entry enabled.

Keycards and biometrics have an advantage over keys in that access policies can be tuned to the individual user and movements of individuals can be logged for auditing purposes. Schedules can be set to forbid off-hours access, or forbid users from accessing a security zone where they are not authorized. Perhaps best of all, these methods allow for control over exactly who possesses the credentials. If a keycard is lost or stolen it can be immediately disabled. If an employee is terminated or resigns, that user's access can be disabled. The granular control offered by keycards and biometrics make them appealing access control methods.

4.1.3 Alarm System

A security alarm system is a good way to minimize risk of theft, or reduce loss in the event of a theft. The company does use an alarm system.

4.2 Physical Data Security

Certain physical precautions must be taken to ensure the integrity of the company's data. At a minimum, the following guidelines must be followed:

- Computer screens must be positioned where information on the screens cannot be seen by outsiders.
- Confidential and sensitive information must not be displayed on a computer screen where the screen can be viewed by those not authorized to view the information.
- Users must log off their workstations when leaving for an extended time period or at the end of the workday. At a minimum, users must lock their workstations when leaving for a shorter period of time. For shared

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title:	Physical Security Policy	Effective Date:	January 14, 2015
Department:	Information Technology	Policy Number:	N/A

resources such as medication dispensing and electronic health record workstations that stay logged in for extended periods of time, physical security of the device must be ensured when it is not in use.

- Network cabling must not run through non-secured areas unless the cabling is carrying only public data (i.e., extended wiring for an Internet circuit).
- Network ports that are not in use must be disabled.

4.3 Physical System Security

In addition to protecting the data on the company's information technology assets, this policy provides the guidelines below on keeping the systems themselves secure from damage or theft.

4.3.1 Minimizing Risk of Loss and Theft

In order to minimize the risk of data loss through loss or theft of company property, the following guidelines must be followed:

- **Unused systems:** If a system is not in use for an extended period of time it should be moved to a secure area or otherwise secured.
- **Mobile devices:** Special precautions must be taken to prevent loss or theft of mobile devices. Refer to the company's Mobile Device Policy for guidance.
- **Systems that store confidential data:** Special precautions must be taken to prevent loss or theft of these systems. Refer to the company's Network Security Policy for guidance.

4.3.2 Minimizing Risk of Damage

Systems that store company data are often sensitive electronic devices that are susceptible to being inadvertently damaged. In order to minimize the risk of damage, the following guidelines must be followed:

- **Environmental controls** should keep the operating environment of company systems within standards specified by the manufacturer. These standards often involve, but are not limited to, temperature and humidity.
- **Proper grounding procedures** must be followed when opening system cases. This may include use of a grounding wrist strap or other means to ensure that the danger from static electricity is minimized.

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Physical Security Policy** Effective Date: January 14, 2015

Department: **Information Technology** Policy Number: N/A

- Strong magnets must not be used in proximity to company systems or media.
- Except in the case of a fire suppression system, open liquids must not be located near company systems. Food and beverages will not be consumed near company systems or in data center / communications rooms.
- Uninterruptible Power Supplies (UPSs) and/or surge-protectors are required for important systems and encouraged for all systems. These devices should carry a warranty that covers the value of the systems if the systems were to be damaged by a power surge.
- It is recommended that Data Centers and communications closets not be used for storage of any kind, to include spare equipment and supplies, as this may affect HVAC circulation of cooling air.

4.4 Fire Prevention

It is the company's policy to provide a safe workplace that minimizes the risk of fire. In addition to the danger to employees, even a small fire can be catastrophic to computer systems. Further, due to the electrical components of IT systems, the fire danger in these areas is typically higher than other areas of the company's office. The guidelines below are intended to be specific to the company's information technology assets and should conform to the company's overall fire safety policy.

- Fire, smoke alarms, and/or suppression systems must be used, and must conform to local fire codes and applicable ordinances.
- Electrical outlets must not be overloaded. Users must not chain multiple power strips, extension cords, uninterruptible power supplies, or surge protectors together.
- Extension cords, surge protectors, power strips, and uninterruptible power supplies must be of the three-wire/three-prong variety.
- Only electrical equipment that has been approved by Underwriters Laboratories and bears the UL seal of approval must be used.
- Unused electrical equipment should be turned off when not in use for extended periods of time if possible.
- Periodic inspection of electrical equipment must be performed. Power cords, cabling, and other

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title:	Physical Security Policy	Effective Date:	January 14, 2015
Department:	Information Technology	Policy Number:	N/A

electrical devices must be checked for excessive wear or cracks. If overly-worn equipment is found, the equipment must be replaced or taken out of service immediately depending on the degree of wear.

- A smoke alarm monitoring service may be used that will alert a designated company employee if an alarm is tripped during non-business hours.

4.5 Entry Security

From time to time, the company may have outside IT or telecommunications professionals on company premises. Monitoring those who enter and exit the premises is a good security practice in general, but is particularly true for minimizing risk to company systems and data. The guidelines below are intended to be specific to the company's information technology assets and should conform to the company's overall security policy.

4.5.1 Use of Identification Badges

Identification (ID) badges are useful to identify authorized persons on the company premises. The company has established the following guidelines for the use of ID badges.

- Non-employees/Visitors: Visitor badges are required. If possible, specific, non-generic, badges should identify visitors by name.
- Visitors must report a lost or stolen badge immediately.

4.5.2 Sign-in Requirements

The company must maintain a sign-in log (or similar device) in the lobby or entry area and visitors must be required to sign in upon arrival. At minimum, the register must include the following information: visitor's name, company name, reason for visit, name of person visiting, sign-in time, and sign-out time.

4.5.3 Visitor Access

Visitors should be given only the level of access to the company premises that is appropriate to the reason for their visit. After checking in, visitors must be escorted unless they are considered "trusted" by the company.

4.6 Applicability of Other Policies

This document is part of the company's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title:	Physical Security Policy	Effective Date:	January 14, 2015
Department:	Information Technology	Policy Number:	N/A

5.0 Enforcement

This policy will be enforced by the Chief Information Officer and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

6.0 Review and/or Revisions

This policy will be reviewed and edited if applicable at a minimum per annum or when changes are required that affect how this policy is applied and enforced. All modifications will be recorded in the Change Log at the end of this document.

7.0 Definitions

Biometrics - The process of using a person's unique physical characteristics to prove that person's identity. Commonly used are fingerprints, retinal patterns, and hand geometry.

Datacenter - A location used to house a company's servers or other information technology assets. Typically offers enhanced security, redundancy, and environmental controls.

Keycard - A plastic card that is swiped, or that contains a proximity device, that is used for identification purposes. Often used to grant and/or track physical access.

Keypad - A small keyboard or number entry device that allows a user to input a code for authentication purposes. Often used to grant and/or track physical access.

Mobile Device - A portable device that can be used for certain applications and data storage. Examples are PDAs or Smartphones.


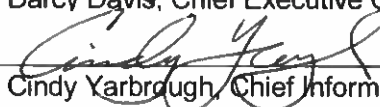
PDA - Stands for Personal Digital Assistant. A portable device that stores and organizes personal information, such as contact information, calendar, and notes.

Smartphone - A mobile telephone that offers additional applications, such as PDA functions and email.

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: Physical Security Policy	Effective Date: January 14, 2015
Department: Information Technology	Policy Number: N/A

Uninterruptible Power Supplies (UPSs) - A battery system that automatically provides power to electrical devices during a power outage for a certain period of time. Typically also contains power surge protection.

APPROVED BY	DATE
 Darcy Davis, Chief Executive Officer	<u>10-29-18</u>
 Cindy Yarbrough, Chief Information Officer	<u>10/12/18</u>

PROCEDURE REVISION OR REVIEWED HISTORY

Original Procedure Date

March 12, 2014

Reviewed or Revised

1/14/2015 TFS	"[Next Revised Procedure Date]"
10/12/2018 CY	"[Next Revised Procedure Date]"
"[Next Revised Procedure Date]"	"[Next Revised Procedure Date]"
"[Next Revised Procedure Date]"	"[Next Revised Procedure Date]"
"[Next Revised Procedure Date]"	"[Next Revised Procedure Date]"

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title:	Remote Access Policy	Effective Date:	January 14, 2015
Department:	Information Technology	Policy Number:	N/A

POLICY

The Health Care District of Palm Beach County is hereinafter referred to as "the company."

1.0 Overview

It is often necessary to provide access to corporate information resources to employees or others working outside the company's network. While this can lead to productivity improvements it can also create certain vulnerabilities if not implemented properly. The goal of this policy is to provide the framework for secure remote access implementation.

2.0 Purpose

This policy is provided to define standards for accessing corporate information technology resources from outside the network. This includes access for any reason from the employee's home, remote working locations, while traveling, etc. The purpose is to define how to protect information assets when using an insecure transmission medium.

3.0 Scope

The scope of this policy covers all employees, contractors, and external parties that access company resources over a third-party network, whether such access is performed with company-provided or non-company-provided equipment.

4.0 Policy

4.1 Prohibited Actions

Remote access to corporate systems is only to be offered through a company-provided means of remote access in a secure fashion. The following are specifically **prohibited**:

- Installing a modem, router, or other remote access device on a company system without the approval of the Chief Information Officer .

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: Remote Access Policy	Effective Date: January 14, 2015
Department: Information Technology	Policy Number: N/A

- Remotely accessing corporate systems with a remote desktop tool, such as Citrix, or RDP without the written approval from a department manager and the IT Director of Software Support.
- If the use of remote desktop tools has been authorized, remoting to a user's device without the user knowing and approving of the remote access each time remote access is initiated.
- Use of non-company-provided remote access software.
- Split Tunneling to connect to an insecure network (the internet) in addition to the corporate network, or in order to bypass security restrictions.

4.2 Use of Non-company-provided Machines

Accessing the corporate network through home or public machines can present a security risk, as the company cannot completely control the security of the system accessing the network. Use of non-company-provided machines to access the corporate network is permitted as long as this policy is adhered to, and as long as the machine meets the following criteria:

- It has up-to-date antivirus software installed
- Its software patch levels are current

If any of the above conditions can't be met, the company may provide guidance and/or assistance with commercially available or open source products to ensure the security of the machine.

When accessing the network remotely, users will not store confidential information on home or public hard drives.

4.3 Client Software

The company will supply users with remote access software that allows for secure access and enforces the remote access policy. The software will provide traffic encryption in order to protect the data during transmission as well as a firewall that protects the machine from unauthorized access. Two factor authentication software will be used to access Health Care District systems remotely through the Virtual Private Network (VPN). Additional VPN procedures can be found in the VPN Policy.

4.4 Network Access

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title:	Remote Access Policy	Effective Date:	January 14, 2015
Department:	Information Technology	Policy Number:	N/A

There are no restrictions on what information or network segments company employees can access when working remotely, however the level of access should not exceed the access a user receives when working in the office. Vendors and Business Associates will be granted access to only those resources required to conduct business on behalf of the company.

4.5 Idle Connections

Due to the security risks associated with remote network access, it is a good practice to dictate that idle connections be timed out periodically.

4.6 Applicability of Other Policies

This document is part of the company's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

5.0 Enforcement

This policy will be enforced by the Chief Information Officer and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

6.0 Review and/or Revisions

This policy will be reviewed and edited if applicable at a minimum per annum or when changes are required that affect how this policy is applied and enforced. All modifications will be recorded in the Change Log at the end of this document.

7.0 Definitions

Modem - A hardware device that allows a computer to send and receive digital information over a telephone line.

Remote Access - The act of communicating with a computer or network from an off-site location. Often performed by home-based or traveling users to access documents, email, or other resources at a main site.


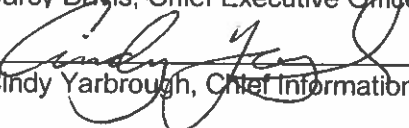
Split Tunneling - A method of accessing a local network and a public network, such as the Internet, using the same connection at the same time.

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: Remote Access Policy	Effective Date: January 14, 2015
Department: Information Technology	Policy Number: N/A

Timeout - A technique that drops or closes a connection after a certain period of inactivity.

Two Factor Authentication - A means of authenticating a user that utilizes two methods: something the user has, and something the user knows. Examples are smart cards, tokens, or biometrics, in combination with a password.

APPROVED BY	DATE
 Darcy Davis, Chief Executive Officer	10-29-18
 Cindy Yarbrough, Chief Information Officer	10/10/18

PROCEDURE REVISION OR REVIEWED HISTORY

Original Procedure Date	Reviewed or Revised	
March 12, 2014	1/14/2015 TFS	"[Next Revised Procedure Date]"
	10/15/2018 CY	"[Next Revised Procedure Date]"
	"[Next Revised Procedure Date]"	"[Next Revised Procedure Date]"
	"[Next Revised Procedure Date]"	"[Next Revised Procedure Date]"
	"[Next Revised Procedure Date]"	"[Next Revised Procedure Date]"

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Removable Media**

Effective Date: 10/03/2018

Department: **Information Technology**

Policy Number: N/A

POLICY

The purpose of this policy is to minimize the risk of loss or exposure of sensitive information maintained by the Health Care District of Palm Beach County (HCD) and to reduce the risk of acquiring malware infections on systems operated by the Health Care District of Palm Beach County.

The Health Care District of Palm Beach County staff and contractors working on behalf of HCD may only use HCD assigned removable media DataLocker USB drives on their work computers. These drives may not be connected to or used in computers that are not owned by the Health Care District of Palm Beach County. Sensitive information should only be stored on removable media when required in the performance of your assigned duties. When sensitive information is stored on removable media it must be encrypted.

APPLICABILITY

This policy applies to all staff, contractors working on behalf of HCD and computer systems that access the Health Care District of Palm Beach County's Information Resources.

DEFINITIONS

- Encryption** A procedure used to convert data from its original form to a format that is unreadable and unusable to anyone without the tools and information needed to reverse the encryption process.
- Malware** Software of malicious intent or impact such as viruses, worms, and spyware.
- Removable Media** A device or media that is readable and/or writeable by the end user and is able to be moved from computer to computer without modification to the computer. This includes, but is not limited to, flash memory devices such as thumb drives, cameras; removable hard drives (including hard drive-based MP3 players); optical disks such as CD and DVD disks; mobile devices such as smartphones and tablets; floppy disks and any commercial music and software disks not provided by HCD.
- USB** A Universal Serial Bus (USB) is a common interface that enables communication between devices and a host controller such as a personal computer (PC). It connects peripheral devices such as digital cameras, mice, keyboards, printers, scanners, media devices, external hard drives, and flash drives.

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Removable Media**

Effective Date: 10/03/2018

Department: **Information Technology**

Policy Number: N/A

PROCEDURE

- Explicit approval shall be obtained by submitting a User Registration Form (URF) and approved by an Executive Officer and the IT Department.
- Group Policy Object (GPO) will control what USB devices will be allowed based on class ID and/or hardware ID. The hardware ID for the DataLocker devices will be allowed and the class ID's for mice, keyboards, scanners, and other identified peripherals will be allowed for use on HCD workstations and or laptops.
- The cloud version of safe console will be used to manage the DataLocker USB devices. The cloud version of safe console identifies the HCD network based on our public IP (internet protocol) addresses. The default policy allows the devices to be used on the trusted network for HCD as identified by HCD's public IP addresses.
- When the computer is not in the HCD network, you must be connected via VPN to use the DataLocker USB device.
- Password policy is currently set at 12 characters long and requires 1 each of alpha-numeric characters, upper case, lower case, and special characters be part of the password. The password will expire in 90 days and will need to be reset by the user when prompted.
- The Helpdesk will have the ability to remotely reset the DataLocker USB device passwords in case the user forgets the password. Users will be able to request the password reset from the safe console application located on the USB device, which will generate a ticket to the Helpdesk, who can then reset the password on the device and email the user the reset codes.
- The following file types will be restricted from being saved to the device: .exe, .dll, .com, .bat, .js, .jse, .msi, .msp, .ocx, .reg, .sct, .scr, .sys, .vb, .vbe, .vbs, .wsc, .wsf, except for the IT Department.
- Devices will be audited for connections to a machine, failed login attempts and password resets.
- The name of files saved and removed to the device will be logged.
- After 30 minutes of inactivity, the device will lock itself, requiring the password to unlock it.
- If 30 days have passed since the device was last used, the device will issue a warning and will connect to the safe server console. This will just be a warning to the user, and the device will still be usable. The Helpdesk will change the status back to "in use".

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Removable Media**

Effective Date: 10/03/2018

Department: **Information Technology**

Policy Number: N/A

- IT can reset the device to factory default settings remotely which will wipe all data off the device the next time it is connected to any workstation with an internet connection.
- Devices will be assigned to approved users. After submitting a URF form, users will need to complete an equipment sign out form. When a user is terminated, the device should be returned and reset to factory defaults.
- If the DataLocker USB drive is lost, stolen or damaged, it should be reported to the IT Help Desk as soon as possible. The user will be responsible for the cost of the device replacement, as specified on the equipment sign out form.

RESPONSIBILITY

Operations Manager

- Ensure this document remains current and is updated whenever changes to this policy occur
- Review and approve changes to this document

Chief Information Officer

- Review and approve changes to this document

CROSS-REFERENCES

N/A

ADDENDA

N/A



DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Removable Media**

Effective Date: 10/03/2018

Department: **Information Technology**

Policy Number: N/A

APPROVED BY	DATE
 Cindy Yarbrough, Chief Information Officer	<u>10/3/18</u>
 Darcy J. Davis, Chief Executive Officer	<u>10-8-18</u>

PROCEDURE REVISION HISTORY

Original Procedure Date

10/03/2018

Revisions

Procedure Date	Description of Changes

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Security Awareness
Program Procedure**

Effective Date: September 13, 2013

Department: **Information Technology**

Policy Number: N/A

The Health Care District of Palm Beach County is hereinafter referred to as "the company."

POLICY

The purpose of this procedure is to protect the company's information systems and data by setting standards for the continual education of users.

People are one of the weakest links in attempts to secure systems and networks. The "people factor" - not technology - is key to providing an adequate and appropriate level of security. If people are the key, but are also a weak link, more and better attention must be paid to this "asset." A robust and enterprise wide awareness program is paramount to ensuring that people understand their IT security responsibilities, organizational policies, how to properly use and protect the IT resources entrusted to them, and how to report or respond to security concerns.

APPLICABILITY

The scope of this procedure primarily applies to those charged with providing an ongoing User Security Awareness Program for all company employees. This responsibility currently falls on the IT Security Analyst.

The scope of this procedure also applies to all company personnel as they are the recipients of the awareness training.

This procedure will be reviewed and edited if applicable at a minimum per annum or when changes are required that affect how this policy is applied and enforced. All modifications will be recorded in the Change Log at the end of this document.

DEFINITIONS

N/A

PROCEDURE

The following lists criteria for implementing a successful user security awareness program:

1. Select awareness topics. Educate the audience on company IT security policies and their responsibilities to protect assets and data. Select topics that are relevant to current technologies, current malware trends, and current methodologies of data loss. Also consider how topics applied to the workplace can be applied to the users' personal life.
2. Management approval. Confer with the Chief Information Officer and/or Executive Management on individual topics for approval. Management support and approval is paramount to the success of the

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Security Awareness
Program Procedure**

Effective Date: September 13, 2013

Department: **Information Technology**

Policy Number: N/A

success of the program.

3. Find sources of awareness material. Utilize all sources of material, free as well as commercially available.
4. Develop and implement relevant material using a variety of methods. Make the training simple, interesting, and fun for the user; he or she is more likely to retain the material if they find it interesting and they are able to apply the material to everyday life.
5. Distribute the material. Mass emailing of all employees and posting of security reminders on intranet sites is the best way to reach everyone considering our distributed workforce. Consider distributing flyers or posting flyers in spaces employees frequent. Conducting in-person training to groups may be an option, time permitting. Information can also be posted on our digital communication monitors.
6. Reinforce concepts. A successful program should reach out to employees often. The more a user knows, the more that user can contribute to network defense. Monthly distribution of security awareness materials should be enough to educate users without flooding them with too much information they might otherwise ignore. Reinforce concepts by repeating them every few months.
7. Update and improve the focus of the training as technology advances and organizational priorities change. Technology does not stand still, neither should the topics presented.
8. Logging. Develop a schedule of planned awareness events. Keep a detailed log of previously completed subjects, method of delivery, and delivery dates.
9. Evaluation and Feedback. Consider contacting selected users for feedback on the awareness subjects and delivery methods for possible opportunities for improvement in the program.

RESPONSIBILITY

The IT Security Analyst is responsible for administering as well as ensuring compliance with this procedure. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

CROSS-REFERENCES

45 CFR § 164.308(a)(5)

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Security Awareness Program Procedure**


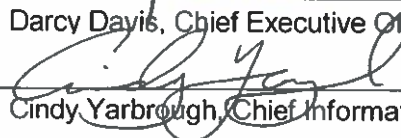
Effective Date: September 13, 2013

Department: **Information Technology**

Policy Number: N/A

ADDENDA

N/A

APPROVED BY	DATE
 Darcy Davis, Chief Executive Officer	10-29-18
 Cindy Yarbrough, Chief Information Officer	10/16/18

PROCEDURE REVISION OR REVIEWED HISTORY

Original Procedure Date	Reviewed or Revised	
September 13, 2013	10/10/2014 TFS	"[Next Revised Procedure Date]"
	10/16/2018 CY	"[Next Revised Procedure Date]"
	"[Next Revised Procedure Date]"	"[Next Revised Procedure Date]"
	"[Next Revised Procedure Date]"	"[Next Revised Procedure Date]"
	"[Next Revised Procedure Date]"	"[Next Revised Procedure Date]"

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Termination and Transfer** Effective Date: January 8, 2014

Department: **Information Technology** Policy Number: N/A

The Health Care District of Palm Beach County is hereinafter referred to as "the company."

POLICY

When an employee, vendor, contractor, or business associate either resigns, is terminated, transfers within or between departments, or the relationship with the company ceases, IT must review the user's account(s) in regards to access rights, data, files, and systems used during his/her employment or relationship with the company and either terminate or modify those access rights.

Coordination with Human Resources and the affected Business Unit(s) is imperative for the timely execution of the required actions listed below.

APPLICABILITY

The scope of this procedure applies to all personnel who are responsible for creating, modifying, or deleting user accounts or user access to company data and information systems.

This procedure will be reviewed and edited if applicable at a minimum per annum or when changes are required that affect how this policy is applied and enforced. All modifications will be recorded in the Change Log at the end of this document.

DEFINITIONS

N/A

PROCEDURE

1. Terminations and/or Resignations:

- a. After receipt of a User Registration Form (URF) or direct notification from Human Resources or senior management, inventory all systems, network devices, applications and data that the user had access to.
- b. Immediately disable all user and administrative accounts.
- c. Remove all security groups from the user's Active Directory Profile except for "Domain User".
- d. Move the account to the appropriate Active Directory Organizational Unit (OU), i.e. Terminated employees.
- e. If improper behavior is suspected on systems the user had access to, confiscation of the systems may be required.
- f. If the user had Virtual Private Network (VPN) accounts or remote access separate from Microsoft or

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Termination and Transfer**

Effective Date: January 8, 2014

Department: **Information Technology**

Policy Number: N/A

Citrix, disable the account or change the VPN Pre-Share Key.

- g. Hide the user's Exchange mailbox from public view. The mailbox may be deleted soon thereafter or the mailbox may be left operational based on administrative or business need. There may also be a need to forward emails to another user. Coordinate with the business unit manager if this will be required.
- h. Document and complete the URF with all actions accomplished.
- i. Remove access of the user's mobile device(s) from the Mobile Device Management environment by performing an "enterprise" or "corporate" wipe. Do not perform a full "device wipe".

2. Transfers Within or Between Departments

- a. After receipt of a URF, inventory all systems, network devices, applications and data that the user had access to.
- b. Remove all security groups from the user's Active Directory Profile that are no longer required for the user's former position.
- c. Remove access to any systems, applications, network devices, and data that the user no longer requires access to.
- d. Add the security groups to the user's Active Directory Profile that are now required for the user to perform the responsibilities of the new position. Add any new access to systems not controlled by Active Directory that is required for the user's new position.
- e. The responsible Business Owner is ultimately responsible for the verification of the proper access rights. This procedure can be referenced in the User Account Review Policy.
- f. If the user had mobile device access to the corporate environment and he or she no longer requires that access, remove access of the user's mobile device(s) from the Mobile Device Management environment by performing an "enterprise" or "corporate" wipe. Do not perform a full "device wipe". If the user requires mobile device access to the corporate environment in their new role, follow the appropriate enrollment for the device(s).

RESPONSIBILITY

The Chief Information Officer is responsible for administering as well as ensuring compliance with this procedure. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Termination and Transfer** Effective Date: January 8, 2014


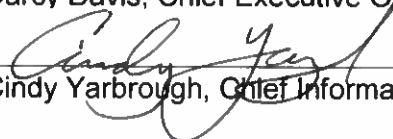
Department: **Information Technology** Policy Number: N/A

applicable authorities.

CROSS-REFERENCES

ADDENDA

N/A

APPROVED BY	DATE
 Darcy Davis, Chief Executive Officer	10-29-18
 Cindy Yarbrough, Chief Information Officer	10/16/18

PROCEDURE REVISION OR REVIEWED HISTORY

Original Procedure Date	Reviewed or Revised	
January 8, 2018	10/13/2014 TFS	"[Next Revised Procedure Date]"
	10/16/2018 CY	"[Next Revised Procedure Date]"
	"[Next Revised Procedure Date]"	"[Next Revised Procedure Date]"
	"[Next Revised Procedure Date]"	"[Next Revised Procedure Date]"
	"[Next Revised Procedure Date]"	"[Next Revised Procedure Date]"

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title:	Third Party Connection Policy	Effective Date:	January 14, 2015
Department:	Information Technology	Policy Number:	N/A

- Connections to third parties must use a firewall or Access Control List (ACL) to separate the company's network from the third party's network.
- Third parties will be provided only the minimum access necessary to perform the function requiring access. If possible this should include time-of-day restrictions to limit access to only the hours when such access is required.
- Wherever possible, systems requiring third party access should be placed in a public network segment or demilitarized zone (DMZ) in order to protect internal network resources.
- If a third party connection is deemed to be a serious security risk, the Chief Information Officer will have the authority to prohibit the connection. If the connection is absolutely required for business functions, additional security measures should be taken at the discretion of the Chief Information Officer.

4.3 Restricting Third Party Access

Best practice for a third party connection requires that the link be held to higher security standards than an intra-company connection. As such, the third party must agree to:

- Restrict access to the company's network to only those users that have a legitimate business need for access.
- Supply the company with on-hours and off-hours contact information for the person or persons responsible for the connection.
- (If confidential data is involved) provide the company with the names and any other requested information about individuals that will have access to the company's confidential data. The steward or owner of the confidential data will have the right to approve or deny this access.

4.4 Auditing of Connections

In order to ensure that third-party connections are in compliance with this policy, they must be audited periodically.

4.5 Applicability of Other Policies

This document is part of the company's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title:	Third Party Connection Policy	Effective Date:	January 14, 2015
Department:	Information Technology	Policy Number:	N/A

5.0 Enforcement

This policy will be enforced by the Chief Information Officer and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

6.0 Review and/or Revisions

This policy will be reviewed and edited if applicable at a minimum per annum or when changes are required that affect how this policy is applied and enforced. All modifications will be recorded in the Change Log at the end of this document.

7.0 Definitions

Access Control List (ACL) - A list that defines the permissions for use of, and restricts access to, network resources. This is typically done by port and IP address.

Demilitarized Zone (DMZ) - A perimeter network, typically inside the firewall but external to the private or protected network, where publicly-accessible machines are located. A DMZ allows higher-risk machines to be segmented from the internal network while still providing security controls.


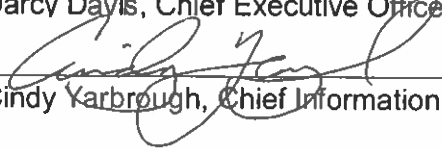
Firewall - A security system that secures the network by enforcing boundaries between secure and insecure areas. Firewalls are often implemented at the network perimeter as well as in high-security or high-risk areas.

Third Party Connection - A direct connection to a party external to the company. Examples of third party connections include connections to customers, vendors, partners, or suppliers.

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Third Party Connection Policy** Effective Date: January 14, 2015

Department: **Information Technology** Policy Number: N/A

APPROVED BY	DATE
 Darcy Davis, Chief Executive Officer	10-29-18
 Cindy Yarbrough, Chief Information Officer	10/16/18

PROCEDURE REVISION OR REVIEWED HISTORY

Original Procedure Date	Reviewed or Revised
March 12, 2014	1/14/2015 TFS "[Next Revised Procedure Date]"
	10/15/2018 CY "[Next Revised Procedure Date]"
	"[Next Revised Procedure Date]" "[Next Revised Procedure Date]"
	"[Next Revised Procedure Date]" "[Next Revised Procedure Date]"
	"[Next Revised Procedure Date]" "[Next Revised Procedure Date]"

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Two-Factor Authentication** Effective Date: 10/03/2018

Department: **Information Technology** Policy Number: N/A

POLICY

Two-factor authentication adds a second layer of security to the Health Care District of Palm Beach County (HCD) network accounts. This second form of authentication helps to prevent unauthorized access to the network even if an account password is compromised. The Health Care District of Palm Beach County currently uses Duo for two-factor authentication.

Duo can provide a second form of authentication via a mobile device app only installed on company owned cell phones, or hardware token if the user does not have an HCD issued cell phone.

Using Duo for two-factor authentication is mandatory for HCD Virtual Private Network (VPN), Outlook Web Access (OWA) and specific infrastructure.

APPLICABILITY

This policy applies to all staff and contractors working on behalf of HCD and computer systems that access the Health Care District of Palm Beach County's Information Resources and infrastructure.

DEFINITIONS

Two-Factor Authentication (2FA)	Adds a second layer of security to the Health Care District of Palm Beach County user accounts. Some services and websites refer to this second layer of security as two-factor authentication, 2FA, two-step authentication, two-step verification, or login verification. This second form of authentication helps to prevent unauthorized users from accessing the network, even if the password is compromised.
Duo	A cloud-hosted two-factor authentication system that works with several other information systems for an added layer of protection.
The Duo Mobile App	It allows the user to say "Yes" or "No" or provide a passcode for any attempted login to their account for Duo protected services and thereby provides a second factor of authorization for these services.

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Two-Factor Authentication** Effective Date: 10/03/2018

Department: **Information Technology** Policy Number: N/A

Hardware Token Small device that can generate a passcode which can be used as a second factor of authorization to services protected by two-factor authentication.

PROCEDURE

If services are requested on a User Registration Form (URF) that are protected by DUO, the Help Desk will confirm whether or not the user is already enrolled in DUO. If the user is not enrolled in DUO, the Help Desk will determine if the user has a District issued cell phone. If the user does have a District assigned cell phone, the DUO Mobile Application will be downloaded and used for DUO two-factor authentication. If the user does not have a District assigned cell phone, the Help Desk will assign them a security token to be used for Duo two-form authentication. The security tokens will be signed out to employees using the Equipment Sign-Out Form on SharePoint.

When you log into a Health Care District of Palm Beach County system protected by Duo, the system will require an additional authentication, either by approving the login by the Duo Mobile Device App on HCD cell phones or by entering the security code provided on hardware tokens.

If you enter the correct code, you will be allowed into the system. Failed attempts will be handled according to current Health Care District of Palm Beach County's Password Policy and Procedure.

Hardware Token Recycling or Disposal:

Tokens must be returned to the IT Help Desk for recycling or disposal.

Lost or Stolen Devices

If you have a hardware token lost or stolen, please contact the IT Help Desk immediately at helpdesk@hcdpbc.org or 561-804-5800. The user will be responsible for the cost of replacing the device.

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Two-Factor Authentication**

Effective Date: 10/03/2018

Department: **Information Technology**

Policy Number: N/A

RESPONSIBILITY

Operations Manager

- Ensure this document remains current and is updated whenever changes to this policy occur
- Review and approve changes to this document

Chief Information Officer

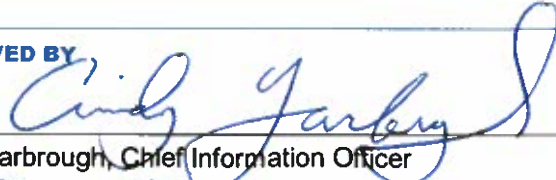

- Review and approve changes to this document

CROSS-REFERENCES

N/A

ADDENDA

N/A

APPROVED BY	DATE
 Cindy Yarbrough, Chief Information Officer	<u>10/3/18</u>
 Darcy Davis, Chief Executive Officer	<u>10-8-18</u>

PROCEDURE REVISION HISTORY

Original Procedure Date

10/03/2018

Revisions

Procedure Revision Date	Description of Changes

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **User Account Review**

Effective Date: 10/28/2018

Department: **Information Technology**

Policy Number: N/A

POLICY

The Health Care District of Palm Beach County is hereinafter referred to as "the company."

User accounts are the means used to grant access to Information Resources. These accounts provide accountability, a key to any computer security program, for information resources usage.

APPLICABILITY

The purpose of this policy is to provide standards in reviewing the company's user accounts to all IT systems.

DEFINITIONS

N/A

PROCEDURE

- Every 90 days, a review of the list of users with access to specific systems shall be performed to ensure they are still valid.
- The Systems Analyst who supports the applications for review, will confirm that all terminated or disabled users are removed by reviewing the terminated report from the financial system and disabled report from AD360. The terminated report will be provided by the Systems Analyst who is responsible for Finance Plus and the AD360 report will be provided by the MS Systems Admin.
- The Systems Analyst will then create a report that includes both the username and security access role.
- The report will be sent to the Business Owner who is responsible for the application for review.

The Business Owner will document any changes that need to be made and attest to reviewing user security access by filling out a Security Signoff Form. This form will be returned to the Systems Analyst within three weeks of receiving the report.

- If applicable, the Systems Analyst will submit a User Registration Form (URF) for User (System Year Quarter Audit) and include the changes on the Security Signoff Form and make the applicable changes.

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **User Account Review**

Effective Date: 10/28/2018

Department: **Information Technology**

Policy Number: N/A

- The attestation and Security Signoff Form returned by the Business Owner will be uploaded to the company's SharePoint system by the Systems Analyst within a one week of receipt.

RESPONSIBILITY


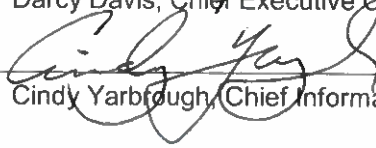
This policy will be enforced by the Chief Information Officer and Director of Software Support. Violations may result in disciplinary actions, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment.

CROSS-REFERENCES

N/A

ADDENDA

N/A

APPROVED BY	DATE
 _____ Darcy Davis, Chief Executive Officer	_____ 10-31-18
 _____ Cindy Yarbrough, Chief Information Officer	_____ 10/28/18

PROCEDURE REVISION OR REVIEWED HISTORY

Original Procedure Date

Reviewed or Revisions

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **User Account Review**

Effective Date: 10/28/2018

Department: **Information Technology**

Policy Number: N/A

10/01/2018

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title:	Third Party Connection Policy	Effective Date:	January 14, 2015
Department:	Information Technology	Policy Number:	N/A

POLICY

The Health Care District of Palm Beach County is hereinafter referred to as "the company."

1.0 Overview

Direct connections to external entities are sometimes required for business operations. These connections are typically to provide access to vendors or customers for service delivery. Since the company's security policies and controls do not extend to the users of the third parties' networks, these connections can present a significant risk to the network and thus require careful consideration.

2.0 Purpose

The policy is intended to provide guidelines for deploying and securing direct connections to third parties.

3.0 Scope

The scope of this policy covers all direct connections to the company's network from non-company owned networks. This policy excludes remote access and Virtual Private Network (VPN) access, which are covered in separate policies.

4.0 Policy

4.1 Use of Third Party Connections

Third party direct connections are to be discouraged and used only if no other reasonable option is available. When it is necessary to grant access to a third party, the access must be restricted and carefully controlled. A requester of a third party connection must demonstrate a compelling business need for the connection. This request must be approved and implemented by the IT Operations Director.

4.2 Security of Third Party Access

Third party connections require additional scrutiny. The following statements will govern these connections:

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **VPN Policy**

Effective Date: January 14, 2015

Department: **Information Technology**

Policy Number: N/A

POLICY

The Health Care District of Palm Beach County is hereinafter referred to as "the company."

1.0 Overview

A Virtual Private Network, or VPN, provides a method to communicate with remote sites securely over a public medium, such as the Internet. A site-to-site or client VPN is a dependable and inexpensive substitute for a point-to-point Wide Area Network (WAN) direct connection. Site-to-site and client VPNs can be used to connect the LAN to a number of different types of networks: branch or home offices, vendors, partners, customers, etc. As with any external access, these connections need to be carefully controlled through a policy.

2.0 Purpose

This policy details the company's standards for site-to-site and client VPNs. The purpose of this policy is to specify the security standards required for such access, ensuring the integrity of data transmitted and received, and securing the VPN pathways into the network.

3.0 Scope

The scope of this policy covers all site-to-site and client VPNs that are a part of the company's infrastructure, including both sites requiring access to the company's network (inbound) and sites where the company connects to external resources (outbound). Note that remote access is covered under a separate Remote Access Policy.

4.0 Policy

4.1 Encryption

Site-to-site and client VPNs must utilize strong encryption to protect data during transmission. Encryption algorithms must meet or exceed current minimum industry standards, such as those that conform to current FIPS standards.

4.2 Authentication

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **VPN Policy**

Effective Date: January 14, 2015

Department: **Information Technology**

Policy Number: N/A

Site-to-site and client VPNs must utilize a strong password, pre-shared key, certificate and/or two factor authentication to verify the identity the remote entity. The strongest authentication method available must be used, which can vary from product-to-product.

4.3 Implementation

When site-to-site and client VPNs are implemented, they must adhere to the policy of least access, providing access limited to only what is required for business purposes. This must be enforced with a firewall or other access control that has the ability to limit access only to the ports and IP addresses required for business purposes. Split tunneling is not authorized.

4.4 Management

The company should manage its own VPN gateways, meaning that a third party must not provide and manage both sides of the VPN, unless this arrangement is covered under an outsourcing agreement. If an existing VPN is to be changed, the changes must only be performed with the approval of the Chief Information Officer.

4.5 Logging and Monitoring

A site-to-site or client VPN can expose the company to additional risk and, as such, traffic passing across the VPN should be subject to logging and monitoring that exceeds that of the general network.

4.6 Encryption Keys

Site-to-site and client VPNs may be created with pre-shared keys. The security of these keys is critical to the security of the VPN, and by extension, the network. Encryption keys should be changed at least annually, semi-annually is preferred.

If certificates are used instead of pre-shared keys, the certificates should expire and be re-generated after one year.

4.7 Applicability of Other Policies

This document is part of the company's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

5.0 Enforcement

This policy will be enforced by the Chief Information Officer and/or Executive Team. Violations may result in

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: VPN Policy	Effective Date: January 14, 2015
Department: Information Technology	Policy Number: N/A

disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

6.0 Review and/or Revisions

This policy will be reviewed and edited if applicable at a minimum per annum or when changes are required that affect how this policy is applied and enforced. All modifications will be recorded in the Change Log at the end of this document.

7.0 Definitions

Certificate - Also called a "Digital Certificate." A file that confirms the identity of an entity, such as a company or person. Often used in VPN and encryption management to establish trust of the remote entity.

Demilitarized Zone (DMZ) - A perimeter network, typically inside the firewall but external to the private or protected network, where publicly-accessible machines are located. A DMZ allows higher-risk machines to be segmented from the internal network while still providing security controls.

Encryption - The process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission or while stored.

FIPS – Federal Information Processing Standards. Standards developed by the U.S. federal government for use in computer systems, but more significantly encryption standards such as *FIPS PUB 197 Advance Encryption Standard (AES)*.

Remote Access VPN - A VPN implementation at the individual user level. Used to provide remote and traveling users secure network access.

Site-to-Site VPN - A VPN implemented between two static sites, often different locations of a business.

Virtual Private Network (VPN) - A secure network implemented over an insecure medium, created by using encrypted tunnels for communication between endpoints.

Two Factor Authentication - Adds a second layer of security to the Health Care District of Palm Beach County user accounts. Some services and websites refer to this second layer of security as two-factor authentication, 2FA, two-step authentication, two-step verification, or login verification. This second form of authentication helps to prevent unauthorized users from accessing the network, even if the password is compromised.

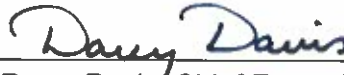
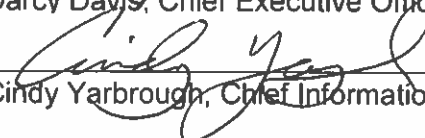
DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **VPN Policy**

Effective Date: January 14, 2015

Department: **Information Technology**

Policy Number: N/A

APPROVED BY	DATE
 Darcy Davis, Chief Executive Officer	10-29-18
 Cindy Yarbrough, Chief Information Officer	10/14/18

PROCEDURE REVISION OR REVIEWED HISTORY

Original Procedure Date

Reviewed or Revised

March 12, 2014

1/14/2015 TFS	"[Next Revised Procedure Date]"
10/12/2018 CY	"[Next Revised Procedure Date]"
"[Next Revised Procedure Date]"	"[Next Revised Procedure Date]"
"[Next Revised Procedure Date]"	"[Next Revised Procedure Date]"
"[Next Revised Procedure Date]"	"[Next Revised Procedure Date]"

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title:	Wireless Access Policy	Effective Date:	January 14, 2015
Department:	Information Technology	Policy Number:	N/A

POLICY

The Health Care District of Palm Beach County is hereinafter referred to as "the company."

1.0 Overview

Wireless communication is playing an increasingly important role in the workplace. In the past, wireless access was the exception; it has now become the norm in many companies. However, while wireless access can increase mobility and productivity of users, it can also introduce security risks to the network. These risks can be mitigated with a sound Wireless Access Policy.

2.0 Purpose

The purpose of this policy is to state the standards for wireless access to the company's network. Wireless access can be done securely if certain steps are taken to mitigate known risks. This policy outlines the steps the company wishes to take to secure its wireless infrastructure.

3.0 Scope

This policy covers anyone who accesses the network via a wireless connection. The policy further covers the wireless infrastructure of the network, including access points, routers, wireless network interface cards, and anything else capable of transmitting or receiving a wireless signal. For specific mobile device guidance, refer to the Mobile Device Policy.

4.0 Policy

4.1 Physical Guidelines

Unless a directional antenna is used, a wireless access point typically broadcasts its signal in all directions. For this reason, access points should be located central to the office space rather than along exterior walls. If it is possible with the technology in use, signal broadcast strength should be reduced to only what is necessary to cover the office space. Directional antennas should be considered in order to focus the signal to areas where it is needed.

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: Wireless Access Policy	Effective Date: January 14, 2015
Department: Information Technology	Policy Number: N/A

Physical security of access points should be considered - access points should not be placed in public or easily accessed areas if possible.

4.2 Configuration and Installation

The following guidelines apply to the configuration and installation of wireless networks:

4.2.1 Security Configuration

- The Service Set Identifier (SSID) of the access point must be changed from the factory default. The SSID should be changed to something completely nondescript. Specifically, the SSID should not identify the company, the location of the access point, or anything else that may allow a third party to associate the access point's signal to the company.
- WPA2-AES encryption will be used to secure wireless communications.
- Administrative access to wireless access points must utilize strong passwords. Passwords will be treated similarly to individual account passwords; they will not be distributed to unauthorized users or individuals not affiliated with the company.
- All logging features should be enabled on the company's access points.

4.2.2 Installation

- Software and/or firmware on the wireless access points and wireless network interface cards (NICs) must be updated prior to deployment.
- Wireless networking must not be deployed in a manner that will circumvent the company's security controls.
- Wireless devices must be installed only by the company's IT department.
- Channels used by wireless devices should be evaluated to ensure that they do not interfere with company equipment.

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Wireless Access Policy** Effective Date: January 14, 2015

Department: **Information Technology** Policy Number: N/A

4.3 Accessing Confidential Data

If confidential data is to be accessed over the wireless network, additional security measures must be taken since the security of the wireless LAN cannot be absolutely verified. The company's remote access policy must be followed in order to provide additional encryption software (IPSec, SSL, etc.) to secure this data during wireless transmission.

4.4 Inactivity

Inactive wireless access points should be disabled. If not regularly used and maintained, inactive access points represent an unacceptable risk to the company.

4.5 Applicability of Other Policies

This document is part of the company's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

5.0 Enforcement

This policy will be enforced by the Chief Information Officer and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

6.0 Review and/or Revisions

This policy will be reviewed and edited if applicable at a minimum per annum or when changes are required that affect how this policy is applied and enforced. All modifications will be recorded in the Change Log at the end of this document.

7.0 Definitions

MAC Address - Short for Media Access Control Address. The unique hardware address of a network interface card (wireless or wired). Used for identification purposes when connecting to a computer network.

SSID - Stands for Service Set Identifier. The name that uniquely identifies a wireless network.

WiFi - Short for Wireless Fidelity. Refers to networking protocols that are broadcast wirelessly using the 802.11

DEPARTMENTAL POLICY AND PROCEDURE

Policy Title: **Wireless Access Policy** Effective Date: January 14, 2015

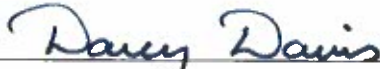
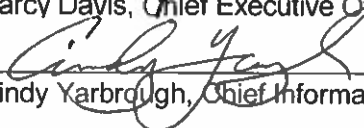
Department: **Information Technology** Policy Number: N/A

family of standards.

Wireless Access Point - A central device that broadcasts a wireless signal and allows for user connections. A wireless access point typically connects to a wired network.

Wireless NIC - A Network Interface Card (NIC) that connects to wireless, rather than wired, networks.

WPA - Stands for WiFi Protected Access. A security protocol for wireless networks that encrypts communications between the computer and the wireless access point. Newer and considered more secure than WEP.

APPROVED BY	DATE
 Darcy Davis, Chief Executive Officer	10-29-18
 Cindy Yarbrough, Chief Information Officer	10/16/18

PROCEDURE REVISION OR REVIEWED HISTORY

Original Procedure Date	Reviewed or Revised
March 12, 2014	1/14/2015 TFS "[Next Revised Procedure Date]"
	10/16/2018 CY "[Next Revised Procedure Date]"
	"[Next Revised Procedure Date]" "[Next Revised Procedure Date]"
	"[Next Revised Procedure Date]" "[Next Revised Procedure Date]"
	"[Next Revised Procedure Date]" "[Next Revised Procedure Date]"

DISTRICT CLINIC HOLDINGS, INC.
BOARD OF DIRECTORS
December 11, 2019

1. Description: Update of Current Charge Master

2. Summary:

Per the HRSA Compliance Manual, District Clinic Holdings, Inc. must prepare a schedule of fees or payments for the provision of its services consistent with locally prevailing rates or charges and designed to cover its reasonable costs of operation.

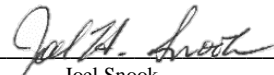
3. Substantive Analysis:

C. L. Brumback Primary Care Clinics requested and received an analysis from our Primary Care Association (FACHC) for 2018 which represents locally prevailing rates in several comparable MSA in the state of Florida. Per the attached analysis, a thorough review shows that amending the Charge Master to be at the 50th percentile would result in the smallest increase and align our organization with prevailing rates.

4. Fiscal Analysis & Economic Impact Statement:

	Amount	Budget
Capital Requirements		Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>
Annual Net Revenue		Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>
Annual Expenditures		Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>

Reviewed for financial accuracy and compliance with purchasing procedure:



 Joel Snook
 VP & Chief Financial Officer

5. Reviewed/Approved by Committee:

Finance Committee

 Committee Name

December 11, 2019

 Date Approved

DISTRICT CLINIC HOLDINGS, INC.
BOARD OF DIRECTORS
December 11, 2019

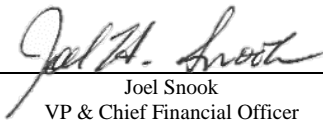
6. Recommendation:

Staff recommends the Board approve the updates to the current Charge Master.

Approved for Legal sufficiency:



Valerie Shahriari
VP & General Counsel



Joel Snook
VP & Chief Financial Officer



Dr. Belma Andric
Chief Medical Officer, VP & Executive Director
of Clinic Services

Brumback Code	Brumback Procedure Description	Brumback Fee	50th Percentile	60th Percentile	75th Percentile	80th Percentile	85th Percentile	90th Percentile	95th Percentile	Medicare Fee
10060	Incision & Drainage Abscess Simple/Singl	\$100.00	\$187.16	\$201.20	\$220.84	\$236.61	\$255.79	\$291.21	\$366.48	\$117.96
10061	Incision&drainage Abscess Complicated/Mu	\$470.00	\$374.33	\$402.40	\$441.68	\$473.22	\$511.58	\$582.43	\$732.97	\$209.03
10080	Incision & Drainage Pilonidal Cyst Simpl	\$370.00	\$291.14	\$312.98	\$343.53	\$368.06	\$397.89	\$453.00	\$570.09	\$178.68
10081	Incision & Drainage Pilonidal Cyst Compl	\$650.00	\$519.90	\$558.89	\$613.44	\$657.25	\$710.53	\$808.93	\$1,018.01	\$270.52
11042	Debridement Subcutaneous Tissue 20 Sq Cm	\$175.00	\$186.59	\$243.83	\$300.38	\$345.74	\$383.80	\$393.04	\$453.17	\$116.46
11100	Bx Skin Subcutaneous&/Mucous Membrane 1	\$130.00	\$140.37	\$165.33	\$192.71	\$201.83	\$206.12	\$207.16	\$210.32	\$103.31
11200	Removal Sk Tgs Mlt Fibrq Tags Any Area U	\$71.00	\$144.45	\$146.05	\$148.28	\$155.97	\$186.44	\$196.80	\$201.91	\$88.92
11400	Exc B9 Les Mrgn Xcp Sk Tg T/A/L 0.5 Cm/<	\$220.00	\$189.78	\$194.61	\$217.39	\$223.75	\$238.83	\$269.31	\$317.45	\$123.97
11401	Exc B9 Les Mrgn Xcp Sk Tg T/A/L 0.6-1.0	\$250.00	\$225.93	\$231.68	\$258.79	\$266.37	\$284.32	\$320.61	\$377.92	\$149.75
11402	Exc B9 Les Mrgn Xcp Sk Tg T/A/L 1.1-2.0	\$325.00	\$289.19	\$296.55	\$331.26	\$340.95	\$363.93	\$410.38	\$483.74	\$167.03
11600	Excision Mal Lesion Trunk/Arm/Leg 0.5 Cm	\$315.00	\$316.78	\$337.39	\$369.89	\$374.09	\$412.49	\$419.44	\$464.49	\$193.05
11601	Excision Mal Lesion Trunk/Arm/Leg 0.6-1.	\$345.00	\$345.58	\$368.06	\$403.51	\$408.10	\$449.99	\$457.57	\$506.71	\$230.52
11602	Excision Mal Lesion Trunk/Arm/Leg 1.1-2.	\$370.00	\$374.37	\$398.74	\$437.14	\$442.10	\$487.49	\$495.70	\$548.94	\$250.12
11750	Excision Nail Matrix Permanent Removal	\$200.00	\$284.85	\$305.78	\$332.96	\$352.34	\$363.93	\$389.92	\$466.11	\$153.04
11981	Insj Non-Biodegradable Drug Delivery Imp	\$121.00	\$225.39	\$245.23	\$270.47	\$295.09	\$316.53	\$362.53	\$368.06	\$143.47
11982	Removal Non-Biodegradable Drug Delivery	\$137.00	\$225.39	\$245.23	\$270.47	\$295.09	\$316.53	\$362.53	\$368.06	\$163.16
11983	Rmvl W/Rinsj Non-Biodegradable Drug Dlvr	\$194.00	\$245.88	\$267.53	\$295.06	\$321.92	\$345.30	\$395.49	\$401.52	\$231.63
12001	Simple Repair Scalp/Neck/Ax/Genit/Trunk	\$85.00	\$574.85	\$602.57	\$770.71	\$790.81	\$844.47	\$906.71	\$979.18	\$89.98
12002	Smpl Repair Scalp/Neck/Ax/Genit/Trunk 2.	\$120.00	\$694.61	\$728.10	\$931.27	\$955.56	\$1,020.40	\$1,095.61	\$1,183.18	\$109.52
15000	Drifting - Mesial	\$0.00								
15001	Drifting - Distal	\$0.00								
15002	Impacted - Distal	\$0.00	\$676.52	\$757.37	\$935.32	\$984.69	\$1,011.15	\$1,091.79	\$1,188.12	\$353.49
15003	Impacted - Mesial	\$0.00	\$161.08	\$180.33	\$222.70	\$234.45	\$240.75	\$259.95	\$282.89	\$77.08
15004	Bleeding	\$0.00	\$805.38	\$901.63	\$1,113.48	\$1,172.25	\$1,203.75	\$1,299.75	\$1,414.43	\$406.63
15005	Abrasion	\$0.00	\$257.72	\$288.52	\$356.31	\$375.12	\$385.20	\$415.92	\$452.62	\$128.63
15006	Periodontal abscess	\$0.00								
15007	Calculus	\$0.00								
15008	Plaque	\$0.00								
15009	Watch Tooth	\$0.00								
15010	Primary - Permanent Change	\$0.00								
15011	Hypersensitivity	\$0.00								
15012	Recession	\$0.00								
15100	Missing tooth, more than a year	\$0.00	\$1,868.47	\$2,091.77	\$2,583.26	\$2,719.62	\$2,792.70	\$3,015.42	\$3,281.47	\$880.35
15101	Missing tooth	\$0.00	\$451.01	\$504.91	\$623.55	\$656.46	\$674.10	\$727.86	\$792.08	\$189.14
15102	Prem. loss, pri tooth, > a year	\$0.00								
15103	Prem. loss, primary tooth	\$0.00								
15104	Deep dentinal/cemental caries	\$0.00								
15105	Caries/decay	\$0.00								
15106	Incipient Caries	\$0.00								
15107	Recurring caries/surface restor	\$0.00								
15108	Restoration,poor marg.integrity	\$0.00								
15109	Fractured restoration	\$0.00								
15110	Fractured th, needs restoration	\$0.00	\$1,836.26	\$2,055.71	\$2,538.72	\$2,672.73	\$2,744.55	\$2,963.43	\$3,224.89	\$819.39
15111	Non-functional tooth	\$0.00	\$289.94	\$324.59	\$400.85	\$422.01	\$433.35	\$467.91	\$509.19	\$122.09
15112	Open contact - Mesial	\$0.00								
15113	Open contact - Distal	\$0.00								
15114	Unerupted tooth	\$0.00								
15115	Periapical abscess	\$0.00	\$1,755.72	\$1,965.54	\$2,427.38	\$2,555.51	\$2,624.18	\$2,833.46	\$3,083.45	\$823.39
15201	Dentition Change Flag Template #1	\$0.00	\$357.59	\$400.32	\$494.38	\$520.48	\$534.47	\$577.09	\$628.00	\$148.09
15202	Dentition Change Flag Template #2	\$0.00								
15203	Dentition Change Flag Template #3	\$0.00								
15204	Dentition Change Flag Template #4	\$0.00								

15205	Dentition Change Flag Template #5	\$0.00								
15206	Dentition Change Flag Template #6	\$0.00								
15207	Dentition Change Flag Template #7	\$0.00								
15220	Tooth Treatment Plan Reset	\$0.00	\$1,449.68	\$1,622.93	\$2,004.26	\$2,110.05	\$2,166.75	\$2,339.55	\$2,545.97	\$784.26
15851	Removal Sutures Under Anesthesia Other S	\$85.00	\$283.05	\$341.18	\$406.02	\$412.22	\$454.76	\$577.07	\$679.31	\$98.66
16000	Furcation	\$0.00								
16001	Mobility	\$0.00								
16002	Mal-positioned	\$0.00								
16003	Bone Loss	\$0.00								
17110	Destruction Benign Lesions Up To 14	\$89.00	\$105.16	\$109.49	\$142.71	\$152.26	\$177.49	\$182.19	\$213.10	\$110.07
17250	Chemical Cauterization Granulation Tissu	\$80.00	\$87.63	\$91.25	\$118.93	\$126.89	\$147.91	\$151.83	\$177.58	\$78.60
20550	Injection 1 Tendon Sheath/Ligament Apone	\$60.00	\$173.53	\$207.96	\$230.88	\$233.42	\$237.11	\$275.00	\$312.47	\$53.88
20999	Orthopedic splint (orthotic)	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
28190	Removal Foreign Body Foot Subcutaneous	\$500.00	\$553.97	\$693.75	\$859.13	\$975.03	\$1,140.31	\$1,195.64	\$1,266.51	\$260.21
30300	Removal Foreign Body Intranasal Office P	\$190.00	\$156.68	\$206.64	\$267.49	\$267.49	\$270.52	\$295.08	\$390.50	\$176.56
36405	Vnpxr <3 Years Phys Skill Scalp Vein	\$80.00	\$39.44	\$57.63	\$63.10	\$77.69	\$78.87	\$86.76	\$101.10	\$26.08
36415	Collj Ven Bld Vnpxr	\$15.00	\$10.52	\$15.37	\$16.83	\$20.72	\$21.03	\$23.14	\$26.96	\$3.00
51701	Insj Non-Ndwellg Bldr Cath	\$60.00	\$198.45	\$224.70	\$268.23	\$325.24	\$396.12	\$442.98	\$632.36	\$47.93
54450	Foreskn Mnpj W/Lss Preputial Ads&stretch	\$400.00	\$218.38	\$246.01	\$308.12	\$317.99	\$323.09	\$336.04	\$349.75	\$72.51
56405	I&d Vulva/Prnl Absc	\$174.00	\$307.40	\$323.13	\$394.27	\$451.99	\$457.13	\$482.12	\$509.92	\$111.65
56420	I&d Of Bartholin's Gland Absc	\$148.00	\$338.14	\$355.44	\$433.70	\$497.19	\$502.84	\$530.33	\$560.91	\$122.76
56440	Marsupialization Bartholin's Gland Cyst	\$295.00	\$676.28	\$710.89	\$867.39	\$994.38	\$1,005.69	\$1,060.66	\$1,121.82	\$187.55
56501	Dstrj Les Vulva Smpl	\$185.00	\$261.29	\$274.66	\$335.13	\$384.19	\$388.56	\$409.80	\$433.43	\$132.86
56515	Dstrj Les Vulva X10sv	\$328.00	\$891.46	\$937.08	\$1,143.38	\$1,310.77	\$1,325.68	\$1,398.15	\$1,478.77	\$232.18
56605	Bx Vulva/Pr Spx 1 Les	\$99.00	\$238.24	\$250.43	\$305.56	\$350.29	\$354.28	\$373.64	\$395.19	\$83.94
56606	Bx Vulva/Pr Spx Ea Sep Addl Les	\$49.00	\$138.33	\$145.41	\$177.42	\$203.40	\$205.71	\$216.95	\$229.46	\$39.02
57061	Dstrj Vag Les Smpl	\$238.00	\$630.96	\$638.85	\$790.34	\$799.05	\$802.13	\$811.23	\$931.37	\$114.85
57065	Dstrj Vag Les X10sv	\$161.00	\$1,261.92	\$1,277.70	\$1,580.67	\$1,598.10	\$1,604.25	\$1,622.46	\$1,862.73	\$200.57
57100	Bx Vag Mucosa Smpl Spx	\$110.00	\$304.96	\$308.78	\$382.00	\$386.21	\$387.69	\$392.09	\$450.16	\$91.98
57105	Bx Vag Mucosa X10sv Req Sutr	\$205.00	\$620.44	\$628.20	\$777.16	\$785.73	\$788.76	\$797.71	\$915.84	\$139.42
57150	Irrg Vag&/Appl Medicament Disease	\$47.00	\$126.19	\$127.77	\$158.07	\$159.81	\$160.43	\$162.25	\$186.27	\$45.61
57160	Fitg&insj Pessary/Oth Intravag Support D	\$76.00	\$147.22	\$149.07	\$184.41	\$186.45	\$187.16	\$189.29	\$217.32	\$77.22
57452	Colposcopy Cervix Up/Adj Vag	\$150.00	\$406.42	\$446.88	\$585.82	\$620.04	\$629.50	\$1,262.62	\$1,296.02	\$111.46
57454	Colposcopy Cervix Bx Cervix&endocrv Curt	\$220.00	\$577.10	\$634.55	\$831.84	\$880.43	\$893.87	\$1,792.88	\$1,840.30	\$156.41
57455	Colposcopy Cervix Vag Bx Cervix	\$484.00	\$532.70	\$585.74	\$767.86	\$812.71	\$825.11	\$1,654.96	\$1,698.74	\$145.51
57500	Biopsy Cervix 1/Mlt Or Excision Of Lesio	\$123.00	\$522.17	\$630.96	\$736.12	\$776.86	\$794.87	\$806.74	\$815.89	\$128.15
57520	Conization Cervix +-D&c Rpr Knife/Laser	\$448.00	\$1,305.42	\$1,577.40	\$1,840.29	\$1,942.14	\$1,987.17	\$2,016.84	\$2,039.73	\$314.90
58100	Endometrial Bx +-Endocrv Bx W/O Dilat Sp	\$142.00	\$621.48	\$675.87	\$736.12	\$768.38	\$776.85	\$779.85	\$788.70	\$111.37
58300	Insj Intrauterine Dev	\$60.00	\$362.53	\$368.06	\$448.22	\$461.03	\$467.91	\$512.25	\$519.90	\$74.19
58301	Rmvl Intrauterine Dev	\$110.00	\$290.02	\$294.45	\$358.58	\$368.82	\$374.33	\$409.80	\$415.92	\$96.35
59425	Antepartum Care Only 4-6 Vsts	\$613.00	\$559.11	\$706.21	\$810.17	\$907.57	\$1,175.61	\$1,193.17	\$1,206.71	\$478.97
59426	Antepartum Care Only 7+ Vsts	\$1,079.00	\$1,666.38	\$2,104.78	\$2,414.63	\$2,704.92	\$3,503.79	\$3,556.12	\$3,596.47	\$855.88
59430	Postpartum Care Only Spx	\$239.00	\$219.26	\$276.95	\$317.72	\$355.91	\$461.03	\$467.91	\$473.22	\$193.88
64550	Transcutan. electric. stimulat.	\$0.00								
65205	Rmvl Fb Xtrnl Eye Cjnl Supfc	\$120.00	\$108.66	\$120.52	\$154.97	\$162.39	\$189.53	\$202.30	\$233.06	\$56.22
69200	Rmvl Fb Xtrnl Aud Canal W/O Anes	\$102.00	\$204.90	\$207.96	\$210.32	\$230.51	\$268.93	\$287.06	\$300.04	\$83.21
69209	Rmvl (indirect) Impacted Cerumen	\$10.00	\$39.49	\$40.08	\$40.53	\$44.43	\$51.83	\$55.32	\$57.83	\$12.49
69210	Rmvl Impacted Cerumen Spx 1/Bth Ears	\$15.00	\$81.96	\$83.18	\$84.13	\$92.20	\$107.57	\$114.82	\$120.01	\$49.61
80053	Compre Metab Panel	\$10.00	\$40.40	\$41.41	\$47.43	\$52.02	\$57.85	\$74.42	\$90.55	\$14.49
80053	Compre Metab Panel	\$10.00	\$40.40	\$41.41	\$47.43	\$52.02	\$57.85	\$74.42	\$90.55	\$0.00
80053	Compre Metab Panel	\$10.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
80076	Hepatc Funcj Panel	\$6.75	\$36.08	\$36.98	\$42.35	\$46.45	\$51.65	\$66.45	\$80.85	\$11.21
80076	Hepatc Funcj Panel	\$6.75	\$36.08	\$36.98	\$42.35	\$46.45	\$51.65	\$66.45	\$80.85	\$0.00

80076	Hepatic Func Panel	\$6.75	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
81002	Urnl Dip Stick/Tablet Rgnt Non-Auto W/O	\$10.00	\$15.78	\$16.70	\$20.72	\$20.80	\$21.03	\$25.89	\$30.00	\$30.00	\$3.50
81002	Urnl Dip Stick/Tablet Rgnt Non-Auto W/O	\$10.00	\$15.78	\$16.70	\$20.72	\$20.80	\$21.03	\$25.89	\$30.00	\$30.00	\$0.00
81002	Urnl Dip Stick/Tablet Rgnt Non-Auto W/O	\$10.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
81025	Urine Pregnancy Tst Vis Color Cmprsn Met	\$15.00	\$29.80	\$31.55	\$39.13	\$39.29	\$39.73	\$48.91	\$56.66	\$56.66	\$8.67
81025	Urine Pregnancy Tst Vis Color Cmprsn Met	\$15.00	\$29.80	\$31.55	\$39.13	\$39.29	\$39.73	\$48.91	\$56.66	\$56.66	\$0.00
81025	Urine Pregnancy Tst Vis Color Cmprsn Met	\$15.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
82272	Blood Occult Peroxidase Actv Qual Feces	\$13.00	\$13.32	\$13.52	\$18.17	\$18.44	\$18.72	\$23.42	\$30.74	\$30.74	\$4.46
82272	Blood Occult Peroxidase Actv Qual Feces	\$13.00	\$13.32	\$13.52	\$18.17	\$18.44	\$18.72	\$23.42	\$30.74	\$30.74	\$0.00
82272	Blood Occult Peroxidase Actv Qual Feces	\$13.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
82948	Gluc Bld Rgnt Strip	\$10.00	\$12.48	\$16.78	\$20.72	\$22.45	\$28.69	\$29.11	\$35.42	\$35.42	\$4.35
82948	Gluc Bld Rgnt Strip	\$10.00	\$12.48	\$16.78	\$20.72	\$22.45	\$28.69	\$29.11	\$35.42	\$35.42	\$0.00
82948	Gluc Bld Rgnt Strip	\$10.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
83036	Hgb Glycosylated	\$10.00	\$31.54	\$41.58	\$44.20	\$53.78	\$58.00	\$69.42	\$94.64	\$94.64	\$13.32
83036	Hgb Glycosylated	\$10.00	\$31.54	\$41.58	\$44.20	\$53.78	\$58.00	\$69.42	\$94.64	\$94.64	\$0.00
83036	Hgb Glycosylated	\$10.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
85025	Bld# Compl Auto Hhrwp&auto Diffial	\$10.00	\$27.97	\$30.49	\$34.87	\$36.82	\$42.75	\$53.22	\$58.40	\$58.40	\$10.66
85025	Bld# Compl Auto Hhrwp&auto Diffial	\$10.00	\$27.97	\$30.49	\$34.87	\$36.82	\$42.75	\$53.22	\$58.40	\$58.40	\$0.00
85025	Bld# Compl Auto Hhrwp&auto Diffial	\$10.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
85027	Bld# Compl Auto Hhrwp	\$10.00	\$26.46	\$28.84	\$32.99	\$34.83	\$40.44	\$50.35	\$55.25	\$55.25	\$8.87
85027	Bld# Compl Auto Hhrwp	\$10.00	\$26.46	\$28.84	\$32.99	\$34.83	\$40.44	\$50.35	\$55.25	\$55.25	\$0.00
85027	Bld# Compl Auto Hhrwp	\$10.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
86382	Neutralization Tst Viral	\$322.00	\$134.68	\$153.14	\$211.19	\$404.30	\$428.09	\$434.46	\$464.95	\$464.95	\$23.20
86382	Neutralization Tst Viral	\$322.00	\$134.68	\$153.14	\$211.19	\$404.30	\$428.09	\$434.46	\$464.95	\$464.95	\$0.00
86382	Neutralization Tst Viral	\$322.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
86580	Skn Tst Tuberculosis Id	\$10.00	\$29.01	\$32.98	\$45.49	\$87.08	\$92.20	\$93.58	\$100.14	\$100.14	\$8.03
86580	Skn Tst Tuberculosis Id	\$10.00	\$29.01	\$32.98	\$45.49	\$87.08	\$92.20	\$93.58	\$100.14	\$100.14	\$0.00
86580	Skn Tst Tuberculosis Id	\$10.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
86703	Antb Hiv-1&hiv-2 1 Assay	\$18.70	\$96.28	\$116.92	\$201.24	\$283.60	\$423.72	\$462.68	\$573.60	\$573.60	\$18.80
86703	Antb Hiv-1&hiv-2 1 Assay	\$18.70	\$96.28	\$116.92	\$201.24	\$283.60	\$423.72	\$462.68	\$573.60	\$573.60	\$0.00
86703	Antb Hiv-1&hiv-2 1 Assay	\$18.70	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
86704	Hep B Core Antb Hbcab Tot	\$10.35	\$84.25	\$102.31	\$176.09	\$248.15	\$370.76	\$404.85	\$501.90	\$501.90	\$16.53
86704	Hep B Core Antb Hbcab Tot	\$10.35	\$84.25	\$102.31	\$176.09	\$248.15	\$370.76	\$404.85	\$501.90	\$501.90	\$0.00
86704	Hep B Core Antb Hbcab Tot	\$10.35	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
86706	Hep B Surf Antb Hbsab	\$9.00	\$74.62	\$90.61	\$155.96	\$219.79	\$328.38	\$358.58	\$444.54	\$444.54	\$14.73
86706	Hep B Surf Antb Hbsab	\$9.00	\$74.62	\$90.61	\$155.96	\$219.79	\$328.38	\$358.58	\$444.54	\$444.54	\$0.00
86706	Hep B Surf Antb Hbsab	\$9.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
86708	Hep Antb Haab Tot	\$12.80	\$89.06	\$108.15	\$186.15	\$262.33	\$391.94	\$427.98	\$530.58	\$530.58	\$16.99
86708	Hep Antb Haab Tot	\$12.80	\$89.06	\$108.15	\$186.15	\$262.33	\$391.94	\$427.98	\$530.58	\$530.58	\$0.00
86708	Hep Antb Haab Tot	\$12.80	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
86735	Antb Mumps	\$24.05	\$96.28	\$116.92	\$201.24	\$283.60	\$423.72	\$462.68	\$573.60	\$573.60	\$17.90
86735	Antb Mumps	\$24.05	\$96.28	\$116.92	\$201.24	\$283.60	\$423.72	\$462.68	\$573.60	\$573.60	\$0.00
86735	Antb Mumps	\$24.05	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
86762	Antb Rubella	\$19.58	\$57.77	\$70.15	\$120.74	\$170.16	\$254.23	\$277.61	\$344.16	\$344.16	\$19.74
86762	Antb Rubella	\$19.58	\$57.77	\$70.15	\$120.74	\$170.16	\$254.23	\$277.61	\$344.16	\$344.16	\$0.00
86762	Antb Rubella	\$19.58	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
86765	Antb Rubeola	\$24.05	\$101.09	\$122.77	\$211.30	\$297.78	\$444.91	\$485.81	\$602.28	\$602.28	\$17.67
86765	Antb Rubeola	\$24.05	\$101.09	\$122.77	\$211.30	\$297.78	\$444.91	\$485.81	\$602.28	\$602.28	\$0.00
86765	Antb Rubeola	\$24.05	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
86787	Antb Varicella-Zoster	\$16.00	\$98.69	\$119.84	\$206.27	\$290.69	\$434.31	\$474.25	\$587.94	\$587.94	\$17.67
86787	Antb Varicella-Zoster	\$16.00	\$98.69	\$119.84	\$206.27	\$290.69	\$434.31	\$474.25	\$587.94	\$587.94	\$0.00
86787	Antb Varicella-Zoster	\$16.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
86803	Hep C Antb	\$12.80	\$117.94	\$143.23	\$246.52	\$347.41	\$519.06	\$566.78	\$702.66	\$702.66	\$19.57

86803	Hep C Antb	\$12.80	\$117.94	\$143.23	\$246.52	\$347.41	\$519.06	\$566.78	\$702.66	\$0.00
86803	Hep C Antb	\$12.80	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
87340	Iaad Eia Hep B Surf Ag	\$10.90	\$43.49	\$44.16	\$49.31	\$49.50	\$51.17	\$55.62	\$59.84	\$14.17
87340	Iaad Eia Hep B Surf Ag	\$10.90	\$43.49	\$44.16	\$49.31	\$49.50	\$51.17	\$55.62	\$59.84	\$0.00
87340	Iaad Eia Hep B Surf Ag	\$10.90	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
90371	Hepatitis B Immune Globulin Hbig Human I	\$10.00	\$259.54	\$266.38	\$321.86	\$329.27	\$338.58	\$388.55	\$437.38	\$124.27
90460	Imadm Through 18yr Any Route 1st Vac/Tox	\$36.00	\$40.98	\$42.06	\$50.82	\$51.99	\$53.46	\$61.35	\$69.06	\$25.11
90461	Imadm Through 18yr Any Route Ea Addl Vac	\$30.00	\$24.59	\$25.24	\$30.49	\$31.19	\$32.08	\$36.81	\$41.44	\$12.73
90471	Imadm Prq Id Subq/Im Njxs 1 Vacc	\$15.00	\$40.98	\$42.06	\$50.82	\$51.99	\$53.46	\$61.35	\$69.06	\$25.11
90472	Imadm Prq Id Subq/Im Njxs Ea Vacc	\$10.00	\$24.59	\$25.24	\$30.49	\$31.19	\$32.08	\$36.81	\$41.44	\$12.73
90473	Imadm Intransl/Oral 1 Vacc	\$10.00	\$27.32	\$28.04	\$33.88	\$34.66	\$35.64	\$40.90	\$46.04	\$25.11
90474	Imadm Intransl/Oral Ea Vacc	\$10.00	\$24.59	\$25.24	\$30.49	\$31.19	\$32.08	\$36.81	\$41.44	\$12.73
90620	Meningococcal (MendB)	\$221.00	\$395.33	\$423.81	\$501.86	\$529.80	\$573.86	\$645.19	\$815.52	\$0.00
90620	Exam and consultation	\$0.00	\$395.33	\$423.81	\$501.86	\$529.80	\$573.86	\$645.19	\$815.52	\$0.00
90632	Hepatitis A Vaccine Adult For Intramuscu	\$110.00	\$120.66	\$129.36	\$153.18	\$161.70	\$175.15	\$196.92	\$248.91	\$53.38
90633	Hepatitis A Vaccine Pediatric 2 Dose Sch	\$30.00	\$58.86	\$63.10	\$74.72	\$78.88	\$85.44	\$96.06	\$121.42	\$0.00
90636	Hepatitis A & B Vaccine Hepa-Hepb Adult	\$55.00	\$161.87	\$173.53	\$205.48	\$216.92	\$234.96	\$264.17	\$333.91	\$0.00
90647	Hemophilus Influenza B Vaccine Prp-Omp 3	\$30.00	\$50.03	\$53.64	\$63.51	\$67.05	\$72.62	\$81.65	\$103.21	\$0.00
90648	Hemophilus Influenza B Vaccine Prp-T 4 D	\$50.00	\$47.09	\$50.48	\$59.78	\$63.10	\$68.35	\$76.85	\$97.14	\$0.00
90649	Human Papilloma Virus Vaccine Quadriv 3	\$250.00	\$223.67	\$239.78	\$283.94	\$299.74	\$324.67	\$365.03	\$461.40	\$0.00
90651	HPV 9	\$250.00	\$252.04	\$270.19	\$319.95	\$337.76	\$365.85	\$411.33	\$519.92	\$0.00
90654	Influenza Vaccine Prsv Free Id Use	\$20.00	\$37.02	\$39.69	\$47.00	\$49.62	\$53.74	\$60.42	\$76.37	\$0.00
90656	Influenza Virus Vacc Split Prsrv Fr 3 Ye	\$20.00	\$26.49	\$28.40	\$33.62	\$35.50	\$38.45	\$43.23	\$54.64	\$19.25
90657	Influenza Virus Vaccine Split Virus 6-35	\$20.00	\$27.22	\$29.18	\$34.56	\$36.48	\$39.52	\$44.43	\$56.16	\$0.00
90658	Influenza Virus Vaccine Split Virus 3 Ye	\$20.00	\$27.22	\$29.18	\$34.56	\$36.48	\$39.52	\$44.43	\$56.16	\$0.00
90660	Influenza Virus Vaccine Live Intranasal	\$43.00	\$35.32	\$37.86	\$44.83	\$47.33	\$51.26	\$57.64	\$72.85	\$0.00
90662	Influenza Vaccine Splt Prsrv Free Inc An	\$40.00	\$71.93	\$77.11	\$91.31	\$96.39	\$104.41	\$117.39	\$148.38	\$49.03
90670	Pneumococcal Conj Vaccine 13 Valent Im	\$220.00	\$193.68	\$207.63	\$245.87	\$259.55	\$281.14	\$316.09	\$399.53	\$192.64
90672	Internasal Live Influenza vaccine	\$15.00	\$80.87	\$86.70	\$102.67	\$108.38	\$117.39	\$131.99	\$166.83	\$0.00
90680	Rotavirus Vaccine Pentavalent 3 Dose Liv	\$140.00	\$132.44	\$141.98	\$168.12	\$177.48	\$192.24	\$216.14	\$273.20	\$0.00
90685	Influenza virus vaccine, 6-35 months	\$0.00	\$48.74	\$52.25	\$61.87	\$65.31	\$70.74	\$79.54	\$100.54	\$21.20
90686	Fluzone (IIV4)	\$20.00	\$35.96	\$38.55	\$45.65	\$48.20	\$52.20	\$58.69	\$74.19	\$19.03
90688	FLUZONE QUADRIVALENT, 3 YRS & OLDER	\$20.00	\$36.20	\$38.81	\$45.95	\$48.51	\$52.55	\$59.08	\$74.67	\$17.83
90696	Dtap-Ipv Inactivated If Admin Pts Age 4-	\$70.00	\$96.82	\$103.80	\$122.91	\$129.76	\$140.55	\$158.02	\$199.74	\$0.00
90698	Dtap-Hib-Ipv Vaccine Im	\$145.00	\$132.44	\$141.98	\$168.12	\$177.48	\$192.24	\$216.14	\$273.20	\$0.00
90700	Dtap Vaccine < 7 Yr Im	\$50.00	\$44.15	\$47.33	\$56.04	\$59.16	\$64.08	\$72.05	\$91.07	\$0.00
90702	Diphtheria Tetanus Toxoid Adsorbed < 7 Y	\$5.00	\$36.05	\$38.65	\$45.77	\$48.31	\$52.33	\$58.84	\$74.37	\$0.00
90703	Tetanus Toxoid Adsorbed Intramuscular	\$20.00								
90704	Mumps Virus Vaccine Live Subcutaneous	\$62.00								
90705	Measles Virus Vaccine Live Subcutaneous	\$47.00								
90706	Rubella Virus Vaccine Live Subcutaneous	\$53.00								
90707	Measles Mumps Rubella Virus Vaccine Live	\$95.00	\$88.29	\$94.65	\$112.08	\$118.32	\$128.16	\$144.09	\$182.13	\$0.00
90708	Measles & Rubella Virus Vaccine Live Sub	\$152.00								
90710	Measles Mumps Rubella Varicella Vacc Liv	\$275.00	\$235.44	\$252.40	\$298.88	\$315.52	\$341.76	\$384.24	\$485.68	\$0.00
90713	Poliovirus Vaccine Inactivated Subq/Im	\$50.00	\$50.03	\$53.64	\$63.51	\$67.05	\$72.62	\$81.65	\$103.21	\$0.00
90714	Td Toxoids Adsorbed Prsrv Fr 7 Yr + Im	\$43.00								
90715	Tdap Vaccine 7 Yr + Im	\$80.00								
90716	Varicella Virus Vaccine Live Subq	\$165.00								
90721	Dtap-Hib Vaccine Intramuscular	\$0.00								
90723	Dtap-Hepb-Ipv Vaccine Intramuscular	\$110.00								
90732	Pneumococcal Polysac Vaccine 23-V 2 Yr +	\$101.00								
90733	Meningococcal Polysac Vaccine Subcutaneo	\$179.00								
90734	Meningococcal Conj Vaccine Tetravalent I	\$205.00								

90743	Hepatitis B Vaccine Adolescent 2 Dose Im	\$0.00									
90744	Hepatitis B Vaccine Pediatric3 Dose Im	\$20.00									
90746	Hepatitis B Vaccine Adult Dosage Intramu	\$94.00									
90748	Hepb-Hib Vaccine Intramuscular	\$90.00									
90791	Psychiatric diagnostic evaluation	\$203.00	\$256.67	\$299.52	\$394.38	\$414.28	\$512.29	\$577.57	\$1,012.48	\$132.50	
90792	Psychiatric diag eval w/medical services	\$232.00	\$270.31	\$315.44	\$415.34	\$436.29	\$539.52	\$608.26	\$1,066.28	\$148.88	
90832	Psychotherapy, 30 minutes	\$99.00	\$112.50	\$121.81	\$149.98	\$171.34	\$193.41	\$196.83	\$199.82	\$64.47	
90834	Psychtherapy, 45 minutes	\$131.00	\$155.38	\$168.23	\$207.14	\$236.63	\$267.12	\$271.84	\$275.98	\$85.77	
90846	Fam PsycTx W/O Pt Present	\$159.00	\$284.38	\$523.51	\$882.24	\$922.31	\$1,030.94	\$1,110.23	\$1,184.94	\$103.83	
90847	Fam PsycTx W/Pt Present	\$165.00	\$302.08	\$556.10	\$937.15	\$979.71	\$1,095.10	\$1,179.33	\$1,258.69	\$107.76	
90863	Pharmacologic mangement	\$0.00	\$350.38	\$350.38	\$383.85	\$389.70	\$406.41	\$470.19	\$475.52	\$0.00	
92551	Scr Tst Pure Tone Air Only	\$0.00	\$26.23	\$29.12	\$47.13	\$47.13	\$47.83	\$50.29	\$66.02	\$11.80	
92567	Tympanometry	\$13.00	\$48.58	\$53.93	\$87.28	\$87.28	\$88.58	\$93.13	\$122.25	\$14.52	
93000	Ecg Routine Ecg W/Least 12 Lds W/I&r	\$40.00	\$51.98	\$62.13	\$85.61	\$91.85	\$98.80	\$133.19	\$166.52	\$17.99	
93005	Ecg Routine Ecg W/Least 12 Lds Trcg Only	\$30.00	\$34.20	\$40.88	\$56.33	\$60.43	\$65.00	\$87.63	\$109.55	\$9.06	
93005	Ecg Routine Ecg W/Least 12 Lds Trcg Only	\$30.00	\$34.20	\$40.88	\$56.33	\$60.43	\$65.00	\$87.63	\$109.55	\$9.06	
93005	Ecg Routine Ecg W/Least 12 Lds Trcg Only	\$30.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	
94640	Pressurized/Nonpressurized Inhalation Tr	\$30.00	\$24.95	\$29.84	\$36.25	\$40.97	\$44.75	\$51.79	\$66.59	\$19.32	
94664	Demo&/Eval Of Pt Utiliz Aersl Gen/Neb/In	\$30.00	\$29.70	\$35.53	\$43.15	\$48.78	\$53.28	\$61.65	\$79.28	\$18.22	
94760	Noninvasive Ear/Pulse Oximetry Single De	\$5.00	\$17.82	\$21.32	\$25.89	\$29.27	\$31.97	\$36.99	\$47.57	\$3.56	
94760	Noninvasive Ear/Pulse Oximetry Single De	\$5.00	\$17.82	\$21.32	\$25.89	\$29.27	\$31.97	\$36.99	\$47.57	\$0.00	
94760	Noninvasive Ear/Pulse Oximetry Single De	\$5.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	
95115	Prof Svcs Allg Immntx X W/Prv Allgic Xtr	\$30.00	\$20.72	\$22.87	\$26.29	\$27.73	\$31.07	\$31.55	\$34.53	\$9.42	
95117	Prof Svcs Allg Immntx X W/Prv Allgic Xtr	\$40.00	\$31.08	\$34.31	\$39.43	\$41.59	\$46.61	\$47.33	\$51.79	\$10.89	
95831	Muscle testing	\$0.00	\$119.19	\$143.01	\$237.91	\$286.07	\$383.46	\$459.86	\$815.40	\$33.46	
95868	Electromyography	\$0.00	\$401.61	\$481.90	\$801.66	\$963.95	\$1,292.08	\$1,549.54	\$2,747.53	\$140.83	
95868	Electromyography	\$0.00	\$120.44	\$144.62	\$240.56	\$289.23	\$387.65	\$464.85	\$824.29	\$73.55	
95868	Electromyography	\$0.00	\$281.17	\$337.28	\$561.10	\$674.72	\$904.43	\$1,084.69	\$1,923.24	\$67.28	
96160	Health risk assessment - pt focused	\$0.00	\$12.46	\$17.80	\$18.27	\$22.25	\$22.50	\$22.84	\$34.78	\$4.76	
96161	Health risk assessment	\$0.01	\$12.46	\$17.80	\$18.27	\$22.25	\$22.50	\$22.84	\$34.78	\$4.76	
96372	Therapeutic Prophylactic/Dx Injection Su	\$20.00	\$46.78	\$53.28	\$57.18	\$72.78	\$77.98	\$82.14	\$84.13	\$26.52	
97602	Rmvl Devital Tiss N-Slctv Dbrdmt W/O Ane	\$21.00	\$73.40	\$82.40	\$98.98	\$118.15	\$174.63	\$179.25	\$960.48	\$0.00	
97700	Adjust orthotic/splint	\$0.00									
97802	Med Nutr Ther 1st Assmt&ivntj Indiv Ea 1	\$0.00	\$32.30	\$36.26	\$43.55	\$51.99	\$76.84	\$78.87	\$422.61	\$36.04	
97803	Med Nutr Ther Re-Assmt&ivntj Indiv Ea 15	\$48.00	\$32.30	\$36.26	\$43.55	\$51.99	\$76.84	\$78.87	\$422.61	\$31.33	
98925	Osteopathic Manipulative Tx 1-2 Bdy Regi	\$60.00	\$103.98	\$105.17	\$109.49	\$110.70	\$111.13	\$112.40	\$112.40	\$33.06	
98926	Osteopathic Manipulative Tx 3-4 Bdy Regi	\$90.00	\$136.71	\$138.27	\$143.95	\$145.55	\$146.12	\$147.79	\$147.79	\$47.79	
98927	Osteopathic Manipulative Tx 5-6 Bdy Regi	\$120.00	\$161.74	\$163.59	\$170.31	\$172.20	\$172.87	\$174.85	\$174.85	\$62.52	
98928	Osteopathic Manipulative Tx 7-8 Bdy Regi	\$194.00	\$177.15	\$179.17	\$186.53	\$188.60	\$189.34	\$191.50	\$191.50	\$76.15	
98929	Osteopathic Manipulative Tx 9-10 Bdy Reg	\$180.00	\$184.85	\$186.96	\$194.64	\$196.80	\$197.57	\$199.82	\$199.82	\$90.89	
99173	Screening	\$0.00	\$31.08	\$32.28	\$32.75	\$41.43	\$51.22	\$52.58	\$69.16	\$3.56	
99188	Application of topical fluoride varnish	\$40.00	\$37.06	\$38.50	\$39.06	\$49.41	\$61.08	\$62.71	\$82.48	\$0.00	
99201	Office Outpt New 10 Min	\$69.00	\$133.48	\$147.35	\$179.30	\$196.37	\$222.21	\$235.84	\$282.49	\$46.39	
99202	Office Outpt New 20 Minutes	\$118.00	\$166.37	\$183.65	\$223.47	\$244.76	\$276.96	\$293.95	\$352.08	\$78.72	
99203	Office Outpt New 30 Min	\$173.00	\$216.66	\$239.18	\$291.03	\$318.75	\$360.70	\$382.82	\$458.53	\$114.65	
99204	Office Outpt New 45 Min	\$266.00	\$309.52	\$341.68	\$415.76	\$455.36	\$515.28	\$546.88	\$655.04	\$173.63	
99205	Office Outpt New 60 Min	\$330.00	\$417.85	\$461.27	\$561.28	\$614.74	\$695.63	\$738.29	\$884.30	\$218.89	
99211	Office O/P Est 5 Min	\$32.00	\$69.94	\$79.91	\$89.15	\$92.66	\$107.45	\$116.79	\$133.95	\$21.01	
99212	Office Outpt Est 10 Min	\$69.00	\$99.39	\$113.56	\$126.68	\$131.68	\$152.69	\$165.97	\$190.35	\$45.76	
99213	Office Outpt Est15 Min	\$116.00	\$126.99	\$145.11	\$161.87	\$168.26	\$195.10	\$212.07	\$243.23	\$76.60	
99214	Office Outpt Est 25 Min	\$171.00	\$184.05	\$210.30	\$234.60	\$243.85	\$282.75	\$307.35	\$352.50	\$112.53	
99215	Office Outpt Est 40 Min	\$228.00	\$294.48	\$336.48	\$375.36	\$390.16	\$452.40	\$491.76	\$564.00	\$151.87	
99245	Office Consltj 80 Min	\$140.00	\$457.72	\$492.34	\$573.16	\$623.55	\$654.47	\$693.27	\$831.89	\$233.44	

99381	1st Preventive Medicine New Patient < 1y	\$176.00	\$161.50	\$171.83	\$180.73	\$186.23	\$192.23	\$195.39	\$208.53	\$115.20
99382	1st Preventive Medicine New Patient Age	\$182.00	\$173.92	\$185.05	\$194.63	\$200.55	\$207.02	\$210.42	\$224.57	\$120.26
99383	1st Preventive Medicine New Patient Age	\$190.00	\$186.35	\$198.27	\$208.53	\$214.88	\$221.81	\$225.45	\$240.62	\$125.57
99384	1st Preventive Medicine New Patient Age	\$215.00	\$198.77	\$211.49	\$222.43	\$229.20	\$236.59	\$240.48	\$256.66	\$141.27
99385	1st Preventive Medicine New Patient Age	\$209.00	\$269.17	\$286.39	\$301.21	\$310.38	\$320.39	\$325.65	\$347.56	\$136.66
99386	1st Preventive Medicine New Patient Age	\$241.00	\$294.01	\$312.83	\$329.01	\$339.03	\$349.96	\$355.71	\$379.64	\$159.13
99387	1st Preventive Medicine New Patient Age	\$263.00	\$331.28	\$352.48	\$370.72	\$382.00	\$394.32	\$400.80	\$427.76	\$172.46
99391	Periodic Preventive Med Established Pati	\$158.00	\$132.51	\$140.99	\$148.29	\$152.80	\$157.73	\$160.32	\$171.10	\$103.31
99392	Periodic Preventive Med Est Patient Age	\$169.00	\$140.79	\$149.80	\$157.56	\$162.35	\$167.59	\$170.34	\$181.80	\$110.44
99393	Periodic Preventive Med Est Patient Age	\$168.00	\$153.22	\$163.02	\$171.46	\$176.68	\$182.37	\$185.37	\$197.84	\$110.07
99394	Periodic Preventive Med Est Patient Age	\$184.00	\$165.64	\$176.24	\$185.36	\$191.00	\$197.16	\$200.40	\$213.88	\$120.81
99395	Periodic Preventive Med Est Patient Age	\$187.00	\$223.61	\$237.92	\$250.24	\$257.85	\$266.17	\$270.54	\$288.74	\$123.34
99396	Periodic Preventive Med Est Patient Age	\$200.00	\$244.32	\$259.95	\$273.41	\$281.73	\$290.81	\$295.59	\$315.47	\$131.55
99397	Periodic Preventive Med Est Patient Age	\$215.00	\$277.45	\$295.20	\$310.48	\$319.93	\$330.24	\$335.67	\$358.25	\$141.63
99401	Prev Med Cnsl Indiv Spx 15 Min	\$65.00	\$70.40	\$74.90	\$78.78	\$81.18	\$83.79	\$85.17	\$90.90	\$37.80
99402	Prev Med Cnsl Indiv Spx 30 Min	\$125.00	\$136.65	\$145.40	\$152.92	\$157.58	\$162.66	\$165.33	\$176.45	\$64.60
99403	Prev Med Cnsl Indiv Spx 45 Min	\$190.00	\$207.05	\$220.30	\$231.70	\$238.75	\$246.45	\$250.50	\$267.35	\$90.68
99404	Prev Med Cnsl Indiv Spx 60 Min	\$250.00	\$269.17	\$286.39	\$301.21	\$310.38	\$320.39	\$325.65	\$347.56	\$116.75
99406	Tobacco Use Cessation Intermediate 3-10	\$0.00	\$41.41	\$44.06	\$46.34	\$47.75	\$49.29	\$50.10	\$53.47	\$15.37
99407	Tobacco Use Cessation Intensive >10 Minu	\$44.00	\$82.82	\$88.12	\$92.68	\$95.50	\$98.58	\$100.20	\$106.94	\$29.63
99408	Alcohol/Substance Screen & Interven 15-3	\$20.00	\$99.38	\$105.74	\$111.22	\$114.60	\$118.30	\$120.24	\$128.33	\$36.84
99409	Alcohol/Substance Screen & Interven >30	\$40.00	\$194.63	\$207.08	\$217.80	\$224.43	\$231.66	\$235.47	\$251.31	\$71.85
99455	Work Related/Med Dbt Xm Treating Phys	\$85.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
99456	Work Related/Med Dbt Xm Oth/Thn Treatin	\$90.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00	\$0.00
99490	Chronic Care Management >20 minutes	\$0.00	\$104.39	\$119.28	\$133.07	\$138.31	\$160.38	\$174.33	\$199.94	\$44.20
99495	Transitional Care Mang Service	\$163.00	\$354.15	\$404.66	\$451.42	\$469.22	\$544.07	\$591.40	\$678.28	\$170.76
99496	Transitional Care Mang. Service	\$230.00	\$508.23	\$580.72	\$647.82	\$673.36	\$780.78	\$848.71	\$973.39	\$241.62
209999	Mandibular kinesiograph record	\$0.00								

Brumback Code	This is the CPT Code you provided
Code	This is the matching CPT Code from the software
Modifier	This is the Modifier for the Matching CPT Code (Software), if available/applicable
Sub	This is the Sub-Modifier for the Matching CPT Code (Software), if available/applicable
Brumback Insurance Description	This is the Procedure Code Description you provided
Fee Software Description	This is the matching Procedure Code Description from the Software
Brumback Fee	This is the Fee you provided for the particular procedure
50th Percentile	This is the fee that falls within the 50th percentile of what those providing this service and reported data are charging for that same procedure
60th Percentile	This is the fee that falls within the 60th percentile of what those providing this service and reported data are charging for that same procedure
75th Percentile	This is the fee that falls within the 75th percentile of what those providing this service and reported data are charging for that same procedure
80th Percentile	This is the fee that falls within the 80th percentile of what those providing this service and reported data are charging for that same procedure
85th Percentile	This is the fee that falls within the 85th percentile of what those providing this service and reported data are charging for that same procedure
90th Percentile	This is the fee that falls within the 90th percentile of what those providing this service and reported data are charging for that same procedure
95th Percentile	This is the fee that falls within the 95th percentile of what those providing this service and reported data are charging for that same procedure
Medicare Fee	This is the Standard Medicare Fee being charged in your area for this procedure

Brumback Code	Brumback Procedure Description	Brumback Fee	50th Percentile	60th Percentile	75th Percentile	80th Percentile	85th Percentile	90th Percentile	95th Percentile
D0120	Periodic oral evaluation	\$28.00	\$47.34	\$51.64	\$58.48	\$61.03	\$65.47	\$70.18	\$75.94
D0140	Limited oral evaluation	\$78.00	\$79.37	\$86.57	\$98.04	\$102.31	\$109.77	\$117.65	\$127.31
D0145	Oral evaluation for a patient under 3 yrs	\$30.00	\$73.80	\$80.49	\$91.16	\$95.13	\$102.06	\$109.40	\$118.37
D0150	Comp oral eval-new/estab pat	\$30.00	\$83.55	\$91.13	\$103.20	\$107.69	\$115.54	\$123.85	\$134.01
D0210	Intraoral-complete series (bw)	\$60.00	\$123.11	\$133.10	\$151.88	\$161.82	\$169.52	\$177.99	\$197.77
D0220	Intraoral-periapical-1st film	\$13.00	\$24.62	\$26.62	\$30.38	\$32.36	\$33.90	\$35.60	\$39.55
D0230	Intraoral-periapical-each add'l	\$10.00	\$22.16	\$23.96	\$27.34	\$29.13	\$30.51	\$32.04	\$35.60
D0240	Intraoral-occlusal film	\$18.00	\$38.17	\$41.26	\$47.08	\$50.17	\$52.55	\$55.18	\$61.31
D0250	Extraoral-first film	\$58.00	\$46.78	\$50.58	\$57.71	\$61.49	\$64.42	\$67.64	\$75.15
D0260	Extraoral-each additional film	\$32.00							
D0270	Bitewing-single film	\$12.00	\$26.55	\$29.13	\$33.40	\$34.06	\$35.10	\$36.71	\$39.23
D0272	Bitewings-two films	\$17.00	\$42.48	\$46.61	\$53.44	\$54.49	\$56.16	\$58.74	\$62.78
D0274	Bitewings-four films	\$24.00	\$59.74	\$65.54	\$75.15	\$76.63	\$78.98	\$82.60	\$88.28
D0290	Skull &facial bone survey film	\$78.00							
D0330	Panoramic film	\$50.00	\$103.27	\$113.91	\$130.61	\$138.14	\$144.19	\$151.87	\$166.37
D0340	Cephalometric film	\$52.00	\$116.60	\$128.61	\$147.47	\$155.96	\$162.79	\$171.47	\$187.84
D0350	Oral/Facial Photographic Images	\$27.00	\$55.52	\$61.24	\$70.22	\$74.27	\$77.52	\$81.65	\$89.45
D0470	Diagnostic casts	\$40.00	\$118.06	\$134.26	\$155.28	\$166.37	\$177.28	\$178.20	\$192.78
D1110	Prophylaxis-adult	\$38.00	\$93.77	\$97.64	\$105.77	\$107.81	\$111.88	\$117.98	\$128.57
D1120	Prophylaxis-child	\$29.00	\$64.72	\$67.39	\$72.99	\$74.41	\$77.21	\$81.43	\$88.73
D1206	Fluoride Varnish	\$27.00	\$48.35	\$52.88	\$54.92	\$58.99	\$67.13	\$71.38	\$77.06
D1208	Fluoride topical	\$21.00	\$32.23	\$35.26	\$36.62	\$39.32	\$44.75	\$47.59	\$51.37
D1330	Oral hygiene instruction	\$15.00	\$61.06	\$68.19	\$71.35	\$74.46	\$78.10	\$81.00	\$86.78
D1351	Sealant-per tooth	\$24.00	\$49.61	\$55.40	\$57.97	\$60.50	\$63.46	\$65.81	\$70.51
D1352	Preventive Restoration, Perm Th	\$27.00	\$63.61	\$71.03	\$74.33	\$77.56	\$81.36	\$84.38	\$90.40
D1354	Interim caries arresting meds	\$27.00	\$49.61	\$55.40	\$57.97	\$60.50	\$63.46	\$65.81	\$70.51
D1510	Space maint-fixed-unilateral	\$150.00	\$307.37	\$329.06	\$352.91	\$378.11	\$389.21	\$412.99	\$430.31
D1515	Space maint-fixed-bilateral	\$200.00	\$430.31	\$460.69	\$494.07	\$529.36	\$544.89	\$578.19	\$602.44
D1550	Recementation of space maint	\$30.00	\$66.39	\$71.08	\$76.23	\$81.67	\$84.07	\$89.21	\$92.95
D2140	Amalgam-1 surf. prim/perm	\$52.00	\$143.77	\$155.83	\$175.31	\$181.31	\$190.89	\$208.51	\$229.62
D2150	Amalgam-2 surf. prim/perm	\$64.00	\$186.06	\$201.66	\$226.87	\$234.64	\$247.03	\$269.83	\$297.15
D2160	Amalgam-3 surf. prim/perm	\$77.00	\$224.97	\$243.82	\$274.30	\$283.70	\$298.69	\$326.25	\$359.29
D2161	Amalgam-4+ surf. prim/perm	\$95.00	\$274.02	\$296.99	\$334.11	\$345.56	\$363.81	\$397.39	\$437.63
D2330	Resin-one surface, anterior	\$63.00	\$145.57	\$158.02	\$177.99	\$184.22	\$193.48	\$204.51	\$231.11
D2331	Resin-two surfaces, anterior	\$88.00	\$185.78	\$201.67	\$227.15	\$235.10	\$246.91	\$260.99	\$294.95
D2332	Resin-three surfaces, anterior	\$107.00	\$227.37	\$246.82	\$278.01	\$287.74	\$302.19	\$319.42	\$360.98
D2335	Resin-4+ w/incis angle-anterior	\$138.00	\$268.96	\$291.97	\$328.86	\$340.37	\$357.47	\$377.86	\$427.01
D2390	Resin composite crown, anterior	\$214.00	\$298.08	\$323.57	\$364.46	\$377.22	\$396.16	\$418.76	\$473.23
D2391	Resin composite-1s, posterior	\$180.00	\$170.53	\$185.11	\$208.51	\$215.80	\$226.64	\$239.57	\$270.73
D2392	Resin composite-2s, posterior	\$225.00	\$223.21	\$242.30	\$272.92	\$282.47	\$296.66	\$313.58	\$354.38
D2393	Resin composite-3s, posterior	\$229.00	\$277.28	\$301.00	\$339.03	\$350.90	\$368.52	\$389.54	\$440.22
D2394	Resin composite-4+s, posterior	\$335.00	\$339.67	\$368.72	\$415.32	\$429.85	\$451.44	\$477.19	\$539.27
D2710	Crown-resin composite(indirect)	\$395.00	\$478.32	\$508.33	\$547.68	\$557.69	\$589.05	\$616.30	\$646.41
D2721	Crown-resin w/ most base metal	\$465.00	\$1,104.86	\$1,174.17	\$1,265.06	\$1,288.19	\$1,360.63	\$1,423.57	\$1,493.11
D2740	Crown-porcelain/ceramic subst	\$557.00	\$1,209.96	\$1,285.86	\$1,385.39	\$1,410.72	\$1,490.05	\$1,558.98	\$1,635.13

Brumback Code	Brumback Procedure Description	Brumback Fee	50th Percentile	60th Percentile	75th Percentile	80th Percentile	85th Percentile	90th Percentile	95th Percentile
D2751	Crown-porc fused to base metal	\$497.00	\$1,111.60	\$1,181.33	\$1,272.77	\$1,296.04	\$1,368.92	\$1,432.25	\$1,502.21
D2920	Recement crown	\$52.00	\$96.85	\$107.59	\$118.54	\$125.55	\$127.71	\$135.59	\$151.09
D2930	Prefab stain steel crn-primary	\$132.00	\$264.02	\$293.29	\$323.15	\$342.25	\$348.15	\$369.62	\$411.89
D2931	Prefab stain steel crown-perm	\$155.00	\$298.51	\$331.61	\$365.38	\$386.97	\$393.64	\$417.91	\$465.70
D2932	Prefabricated resin crown	\$165.00	\$318.41	\$353.72	\$389.73	\$412.77	\$419.88	\$445.77	\$496.75
D2933	Prefab stl crown w/resin window	\$206.00	\$364.85	\$405.31	\$446.57	\$472.96	\$481.12	\$510.78	\$569.19
D2940	Protective Restoration	\$54.00	\$100.83	\$112.01	\$123.42	\$130.71	\$132.96	\$141.16	\$157.30
D2950	Crown buildup, includ any pins	\$132.00	\$252.07	\$280.03	\$308.54	\$326.77	\$332.41	\$352.90	\$393.26
D2951	Pin retention-/tooth, (+ rest)	\$32.00	\$57.05	\$63.38	\$69.83	\$73.95	\$75.23	\$79.87	\$89.00
D2954	Prefab post&core in add to crn	\$163.00	\$318.41	\$353.72	\$389.73	\$412.77	\$419.88	\$445.77	\$496.75
D3110	Pulp cap-direct, (+rest)	\$37.00	\$90.75	\$100.83	\$121.50	\$126.04	\$127.30	\$130.28	\$151.88
D3120	Pulp cap-indirect, (+ rest)	\$35.00	\$72.60	\$80.66	\$97.20	\$100.83	\$101.84	\$104.22	\$121.50
D3220	Therapeutic pulpotomy(exc rest)	\$88.00	\$186.03	\$206.70	\$249.08	\$258.38	\$260.96	\$267.07	\$311.34
D3221	Pulpal debridemnt-prim/perm th	\$93.00	\$204.18	\$226.87	\$273.38	\$283.59	\$286.42	\$293.12	\$341.72
D3222	Partial pulpototomy apexogen	\$105.00	\$189.06	\$210.06	\$253.13	\$262.58	\$265.20	\$271.41	\$316.41
D3230	Pulpal therapy-anterior,primary	\$118.00	\$201.32	\$216.50	\$241.40	\$251.65	\$263.25	\$277.99	\$295.18
D3240	Pulpal therapy-posterior, prim	\$133.00	\$247.78	\$266.46	\$297.10	\$309.72	\$324.00	\$342.14	\$363.30
D3310	Root canal therapy - anterior	\$320.00	\$789.80	\$849.33	\$947.01	\$987.24	\$1,032.75	\$1,090.58	\$1,158.01
D3320	Root canal therapy - bicuspid	\$388.00	\$967.89	\$1,040.85	\$1,160.56	\$1,209.86	\$1,265.63	\$1,336.50	\$1,419.13
D3330	Root canal therapy - molar	\$473.00	\$1,200.18	\$1,290.65	\$1,439.09	\$1,500.22	\$1,569.38	\$1,657.26	\$1,759.72
D3331	Treatmnt of root canal obstruct	\$121.00	\$309.72	\$333.07	\$371.38	\$387.15	\$405.00	\$427.68	\$454.12
D3333	Int root repair of perf defects	\$75.00	\$271.01	\$291.44	\$324.96	\$338.76	\$354.38	\$374.22	\$397.36
D3351	Apexification/recalcif, initial	\$159.00	\$430.72	\$479.55	\$498.48	\$562.32	\$589.92	\$730.29	\$867.36
D3352	Apexification/recalcif, interim	\$113.00	\$193.08	\$214.97	\$223.46	\$252.08	\$264.45	\$327.37	\$388.82
D3353	Apexification/recalcif, final	\$209.00	\$594.10	\$661.44	\$687.56	\$775.62	\$813.68	\$1,007.30	\$1,196.36
D3410	Apicoectomy/Periradic surg-ant	\$300.00	\$854.02	\$950.83	\$988.37	\$1,114.95	\$1,169.67	\$1,447.99	\$1,719.77
D3430	Retrograde filling-per root	\$114.00	\$267.35	\$297.65	\$309.40	\$349.03	\$366.16	\$453.29	\$538.36
D4210	Gingivectomy-4+ per quadrant	\$260.00	\$566.61	\$623.88	\$799.92	\$843.75	\$934.16	\$1,066.55	\$1,226.46
D4211	Gingivectomy-1-3 contig th/quad	\$92.00	\$251.83	\$277.28	\$355.52	\$375.00	\$415.18	\$474.02	\$545.09
D4240	Ging flap,root pln, 4+ per quad	\$304.00	\$717.70	\$790.25	\$1,013.23	\$1,068.75	\$1,183.27	\$1,350.97	\$1,553.52
D4241	Ging flap rt pln 1-3 cntg th/qu	\$255.00	\$415.51	\$457.52	\$586.60	\$618.75	\$685.05	\$782.14	\$899.41
D4260	Osseous surgery-4+ per quad	\$276.00	\$1,196.17	\$1,317.09	\$1,688.71	\$1,781.25	\$1,972.11	\$2,251.61	\$2,589.20
D4261	Osseous surg- 1-3 contg th/quad	\$116.00	\$642.16	\$707.07	\$906.57	\$956.25	\$1,058.71	\$1,208.76	\$1,389.99
D4341	Perio scale&root pln-4+per quad	\$95.00	\$221.97	\$241.75	\$274.59	\$292.12	\$306.52	\$323.73	\$371.63
D4342	Perio scale&root pln-1-3th,quad	\$72.00	\$128.51	\$139.96	\$158.97	\$169.12	\$177.46	\$187.42	\$215.16
D4355	Full mouth debridemnt,eval/diag	\$130.00	\$151.88	\$165.41	\$187.87	\$199.87	\$209.73	\$221.50	\$254.27
D4910	Periodontal maintenance	\$149.00	\$136.69	\$148.87	\$169.09	\$179.88	\$188.75	\$199.35	\$228.85
D5110	Complete denture - maxillary	\$749.00	\$1,372.31	\$1,473.46	\$1,729.99	\$1,877.95	\$2,029.58	\$2,232.23	\$2,463.81
D5120	Complete denture - mandibular	\$749.00	\$1,372.31	\$1,473.46	\$1,729.99	\$1,877.95	\$2,029.58	\$2,232.23	\$2,463.81
D5211	Maxillary partial - resin base	\$676.00	\$1,158.20	\$1,243.57	\$1,460.08	\$1,584.95	\$1,712.92	\$1,883.96	\$2,079.40
D5212	Mandibular partial - resin base	\$676.00	\$1,346.02	\$1,445.23	\$1,696.84	\$1,841.97	\$1,990.70	\$2,189.46	\$2,416.60
D5213	Maxil partial-metal Base W/sdls	\$761.00	\$1,516.31	\$1,628.07	\$1,911.52	\$2,075.00	\$2,242.54	\$2,466.46	\$2,722.33
D5214	Mand partial-metal base w/sdls	\$761.00	\$1,516.31	\$1,628.07	\$1,911.52	\$2,075.00	\$2,242.54	\$2,466.46	\$2,722.33
D5225	Maxil partial-flex base incl cl	\$676.00	\$1,158.20	\$1,243.57	\$1,460.08	\$1,584.95	\$1,712.92	\$1,883.96	\$2,079.40
D5226	Mand partial-flex base incl cl	\$676.00	\$1,346.02	\$1,445.23	\$1,696.84	\$1,841.97	\$1,990.70	\$2,189.46	\$2,416.60

Brumback Code	Brumback Procedure Description	Brumback Fee	50th Percentile	60th Percentile	75th Percentile	80th Percentile	85th Percentile	90th Percentile	95th Percentile
D5410	Adjust complete denture-maxil	\$34.00	\$75.13	\$80.66	\$94.71	\$102.81	\$111.11	\$122.20	\$134.88
D5411	Adjust complete denture-mand	\$34.00	\$75.13	\$80.66	\$94.71	\$102.81	\$111.11	\$122.20	\$134.88
D5421	Adjust partial denture-maxil	\$34.00	\$75.13	\$80.66	\$94.71	\$102.81	\$111.11	\$122.20	\$134.88
D5422	Adjust partial denture-mand	\$34.00	\$75.13	\$80.66	\$94.71	\$102.81	\$111.11	\$122.20	\$134.88
D5510	Repair complete denture base	\$107.00	\$150.25	\$161.33	\$189.42	\$205.62	\$222.22	\$244.41	\$269.76
D5520	Replace teeth-comp dent (ea th)	\$95.00	\$125.21	\$134.44	\$157.85	\$171.35	\$185.18	\$203.67	\$224.80
D5610	Repair resin denture base	\$107.00	\$162.77	\$174.77	\$205.20	\$222.75	\$240.74	\$264.77	\$292.24
D5620	Repair cast framework	\$114.00	\$175.30	\$188.22	\$220.98	\$239.88	\$259.25	\$285.14	\$314.72
D5630	Repair or replace broken clasp	\$136.00	\$212.86	\$228.55	\$268.34	\$291.29	\$314.81	\$346.24	\$382.16
D5640	Replace broken teeth-per tooth	\$95.00	\$137.73	\$147.88	\$173.63	\$188.48	\$203.70	\$224.04	\$247.28
D5650	Add tooth to exist part denture	\$102.00	\$187.82	\$201.66	\$236.77	\$257.02	\$277.77	\$305.51	\$337.20
D5660	Add clasp, exist part denture	\$126.00	\$225.38	\$241.99	\$284.12	\$308.42	\$333.33	\$366.61	\$404.64
D5730	Reline complete maxil-chairside	\$153.00	\$314.28	\$337.44	\$396.19	\$430.08	\$464.80	\$511.21	\$564.25
D5731	Reline complete mand-chairside	\$153.00	\$314.28	\$337.44	\$396.19	\$430.08	\$464.80	\$511.21	\$564.25
D5740	Reline maxil partial-chairside	\$153.00	\$287.99	\$309.21	\$363.05	\$394.10	\$425.92	\$468.44	\$517.04
D5741	Reline mand partial-chairside	\$153.00	\$287.99	\$309.21	\$363.05	\$394.10	\$425.92	\$468.44	\$517.04
D5750	Reline complete maxillary (lab)	\$273.00	\$419.46	\$450.37	\$528.78	\$574.01	\$620.36	\$682.30	\$753.08
D5751	Reline complete mand (lab)	\$273.00	\$419.46	\$450.37	\$528.78	\$574.01	\$620.36	\$682.30	\$753.08
D5760	Reline maxillary partial (lab)	\$273.00	\$413.20	\$443.65	\$520.89	\$565.44	\$611.10	\$672.11	\$741.84
D5761	Reline mandibular partial (lab)	\$273.00	\$413.20	\$443.65	\$520.89	\$565.44	\$611.10	\$672.11	\$741.84
D5820	Interim partial denture (maxil)	\$266.00	\$513.37	\$551.20	\$647.17	\$702.52	\$759.24	\$835.05	\$921.68
D6985	Pediatric part'l denture, fixed	\$399.00	\$499.35	\$575.60	\$625.48	\$633.79	\$675.00	\$752.14	\$871.80
D7111	Extraction crnl remnts-decid th	\$64.00	\$124.09	\$134.89	\$152.34	\$164.53	\$172.77	\$193.24	\$224.70
D7140	Extract,erupted th/exposed rt	\$75.00	\$164.94	\$179.30	\$202.50	\$218.70	\$229.66	\$256.86	\$298.69
D7210	Extract, erupted th, rem oth	\$134.00	\$279.70	\$297.45	\$330.72	\$350.90	\$359.28	\$389.81	\$428.53
D7220	Extraction-impacted/soft tis	\$148.00	\$350.72	\$372.97	\$414.69	\$439.99	\$450.49	\$488.78	\$537.32
D7230	Extraction-impacted/part bony	\$184.00	\$466.66	\$496.26	\$551.78	\$585.44	\$599.41	\$650.36	\$714.95
D7240	Extraction-impacted/compl bony	\$230.00	\$547.81	\$582.57	\$647.74	\$687.25	\$703.66	\$763.47	\$839.29
D7241	Remov impact-comp bony w/ comp	\$263.00	\$688.39	\$732.06	\$813.96	\$863.61	\$884.23	\$959.38	\$1,054.67
D7250	Removal residual tooth roots	\$157.00	\$295.64	\$314.40	\$349.57	\$370.90	\$379.75	\$412.03	\$452.95
D7260	Oral antral fistula closure	\$406.00	\$1,743.60	\$1,901.36	\$2,110.15	\$2,169.65	\$2,266.68	\$2,539.36	\$2,835.00
D7261	Prim closure sinus perforation	\$290.00	\$726.50	\$792.24	\$879.23	\$904.02	\$944.45	\$1,058.07	\$1,181.25
D7270	Reimplantation/stabilization	\$245.00	\$544.88	\$594.18	\$659.42	\$678.02	\$708.34	\$793.55	\$885.94
D7280	Exposure of an unerupted tooth	\$227.00	\$508.55	\$554.56	\$615.46	\$632.81	\$661.12	\$740.65	\$826.88
D7283	Plcmnt of devc fo facil erup th	\$264.00	\$217.95	\$237.67	\$263.77	\$271.21	\$283.34	\$317.42	\$354.38
D7310	Alveoloplasty w/ extract- /quad	\$133.00	\$237.01	\$272.83	\$362.48	\$388.80	\$421.08	\$460.85	\$549.64
D7311	Alveoloplasty w/ext 1-3 th/quad	\$184.50	\$207.39	\$238.73	\$317.17	\$340.20	\$368.45	\$403.25	\$480.94
D7320	Alveoloplasty w/o extract /quad	\$194.00	\$385.14	\$443.36	\$589.02	\$631.80	\$684.26	\$748.88	\$893.17
D7510	Incis&drain abscess-intra soft	\$104.00	\$254.79	\$293.30	\$389.66	\$417.96	\$452.66	\$495.42	\$590.87
D7520	Incis&drain abscess-extra soft	\$162.00	\$1,213.50	\$1,396.91	\$1,855.88	\$1,990.66	\$2,155.93	\$2,359.56	\$2,814.17
D7970	Excision, hyperplast tiss-arch	\$227.00	\$474.02	\$545.67	\$724.95	\$777.60	\$842.16	\$921.70	\$1,099.28
D7971	Excision-pericoronal ging /arch	\$75.00	\$177.76	\$204.63	\$271.86	\$291.60	\$315.81	\$345.64	\$412.23
D8070	Comprehensive orth,transitional	\$918.00							
D8080	Comprehensive ortho, adolescent	\$918.00							
D8090	Comprehensive ortho, adult dent	\$918.00							

Brumback Code	Brumback Procedure Description	Brumback Fee	50th Percentile	60th Percentile	75th Percentile	80th Percentile	85th Percentile	90th Percentile	95th Percentile
D8210	Removable appliance therapy	\$261.00							
D8220	Fixed appliance therapy	\$810.00							
D8660	Pre-orthodontic treatment visit	\$157.00							
D8670	Periodic ortho visit (contract)	\$126.00							
D8692	Retainer replacemnt-lost/broken	\$153.00							
D9110	Emerg treatment, palliative	\$125.00	\$100.73	\$101.71	\$115.84	\$132.64	\$156.13	\$167.38	\$200.65
D9220	Deep sedat/gen anesth-1st 30m	\$138.00							
D9221	Deep sedat/gen anesth-ea+15m	\$56.00							
D9230	Analgesia	\$53.00	\$71.59	\$83.68	\$97.64	\$106.10	\$107.78	\$128.31	\$151.09
D9241	IV conscious sed/analg-1st 30m	\$121.00							
D9242	IV conscious sed/analg-ea15m+	\$49.00							
D9248	Non IV conscious sedation	\$120.00	\$104.40	\$122.04	\$142.39	\$154.74	\$157.18	\$187.13	\$220.35
D9310	Consultation-per session	\$44.00	\$110.80	\$111.37	\$127.14	\$151.09	\$166.37	\$210.54	\$243.00
D9420	Hospital Call	\$136.00	\$204.99	\$206.04	\$235.20	\$279.52	\$307.78	\$389.50	\$449.55
D9920	Behavior management, by report	\$58.00							
D9930	Treat complications-postsurgic	\$73.50							
D9951	Occlusal adjustment-limited	\$85.50	\$114.89	\$146.92	\$185.26	\$206.67	\$222.31	\$283.71	\$344.25
D9971	Odontoplasty 1-2 teeth-rmv enam	\$25.00	\$78.40	\$100.25	\$126.41	\$141.02	\$151.69	\$193.59	\$234.90
D0160	Detail/extensive oral eval, B/R	\$0.00	\$167.09	\$182.25	\$206.40	\$215.39	\$231.09	\$247.69	\$268.02
D0170	Limited re-evaluation estab pat	\$0.00	\$55.70	\$60.75	\$68.80	\$71.80	\$77.03	\$82.56	\$89.34
D0171	Re-eval - Post-op Office Visit	\$0.00	\$55.70	\$60.75	\$68.80	\$71.80	\$77.03	\$82.56	\$89.34
D0180	Comprehensive perio evaluation	\$0.00	\$90.51	\$98.72	\$111.80	\$116.67	\$125.17	\$134.17	\$145.17
D0190	Triage	\$0.00	\$47.34	\$51.64	\$58.48	\$61.03	\$65.47	\$70.18	\$75.94
D0190.a	Test	\$0.00							
D0251	Extraoral posterior Xray image	\$0.00	\$43.09	\$46.58	\$53.16	\$56.64	\$59.33	\$62.30	\$69.22
D0277	Vertical bitewings-7 to 8 films	\$0.00	\$90.27	\$99.04	\$113.56	\$115.80	\$119.34	\$124.82	\$133.40
D0310	Saliography	\$0.00	\$333.14	\$367.47	\$421.33	\$445.61	\$465.12	\$489.92	\$536.68
D0320	TMJ arthrogram, incl injection	\$0.00	\$588.55	\$649.19	\$744.35	\$787.24	\$821.71	\$865.52	\$948.13
D0321	Other TMJ films, by report	\$0.00							
D0322	Tomographic survey	\$0.00	\$477.51	\$526.70	\$603.91	\$638.70	\$666.67	\$702.22	\$769.24
D0351	3D Photographic Image	\$0.00	\$55.52	\$61.24	\$70.22	\$74.27	\$77.52	\$81.65	\$89.45
D0393	Treatment sim. using 3D limgs	\$0.00							
D0394	Digital Subtraction of 2+ limgs	\$0.00							
D0395	3D image fusion	\$0.00							
D0414	Lab, microbial specimen, report	\$0.00	\$53.66	\$61.03	\$70.58	\$75.62	\$80.58	\$81.00	\$87.63
D0415	Collection of microorg culture	\$0.00	\$38.91	\$44.24	\$51.17	\$54.83	\$58.42	\$58.73	\$63.53
D0416	Viral Culture	\$0.00	\$57.69	\$65.60	\$75.87	\$81.29	\$86.63	\$87.08	\$94.20
D0417	Collection of saliva sample	\$0.00	\$52.32	\$59.50	\$68.82	\$73.73	\$78.57	\$78.98	\$85.44
D0418	Analysis of saliva sample	\$0.00	\$53.66	\$61.03	\$70.58	\$75.62	\$80.58	\$81.00	\$87.63
D0421	Genetic test-suscept oral dis	\$0.00							
D0422	Sample collection for analysis	\$0.00	\$38.91	\$44.24	\$51.17	\$54.83	\$58.42	\$58.73	\$63.53
D0423	Genetic test-suspect disease	\$0.00							
D0425	Caries susceptibility tests	\$0.00	\$33.54	\$38.14	\$44.11	\$47.26	\$50.37	\$50.63	\$54.77
D0431	Adjunc pre-diag test-detect muc	\$0.00	\$53.66	\$61.03	\$70.58	\$75.62	\$80.58	\$81.00	\$87.63
D0460	Pulp vitality tests	\$0.00	\$53.66	\$61.03	\$70.58	\$75.62	\$80.58	\$81.00	\$87.63

Brumback Code	Brumback Procedure Description	Brumback Fee	50th Percentile	60th Percentile	75th Percentile	80th Percentile	85th Percentile	90th Percentile	95th Percentile
D0472	Accession of tiss, gr exam/rpt	\$0.00	\$73.79	\$83.91	\$97.05	\$103.98	\$110.80	\$111.38	\$120.49
D0473	Acc of tissue, gr mic exam/rpt	\$0.00	\$155.62	\$176.98	\$204.69	\$219.30	\$233.69	\$234.90	\$254.12
D0474	Acc of tiss-gr mic ex surg mar	\$0.00	\$174.40	\$198.33	\$229.39	\$245.77	\$261.90	\$263.25	\$284.79
D0475	Decalcification Procedure	\$0.00	\$93.91	\$106.80	\$123.52	\$132.34	\$141.02	\$141.75	\$153.35
D0476	Special stains for microorg	\$0.00	\$91.23	\$103.74	\$119.99	\$128.56	\$136.99	\$137.70	\$148.97
D0477	Special stains-not for microorg	\$0.00	\$124.77	\$141.89	\$164.10	\$175.82	\$187.36	\$188.33	\$203.73
D0478	Immunohistochemical stains	\$0.00	\$114.03	\$129.68	\$149.99	\$160.70	\$171.24	\$172.13	\$186.21
D0479	Tissue in-situ hybrid-inclu int	\$0.00	\$174.40	\$198.33	\$229.39	\$245.77	\$261.90	\$263.25	\$284.79
D0480	Process/interpret exf cyt smear	\$0.00	\$107.32	\$122.05	\$141.16	\$151.24	\$161.17	\$162.00	\$175.25
D0481	Electron microscopy-diagnostic	\$0.00	\$402.47	\$457.70	\$529.36	\$567.17	\$604.38	\$607.50	\$657.20
D0482	Direct immunofluorescence	\$0.00	\$134.16	\$152.57	\$176.45	\$189.06	\$201.46	\$202.50	\$219.07
D0483	Indirect immunofluorescence	\$0.00	\$134.16	\$152.57	\$176.45	\$189.06	\$201.46	\$202.50	\$219.07
D0484	Consult on slides prp elsewhere	\$0.00	\$201.23	\$228.85	\$264.68	\$283.58	\$302.19	\$303.75	\$328.60
D0485	Consult inc prep/slides biop mt	\$0.00	\$277.70	\$315.81	\$365.26	\$391.35	\$417.02	\$419.18	\$453.47
D0502	Other oral path procedure, B/R	\$0.00							
D0600	Diagnose enamel,dentin,cementum	\$0.00							
D0601	Low risk for caries	\$0.00	\$80.49	\$91.54	\$105.87	\$113.43	\$120.88	\$121.50	\$131.44
D0602	Moderate risk for caries	\$0.00	\$80.49	\$91.54	\$105.87	\$113.43	\$120.88	\$121.50	\$131.44
D0603	High risk for caries	\$0.00	\$80.49	\$91.54	\$105.87	\$113.43	\$120.88	\$121.50	\$131.44
D0999	Unspecified diag procedure, B/R	\$0.00							
D1201	Prophylaxis with fluoride-child	\$0.00							
D1205	Prophylaxis with fluoride-adult	\$0.00							
D1310	Nutritional counseling	\$0.00	\$44.52	\$49.72	\$52.03	\$54.29	\$56.95	\$59.06	\$63.28
D1320	Tobacco counseling	\$0.00	\$48.34	\$53.98	\$56.49	\$58.95	\$61.83	\$64.13	\$68.70
D1353	Sealant repair - per tooth	\$0.00	\$63.61	\$71.03	\$74.33	\$77.56	\$81.36	\$84.38	\$90.40
D1520	Space maint-remov-unilateral	\$0.00	\$338.10	\$361.97	\$388.20	\$415.92	\$428.13	\$454.29	\$473.34
D1525	Space maint-remov-bilateral	\$0.00	\$522.52	\$559.41	\$599.94	\$642.79	\$661.65	\$702.09	\$731.53
D1575	Space maint-fixed-unil,dst shoe	\$0.00	\$338.10	\$361.97	\$388.20	\$415.92	\$428.13	\$454.29	\$473.34
D1999	Unspecified prev procedure, B/R	\$0.00							
D2410	Gold foil-one surface	\$0.00	\$270.61	\$291.78	\$312.54	\$349.68	\$364.85	\$387.52	\$413.58
D2420	Gold foil-two surfaces	\$0.00	\$451.02	\$486.31	\$520.90	\$582.80	\$608.08	\$645.86	\$689.30
D2430	Gold foil-three surfaces	\$0.00	\$781.77	\$842.93	\$902.90	\$1,010.18	\$1,054.01	\$1,119.49	\$1,194.78
D2510	Inlay-metallic-one surface	\$0.00	\$715.62	\$771.61	\$826.50	\$924.70	\$964.82	\$1,024.76	\$1,093.69
D2520	Inlay-metallic-two surfaces	\$0.00	\$811.84	\$875.35	\$937.62	\$1,049.03	\$1,094.55	\$1,162.55	\$1,240.74
D2530	Inlay-metallic-three + surfaces	\$0.00	\$935.72	\$1,008.93	\$1,080.70	\$1,209.11	\$1,261.57	\$1,339.94	\$1,430.07
D2542	Onlay-metallic-two surfaces	\$0.00	\$917.68	\$989.47	\$1,059.86	\$1,185.79	\$1,237.24	\$1,314.11	\$1,402.49
D2543	Onlay-metallic-three surfaces	\$0.00	\$959.78	\$1,034.86	\$1,108.48	\$1,240.19	\$1,294.00	\$1,374.39	\$1,466.83
D2544	Onlay-metallic-four + surfaces	\$0.00	\$998.27	\$1,076.36	\$1,152.93	\$1,289.92	\$1,345.89	\$1,429.50	\$1,525.65
D2610	Inlay-porcel/ceramic-1 surface	\$0.00	\$841.91	\$907.77	\$972.35	\$1,087.88	\$1,135.09	\$1,205.60	\$1,286.69
D2620	Inlay-porcel/ceramic-2 surface	\$0.00	\$888.82	\$958.35	\$1,026.52	\$1,148.49	\$1,198.33	\$1,272.77	\$1,358.38
D2630	Inlay-porcel/ceramic-3+ surface	\$0.00	\$946.55	\$1,020.60	\$1,093.20	\$1,223.09	\$1,276.16	\$1,355.44	\$1,446.61
D2642	Onlay-porcel/ceram-2 surface	\$0.00	\$920.09	\$992.07	\$1,062.64	\$1,188.90	\$1,240.49	\$1,317.55	\$1,406.17
D2643	Onlay-porcel/ceram-3 surface	\$0.00	\$992.25	\$1,069.88	\$1,145.98	\$1,282.15	\$1,337.78	\$1,420.89	\$1,516.46
D2644	Onlay-porcel/ceram-4 + surface	\$0.00	\$1,052.39	\$1,134.72	\$1,215.44	\$1,359.86	\$1,418.86	\$1,507.00	\$1,608.36
D2650	Inlay-resin based composite-1s	\$0.00	\$553.26	\$596.54	\$638.97	\$714.90	\$745.91	\$792.25	\$845.54

Brumback Code	Brumback Procedure Description	Brumback Fee	50th Percentile	60th Percentile	75th Percentile	80th Percentile	85th Percentile	90th Percentile	95th Percentile
D2651	Inlay-resin based composite-2s	\$0.00	\$659.10	\$710.66	\$761.21	\$851.66	\$888.61	\$943.81	\$1,007.30
D2652	Inlay-resin based composite-3+s	\$0.00	\$692.77	\$746.97	\$800.10	\$895.17	\$934.01	\$992.04	\$1,058.76
D2662	Onlay-resin based composite-2s	\$0.00	\$601.37	\$648.41	\$694.54	\$777.06	\$810.78	\$861.15	\$919.07
D2663	Onlay-resin based composite-3s	\$0.00	\$707.21	\$762.53	\$816.77	\$913.82	\$953.47	\$1,012.71	\$1,080.82
D2664	Onlay-resin based composite-4+s	\$0.00	\$757.72	\$817.00	\$875.11	\$979.10	\$1,021.58	\$1,085.04	\$1,158.02
D2712	Crown-3/4 resin-based comp-ind	\$0.00	\$478.32	\$508.33	\$547.68	\$557.69	\$589.05	\$616.30	\$646.41
D2720	Crown-resin w/high noble metal	\$0.00	\$1,178.97	\$1,252.92	\$1,349.91	\$1,374.59	\$1,451.89	\$1,519.05	\$1,593.25
D2722	Crown-resin with noble metal	\$0.00	\$1,129.11	\$1,199.94	\$1,292.82	\$1,316.46	\$1,390.49	\$1,454.82	\$1,525.88
D2750	Crown-porc fuse high noble mtl	\$0.00	\$1,193.79	\$1,268.67	\$1,366.88	\$1,391.87	\$1,470.14	\$1,538.15	\$1,613.28
D2752	Crown-porc fused noble metal	\$0.00	\$1,138.54	\$1,209.96	\$1,303.62	\$1,327.46	\$1,402.11	\$1,466.97	\$1,538.63
D2780	Crown-3/4 cast high noble metal	\$0.00	\$1,145.28	\$1,217.12	\$1,311.34	\$1,335.32	\$1,410.41	\$1,475.65	\$1,547.73
D2781	Crown-3/4 cast most base metal	\$0.00	\$1,077.91	\$1,145.53	\$1,234.20	\$1,256.77	\$1,327.44	\$1,388.85	\$1,456.69
D2782	Crown-3/4 cast noble metal	\$0.00	\$1,112.94	\$1,182.76	\$1,274.31	\$1,297.61	\$1,370.58	\$1,433.99	\$1,504.03
D2783	Crown-3/4 porcelain/ceramic	\$0.00	\$1,177.62	\$1,251.49	\$1,348.36	\$1,373.02	\$1,450.23	\$1,517.32	\$1,591.43
D2790	Crown-full cast high noble mtl	\$0.00	\$1,152.02	\$1,224.28	\$1,319.05	\$1,343.17	\$1,418.70	\$1,484.33	\$1,556.84
D2791	Crown-full cast base metal	\$0.00	\$1,091.39	\$1,159.85	\$1,249.63	\$1,272.48	\$1,344.03	\$1,406.21	\$1,474.90
D2792	Crown-full cast noble metal	\$0.00	\$1,111.60	\$1,181.33	\$1,272.77	\$1,296.04	\$1,368.92	\$1,432.25	\$1,502.21
D2794	Crown-titanium	\$0.00	\$1,178.97	\$1,252.92	\$1,349.91	\$1,374.59	\$1,451.89	\$1,519.05	\$1,593.25
D2799	Provisional crown	\$0.00	\$478.32	\$508.33	\$547.68	\$557.69	\$589.05	\$616.30	\$646.41
D2910	Recement inlay/onlay/partial	\$0.00	\$95.52	\$106.12	\$116.92	\$123.83	\$125.97	\$133.73	\$149.02
D2915	Recemnt cast or prefab pst/cor	\$0.00	\$95.52	\$106.12	\$116.92	\$123.83	\$125.97	\$133.73	\$149.02
D2921	Reattach Th Fragment, incisal	\$0.00	\$139.30	\$154.75	\$170.51	\$180.59	\$183.70	\$195.03	\$217.33
D2934	Prefb esth ctd stnl stl crn-prm	\$0.00	\$364.85	\$405.31	\$446.57	\$472.96	\$481.12	\$510.78	\$569.19
D2941	Interim Therapeutic Rest - Prim	\$0.00	\$100.83	\$112.01	\$123.42	\$130.71	\$132.96	\$141.16	\$157.30
D2949	Foundation for Indirect Rest	\$0.00	\$100.83	\$112.01	\$123.42	\$130.71	\$132.96	\$141.16	\$157.30
D2952	Cast post & core in add to crown	\$0.00	\$398.01	\$442.15	\$487.17	\$515.96	\$524.86	\$557.22	\$620.94
D2953	Each add'l cast post-same tooth	\$0.00	\$199.01	\$221.08	\$243.58	\$257.98	\$262.43	\$278.61	\$310.47
D2955	Post removal (not with endo)	\$0.00	\$245.44	\$272.66	\$300.42	\$318.17	\$323.66	\$343.62	\$382.91
D2957	Each + prefab post-same tooth	\$0.00	\$159.21	\$176.86	\$194.87	\$206.38	\$209.94	\$222.89	\$248.37
D2960	Labial veneer(laminate)-chairsd	\$0.00	\$769.49	\$854.83	\$941.86	\$997.52	\$1,014.72	\$1,077.29	\$1,200.48
D2961	Labial veneer (resin lamin)-lab	\$0.00	\$872.98	\$969.79	\$1,068.52	\$1,131.67	\$1,151.18	\$1,222.16	\$1,361.92
D2962	Labial veneer (porceln lam)-lab	\$0.00	\$948.60	\$1,053.80	\$1,161.08	\$1,229.70	\$1,250.91	\$1,328.03	\$1,479.90
D2971	Add'l prc-new crn undr exs dent	\$0.00	\$152.57	\$169.49	\$186.75	\$197.78	\$201.19	\$213.60	\$238.03
D2975	Coping	\$0.00	\$464.35	\$515.84	\$568.36	\$601.95	\$612.33	\$650.09	\$724.43
D2980	Crown repair, by report	\$0.00	\$185.74	\$206.34	\$227.34	\$240.78	\$244.93	\$260.03	\$289.77
D2999	Unspecif restorative proced B/R	\$0.00							
D3332	Incomplt endo ther-inopbl/unres	\$0.00	\$588.48	\$632.84	\$705.62	\$735.59	\$769.50	\$812.59	\$862.83
D3346	Retreat, prev RCT - anterior	\$0.00	\$1,053.06	\$1,132.44	\$1,262.69	\$1,316.32	\$1,377.00	\$1,454.11	\$1,544.01
D3347	Retreat, prev RCT - bicuspid	\$0.00	\$1,238.90	\$1,332.29	\$1,485.51	\$1,548.62	\$1,620.00	\$1,710.72	\$1,816.49
D3348	Retreat, prev RCT - molar	\$0.00	\$1,533.13	\$1,648.71	\$1,838.32	\$1,916.41	\$2,004.75	\$2,117.02	\$2,247.90
D3354	Pulpal Regeneration	\$0.00							
D3355	Pulpal Regeneration - 1st visit	\$0.00	\$430.72	\$479.55	\$498.48	\$562.32	\$589.92	\$730.29	\$867.36
D3356	Pulpal Rgn - interim med Replc	\$0.00	\$193.08	\$214.97	\$223.46	\$252.08	\$264.45	\$327.37	\$388.82
D3357	Pulpal Regen - completion	\$0.00							
D3421	Apicoect/Perirad-bicus/1st root	\$0.00	\$950.56	\$1,058.31	\$1,100.10	\$1,240.99	\$1,301.89	\$1,611.68	\$1,914.18

Brumback Code	Brumback Procedure Description	Brumback Fee	50th Percentile	60th Percentile	75th Percentile	80th Percentile	85th Percentile	90th Percentile	95th Percentile
D3425	Apicoect/Perirad-molar/1st root	\$0.00	\$1,076.81	\$1,198.87	\$1,246.20	\$1,405.80	\$1,474.80	\$1,825.73	\$2,168.41
D3426	Apicoect/Perirad (each + root)	\$0.00	\$363.89	\$405.13	\$421.13	\$475.06	\$498.38	\$616.97	\$732.77
D3428	Bone Graft w/Perirdc Srg 1 Site	\$0.00	\$1,125.82	\$1,253.44	\$1,302.93	\$1,469.79	\$1,541.92	\$1,908.83	\$2,267.11
D3429	Bn Graft w/Berirdc Srg each add	\$0.00	\$1,073.84	\$1,195.56	\$1,242.76	\$1,401.93	\$1,470.73	\$1,820.69	\$2,162.43
D3431	Bio Mtrl to aid Reg w/Prdc Srg	\$0.00	\$1,321.87	\$1,471.71	\$1,529.82	\$1,725.75	\$1,810.44	\$2,241.24	\$2,661.91
D3432	Guided TissRgn PerSite w/PrdSrg	\$0.00	\$1,136.22	\$1,265.01	\$1,314.96	\$1,483.37	\$1,556.16	\$1,926.46	\$2,288.05
D3450	Root amputation-per root	\$0.00	\$556.97	\$620.10	\$644.59	\$727.14	\$762.83	\$944.34	\$1,121.59
D3460	Endodontic endosseous implant	\$0.00	\$2,079.35	\$2,315.05	\$2,406.46	\$2,714.66	\$2,847.88	\$3,525.55	\$4,187.27
D3470	Intentional replant, inc splint	\$0.00	\$1,061.95	\$1,182.33	\$1,229.01	\$1,386.41	\$1,454.45	\$1,800.55	\$2,138.50
D3910	Surg isolation of th w/rub dam	\$0.00	\$148.53	\$165.36	\$171.89	\$193.90	\$203.42	\$251.83	\$299.09
D3920	Hemisection, no root can ther	\$0.00	\$423.30	\$471.28	\$489.89	\$552.63	\$579.75	\$717.70	\$852.41
D3950	Canal prep/fit of dowel/post	\$0.00	\$193.08	\$214.97	\$223.46	\$252.08	\$264.45	\$327.37	\$388.82
D3999	Unspecified endo procedure, B/R	\$0.00							
D4245	Apically positioned flap	\$0.00	\$528.83	\$582.29	\$746.59	\$787.50	\$871.88	\$995.45	\$1,144.70
D4249	Clinic crown lengthen-hard tiss	\$0.00	\$786.96	\$866.51	\$1,110.99	\$1,171.88	\$1,297.44	\$1,481.33	\$1,703.42
D4263	Bone replace graft-1st site/qu	\$0.00	\$428.10	\$471.38	\$604.38	\$637.50	\$705.81	\$805.84	\$926.66
D4264	Bone replace graft-each add/qu	\$0.00	\$365.15	\$402.06	\$515.50	\$543.75	\$602.01	\$687.33	\$790.39
D4265	Bio mat, sft&osseous tiss regen	\$0.00							
D4266	Guided tiss regen-resorb-per	\$0.00	\$440.70	\$485.24	\$622.16	\$656.25	\$726.57	\$829.54	\$953.91
D4267	Guided tiss regen-nonresorb-per	\$0.00	\$566.61	\$623.88	\$799.92	\$843.75	\$934.16	\$1,066.55	\$1,226.46
D4268	Surg revision proc, per tooth	\$0.00							
D4270	Pedicle soft tissue graft proc	\$0.00	\$849.91	\$935.83	\$1,199.87	\$1,265.63	\$1,401.24	\$1,599.83	\$1,839.69
D4271	Free soft tissue graft proced	\$0.00							
D4273	Subepithelial con tis graft/th	\$0.00	\$1,038.78	\$1,143.79	\$1,466.51	\$1,546.88	\$1,712.63	\$1,955.35	\$2,248.51
D4274	Mesial/distal wedge procedure	\$0.00	\$589.27	\$648.84	\$831.91	\$877.50	\$971.53	\$1,109.22	\$1,275.52
D4275	Soft tissue allograft	\$0.00	\$780.66	\$859.57	\$1,102.11	\$1,162.50	\$1,287.06	\$1,469.47	\$1,689.79
D4276	Comb cnct tiss&dbl pedicle grft	\$0.00	\$1,164.70	\$1,282.43	\$1,644.27	\$1,734.38	\$1,920.22	\$2,192.36	\$2,521.06
D4283	Autgen con tiss graft, Each Add	\$0.00	\$885.17	\$974.65	\$1,249.65	\$1,318.13	\$1,459.36	\$1,666.19	\$1,916.01
D4285	Non-autgen con tis grft, Ea Add	\$0.00	\$666.08	\$733.41	\$940.35	\$991.88	\$1,098.16	\$1,253.79	\$1,441.77
D4320	Provisional splinting-intracor	\$0.00	\$385.53	\$419.89	\$476.91	\$507.36	\$532.38	\$562.27	\$645.47
D4321	Provisional splinting-extracor	\$0.00	\$350.48	\$381.71	\$433.56	\$461.24	\$483.98	\$511.16	\$586.79
D4346	Scale,gingival inflam-full mth	\$0.00	\$128.51	\$139.96	\$158.97	\$169.12	\$177.46	\$187.42	\$215.16
D4381	Local deliv antimicrb ag-th B/R	\$0.00							
D4920	Unscheduled dressing change	\$0.00	\$99.30	\$108.15	\$122.84	\$130.68	\$137.13	\$144.83	\$166.26
D4921	Gingival Irrigation - Per Quad	\$0.00							
D4999	Unspecified perio proced, B/R	\$0.00							
D5130	Immediate denture - maxillary	\$0.00	\$1,496.27	\$1,606.56	\$1,886.26	\$2,047.58	\$2,212.91	\$2,433.87	\$2,686.36
D5140	Immediate denture - mandibular	\$0.00	\$1,496.27	\$1,606.56	\$1,886.26	\$2,047.58	\$2,212.91	\$2,433.87	\$2,686.36
D5221	Immed maxil partl dent w/resin	\$0.00	\$1,263.38	\$1,356.50	\$1,592.67	\$1,728.88	\$1,868.48	\$2,055.04	\$2,268.23
D5222	Immed mand partl dent w/resin	\$0.00	\$1,467.47	\$1,575.64	\$1,849.96	\$2,008.18	\$2,170.32	\$2,387.02	\$2,634.66
D5223	lmd Max part-cast metl w/resin	\$0.00	\$1,652.79	\$1,774.61	\$2,083.57	\$2,261.77	\$2,444.39	\$2,688.46	\$2,967.36
D5224	lmd Mand part-cast metl w/resin	\$0.00	\$1,652.79	\$1,774.61	\$2,083.57	\$2,261.77	\$2,444.39	\$2,688.46	\$2,967.36
D5281	Removable unilat part denture	\$0.00	\$883.99	\$949.15	\$1,114.39	\$1,209.70	\$1,307.38	\$1,437.92	\$1,587.09
D5670	Replace all th&acrylic-maxil	\$0.00	\$550.93	\$591.54	\$694.52	\$753.92	\$814.80	\$896.15	\$989.12
D5671	Replace all th&acrylic-mand	\$0.00	\$550.93	\$591.54	\$694.52	\$753.92	\$814.80	\$896.15	\$989.12

Brumback Code	Brumback Procedure Description	Brumback Fee	50th Percentile	60th Percentile	75th Percentile	80th Percentile	85th Percentile	90th Percentile	95th Percentile
D5710	Rebase complete maxil denture	\$0.00	\$557.19	\$598.26	\$702.41	\$762.49	\$824.06	\$906.34	\$1,000.36
D5711	Rebase complete mand denture	\$0.00	\$532.15	\$571.37	\$670.85	\$728.22	\$787.02	\$865.60	\$955.40
D5720	Rebase maxil partial denture	\$0.00	\$525.89	\$564.65	\$662.95	\$719.65	\$777.76	\$855.42	\$944.16
D5721	Rebase mand partial denture	\$0.00	\$525.89	\$564.65	\$662.95	\$719.65	\$777.76	\$855.42	\$944.16
D5810	Interim comp denture (maxil)	\$0.00	\$663.62	\$712.53	\$836.58	\$908.13	\$981.46	\$1,079.46	\$1,191.44
D5811	Interim comp denture (mand)	\$0.00	\$713.70	\$766.31	\$899.72	\$976.67	\$1,055.53	\$1,160.92	\$1,281.36
D5821	Interim partial denture (mand)	\$0.00	\$544.67	\$584.81	\$686.63	\$745.36	\$805.54	\$885.97	\$977.88
D5850	Tissue condition, maxillary	\$0.00	\$131.47	\$141.16	\$165.74	\$179.91	\$194.44	\$213.85	\$236.04
D5851	Tissue condition, mandibular	\$0.00	\$131.47	\$141.16	\$165.74	\$179.91	\$194.44	\$213.85	\$236.04
D5860	Overdenture-complete, B/R	\$0.00							
D5861	Overdenture-partial, by report	\$0.00							
D5862	Precision attachment, B/R	\$0.00							
D5863	Overdenture - Complete Max	\$0.00	\$1,452.45	\$1,559.50	\$1,831.01	\$1,987.61	\$2,148.10	\$2,362.58	\$2,607.68
D5864	Overdenture - Partial Max	\$0.00	\$1,915.73	\$2,056.93	\$2,415.04	\$2,621.59	\$2,833.27	\$3,116.17	\$3,439.44
D5865	Overdenture - Complete Mand	\$0.00	\$1,452.45	\$1,559.50	\$1,831.01	\$1,987.61	\$2,148.10	\$2,362.58	\$2,607.68
D5866	Overdenture - Partial Mand	\$0.00	\$1,990.85	\$2,137.60	\$2,509.75	\$2,724.40	\$2,944.38	\$3,238.37	\$3,574.32
D5867	Replcmt prec attachmt-part/full	\$0.00							
D5875	Mod of removble prosth-post surg	\$0.00							
D5899	Unspecified remove prosth, B/R	\$0.00							
D5911	Facial moulage (sectional)	\$0.00	\$348.09	\$373.74	\$438.81	\$476.34	\$514.80	\$566.21	\$624.94
D5912	Facial moulage (complete)	\$0.00	\$348.09	\$373.74	\$438.81	\$476.34	\$514.80	\$566.21	\$624.94
D5913	Nasal prosthesis	\$0.00	\$7,329.85	\$7,870.12	\$9,240.30	\$10,030.59	\$10,840.50	\$11,922.90	\$13,159.79
D5914	Auricular prosthesis	\$0.00	\$7,329.85	\$7,870.12	\$9,240.30	\$10,030.59	\$10,840.50	\$11,922.90	\$13,159.79
D5915	Orbital prosthesis	\$0.00	\$9,919.22	\$10,650.34	\$12,504.56	\$13,574.03	\$14,670.04	\$16,134.82	\$17,808.66
D5916	Ocular prosthesis	\$0.00	\$2,645.71	\$2,840.72	\$3,335.29	\$3,620.54	\$3,912.87	\$4,303.57	\$4,750.02
D5919	Facial prosthesis	\$0.00							
D5922	Nasal septal prosthesis	\$0.00							
D5923	Ocular prosthesis, interim	\$0.00							
D5924	Cranial prosthesis	\$0.00							
D5925	Facial augmentat implant,prosth	\$0.00							
D5926	Nasal prosthesis, replacement	\$0.00							
D5927	Auricular prosthesis,replacemen	\$0.00							
D5928	Orbital prosthesis, replacement	\$0.00							
D5929	Facial prosthesis, replacement	\$0.00							
D5931	Obturator prosthesis, surgical	\$0.00	\$3,946.65	\$4,237.55	\$4,975.31	\$5,400.83	\$5,836.91	\$6,419.71	\$7,085.70
D5932	Obturator prosthesis,definitive	\$0.00	\$7,381.19	\$7,925.24	\$9,305.02	\$10,100.85	\$10,916.42	\$12,006.41	\$13,251.96
D5933	Obturator prosthesis, modificat	\$0.00							
D5934	Mandibular resection w/ flange	\$0.00	\$6,727.59	\$7,223.46	\$8,481.07	\$9,206.42	\$9,949.78	\$10,943.24	\$12,078.50
D5935	Mandibular resection w/o flange	\$0.00	\$5,853.61	\$6,285.07	\$7,379.30	\$8,010.43	\$8,657.21	\$9,521.62	\$10,509.40
D5936	Obturator prosthesis, interim	\$0.00	\$6,574.83	\$7,059.44	\$8,288.49	\$8,997.38	\$9,723.85	\$10,694.76	\$11,804.25
D5937	Trismus appliance (not TMD)	\$0.00	\$826.39	\$887.30	\$1,041.78	\$1,130.88	\$1,222.19	\$1,344.23	\$1,483.68
D5951	Feeding aid	\$0.00	\$1,074.31	\$1,153.50	\$1,354.32	\$1,470.15	\$1,588.85	\$1,747.50	\$1,928.78
D5952	Speech aid prosthesis,pediatric	\$0.00	\$3,488.38	\$3,745.50	\$4,397.59	\$4,773.70	\$5,159.14	\$5,674.27	\$6,262.93
D5953	Speech aid prosthesis, adult	\$0.00	\$6,624.91	\$7,113.22	\$8,351.63	\$9,065.92	\$9,797.93	\$10,776.23	\$11,894.17
D5954	Palatal augmentation prosthesis	\$0.00	\$6,139.10	\$6,591.59	\$7,739.19	\$8,401.09	\$9,079.42	\$9,985.99	\$11,021.94

Brumback Code	Brumback Procedure Description	Brumback Fee	50th Percentile	60th Percentile	75th Percentile	80th Percentile	85th Percentile	90th Percentile	95th Percentile
D5955	Palatal lift prosth, definitive	\$0.00	\$5,678.32	\$6,096.85	\$7,158.32	\$7,770.54	\$8,397.96	\$9,236.48	\$10,194.68
D5958	Palatal lift prosthesis,interim	\$0.00							
D5959	Palatal lift prosth, modificat	\$0.00							
D5960	Speech aid prosth, modification	\$0.00							
D5982	Surgical stent	\$0.00	\$557.19	\$598.26	\$702.41	\$762.49	\$824.06	\$906.34	\$1,000.36
D5983	Radiation carrier	\$0.00	\$1,252.11	\$1,344.40	\$1,578.46	\$1,713.46	\$1,851.81	\$2,036.71	\$2,248.00
D5984	Radiation shield	\$0.00	\$1,252.11	\$1,344.40	\$1,578.46	\$1,713.46	\$1,851.81	\$2,036.71	\$2,248.00
D5985	Radiation cone locator	\$0.00	\$1,252.11	\$1,344.40	\$1,578.46	\$1,713.46	\$1,851.81	\$2,036.71	\$2,248.00
D5986	Fluoride gel carrier	\$0.00	\$125.21	\$134.44	\$157.85	\$171.35	\$185.18	\$203.67	\$224.80
D5987	Commissure splint	\$0.00	\$1,878.17	\$2,016.60	\$2,367.69	\$2,570.19	\$2,777.72	\$3,055.07	\$3,372.00
D5988	Surgical splint	\$0.00	\$375.63	\$403.32	\$473.54	\$514.04	\$555.54	\$611.01	\$674.40
D5991	Topical medicament carrier	\$0.00	\$143.99	\$154.61	\$181.52	\$197.05	\$212.96	\$234.22	\$258.52
D5992	Adj Max'facial Prosth, Report	\$0.00							
D5993	Maint Max'facial Prosth, Report	\$0.00							
D5994	Periodontal medicament carrier	\$0.00	\$143.99	\$154.61	\$181.52	\$197.05	\$212.96	\$234.22	\$258.52
D5999	Unspec maxillofacial prosth B/R	\$0.00							
D6010	Surg place implant: endosteal	\$0.00	\$2,292.61	\$2,461.60	\$2,890.16	\$3,137.35	\$3,390.66	\$3,729.22	\$4,116.09
D6011	Second stage implant surgery	\$0.00							
D6013	Placement of mini implant	\$0.00	\$2,292.61	\$2,461.60	\$2,890.16	\$3,137.35	\$3,390.66	\$3,729.22	\$4,116.09
D6040	Surgic place: epostal implant	\$0.00	\$7,888.29	\$8,469.72	\$9,944.30	\$10,794.80	\$11,666.40	\$12,831.27	\$14,162.40
D6050	Surg place: transosteal implant	\$0.00	\$5,884.92	\$6,318.68	\$7,418.76	\$8,053.26	\$8,703.51	\$9,572.54	\$10,565.60
D6052	Semi-precision atthcmt abutment	\$0.00	\$971.64	\$1,043.25	\$1,224.88	\$1,329.64	\$1,437.00	\$1,580.49	\$1,744.45
D6053	Imp/abut remov,comp edent arch	\$0.00							
D6054	Imp/abut remov,part edent arch	\$0.00							
D6055	Dent implant sup connecting bar	\$0.00	\$688.66	\$739.42	\$868.15	\$942.40	\$1,018.50	\$1,120.19	\$1,236.40
D6056	Prefab abutment-incl placement	\$0.00	\$475.80	\$510.87	\$599.81	\$651.11	\$703.69	\$773.95	\$854.24
D6057	Custom abutment-incl placement	\$0.00	\$588.49	\$631.87	\$741.88	\$805.33	\$870.35	\$957.25	\$1,056.56
D6058	Abutment supported porc/cer crn	\$0.00	\$1,319.72	\$1,417.00	\$1,663.70	\$1,805.99	\$1,951.81	\$2,146.69	\$2,369.39
D6059	Abtmt supp porc fused to hi-nob	\$0.00	\$1,302.19	\$1,398.18	\$1,641.60	\$1,782.00	\$1,925.88	\$2,118.18	\$2,337.92
D6060	Abtmt supp porc fused-base metl	\$0.00	\$1,230.82	\$1,321.55	\$1,551.63	\$1,684.33	\$1,820.33	\$2,002.09	\$2,209.78
D6061	Abtmt supp porc fused-mtl crown	\$0.00	\$1,255.87	\$1,348.43	\$1,583.20	\$1,718.60	\$1,857.37	\$2,042.82	\$2,254.74
D6062	Abtmt supp cast mtl crown-hinob	\$0.00	\$1,250.86	\$1,343.06	\$1,576.88	\$1,711.75	\$1,849.96	\$2,034.67	\$2,245.75
D6063	Abtmt supp cast mtl crown-base	\$0.00	\$1,089.34	\$1,169.63	\$1,373.26	\$1,490.71	\$1,611.07	\$1,771.94	\$1,955.76
D6064	Abtmt supp cast mtl crown-noble	\$0.00	\$1,139.42	\$1,223.40	\$1,436.40	\$1,559.25	\$1,685.15	\$1,853.41	\$2,045.68
D6065	Implant supp porc/cer crown	\$0.00	\$1,298.44	\$1,394.14	\$1,636.86	\$1,776.86	\$1,920.33	\$2,112.07	\$2,331.18
D6066	Implant supp porc fused mtl crn	\$0.00	\$1,264.63	\$1,357.84	\$1,594.24	\$1,730.59	\$1,870.33	\$2,057.08	\$2,270.48
D6067	Implant supported metal crown	\$0.00	\$1,227.07	\$1,317.51	\$1,546.89	\$1,679.19	\$1,814.77	\$1,995.98	\$2,203.04
D6068	Abtmt supp ret for porc/cer FPD	\$0.00	\$1,308.45	\$1,404.90	\$1,649.49	\$1,790.57	\$1,935.14	\$2,128.36	\$2,349.16
D6069	Abut sup ret-porc fsd mtl FPDhn	\$0.00	\$1,302.19	\$1,398.18	\$1,641.60	\$1,782.00	\$1,925.88	\$2,118.18	\$2,337.92
D6070	Abut sup ret-porc fsd mtl FPDbm	\$0.00	\$1,230.82	\$1,321.55	\$1,551.63	\$1,684.33	\$1,820.33	\$2,002.09	\$2,209.78
D6071	Abut sup ret-porc fsd mtl FPDno	\$0.00	\$1,255.87	\$1,348.43	\$1,583.20	\$1,718.60	\$1,857.37	\$2,042.82	\$2,254.74
D6072	Abut sup ret-cast mtl FPD-hinob	\$0.00	\$1,270.89	\$1,364.57	\$1,602.14	\$1,739.16	\$1,879.59	\$2,067.26	\$2,281.72
D6073	Abut sup ret-cast mtl FPD-base	\$0.00	\$1,160.71	\$1,246.26	\$1,463.23	\$1,588.38	\$1,716.63	\$1,888.03	\$2,083.90
D6074	Abut sup ret-cast mtl FPD-noble	\$0.00	\$1,233.33	\$1,324.23	\$1,554.78	\$1,687.76	\$1,824.03	\$2,006.16	\$2,214.28
D6075	Implant supp ret-ceramic FPD	\$0.00	\$1,298.44	\$1,394.14	\$1,636.86	\$1,776.86	\$1,920.33	\$2,112.07	\$2,331.18

Brumback Code	Brumback Procedure Description	Brumback Fee	50th Percentile	60th Percentile	75th Percentile	80th Percentile	85th Percentile	90th Percentile	95th Percentile
D6076	Implnt supp ret-prc fuse mtlIFPD	\$0.00	\$1,264.63	\$1,357.84	\$1,594.24	\$1,730.59	\$1,870.33	\$2,057.08	\$2,270.48
D6077	Implant supp ret-cast metal FPD	\$0.00	\$1,227.07	\$1,317.51	\$1,546.89	\$1,679.19	\$1,814.77	\$1,995.98	\$2,203.04
D6078	Implnt/abut supp fxd comp edent	\$0.00							
D6079	Implnt/abut supp fxd part edent	\$0.00							
D6080	Implant maintenance procedures	\$0.00	\$107.68	\$115.62	\$135.75	\$147.36	\$159.26	\$175.16	\$193.33
D6081	Scaling/debridement of implant	\$0.00	\$55.09	\$59.15	\$69.45	\$75.39	\$81.48	\$89.62	\$98.91
D6085	Provisional implant crown	\$0.00	\$378.14	\$406.01	\$476.69	\$517.46	\$559.25	\$615.09	\$678.90
D6090	Repair implant sup prosth, B/R	\$0.00	\$12,521.10	\$13,444.00	\$15,784.60	\$17,134.60	\$18,518.10	\$20,367.10	\$22,480.00
D6094	Abutment supp crown - titanium	\$0.00	\$1,032.99	\$1,109.13	\$1,302.23	\$1,413.60	\$1,527.74	\$1,680.29	\$1,854.60
D6095	Repair implant abutment, B/R	\$0.00							
D6100	Implant removal, by report	\$0.00							
D6110	Imp/abt sup RD - ednt max	\$0.00	\$1,711.63	\$1,837.79	\$2,157.75	\$2,342.30	\$2,531.42	\$2,784.18	\$3,073.02
D6111	Imp/abt sup RD - ednt mand	\$0.00	\$1,711.63	\$1,837.79	\$2,157.75	\$2,342.30	\$2,531.42	\$2,784.18	\$3,073.02
D6112	Imp/abt sup RD - Part-ednt max	\$0.00	\$1,711.63	\$1,837.79	\$2,157.75	\$2,342.30	\$2,531.42	\$2,784.18	\$3,073.02
D6113	Imp/abt sup RD - Part-ednt mand	\$0.00	\$1,711.63	\$1,837.79	\$2,157.75	\$2,342.30	\$2,531.42	\$2,784.18	\$3,073.02
D6114	Imp/abt sup FD - ednt max	\$0.00	\$2,997.55	\$3,218.49	\$3,778.83	\$4,102.02	\$4,433.23	\$4,875.88	\$5,381.71
D6115	Imp/abt sup FD - ednt mand	\$0.00	\$2,997.55	\$3,218.49	\$3,778.83	\$4,102.02	\$4,433.23	\$4,875.88	\$5,381.71
D6116	Imp/abt sup FD - Part-ednt max	\$0.00	\$2,298.87	\$2,468.32	\$2,898.05	\$3,145.91	\$3,399.92	\$3,739.40	\$4,127.33
D6117	Imp/abt sup FD - Part-ednt mand	\$0.00	\$2,298.87	\$2,468.32	\$2,898.05	\$3,145.91	\$3,399.92	\$3,739.40	\$4,127.33
D6190	Radiograph/surg impl index B/R	\$0.00	\$231.64	\$248.71	\$292.02	\$316.99	\$342.58	\$376.79	\$415.88
D6194	Abut sup ret-cast mtl FPD-titan	\$0.00	\$1,064.29	\$1,142.74	\$1,341.69	\$1,456.44	\$1,574.04	\$1,731.20	\$1,910.80
D6199	Unspecified implant proced, B/R	\$0.00	\$12,521.10	\$13,444.00	\$15,784.60	\$17,134.60	\$18,518.10	\$20,367.10	\$22,480.00
D6205	Pontic-indirect res based comp	\$0.00	\$768.11	\$801.50	\$867.43	\$894.12	\$918.86	\$979.43	\$1,033.27
D6210	Pontic-cast high noble metal	\$0.00	\$1,174.32	\$1,225.37	\$1,326.17	\$1,366.98	\$1,404.80	\$1,497.40	\$1,579.71
D6211	Pontic-cast predominantly base	\$0.00	\$1,100.46	\$1,148.31	\$1,242.76	\$1,281.01	\$1,316.44	\$1,403.22	\$1,480.36
D6212	Pontic-cast noble metal	\$0.00	\$1,144.78	\$1,194.55	\$1,292.81	\$1,332.59	\$1,369.46	\$1,459.73	\$1,539.97
D6214	Pontic-titanium	\$0.00	\$1,181.70	\$1,233.08	\$1,334.51	\$1,375.58	\$1,413.63	\$1,506.82	\$1,589.65
D6240	Pontic-porcelain fused to knob	\$0.00	\$1,159.55	\$1,209.96	\$1,309.49	\$1,349.78	\$1,387.13	\$1,478.56	\$1,559.84
D6241	Pontic-porcelain fused to base	\$0.00	\$1,070.92	\$1,117.48	\$1,209.40	\$1,246.62	\$1,281.10	\$1,365.55	\$1,440.62
D6242	Pontic-porcelain fused to nobl	\$0.00	\$1,130.00	\$1,179.13	\$1,276.13	\$1,315.39	\$1,351.79	\$1,440.89	\$1,520.10
D6245	Pontic-porcelain/ceramic	\$0.00	\$1,196.48	\$1,248.49	\$1,351.19	\$1,392.77	\$1,431.30	\$1,525.65	\$1,609.52
D6250	Pontic-resin w/ high noble met	\$0.00	\$1,144.78	\$1,194.55	\$1,292.81	\$1,332.59	\$1,369.46	\$1,459.73	\$1,539.97
D6251	Pontic-resin w/ predomnt base	\$0.00	\$1,056.15	\$1,102.07	\$1,192.72	\$1,229.42	\$1,263.43	\$1,346.72	\$1,420.75
D6252	Pontic-resin with noble metal	\$0.00	\$1,090.12	\$1,137.52	\$1,231.09	\$1,268.97	\$1,304.08	\$1,390.04	\$1,466.45
D6253	Provisional pontic	\$0.00	\$493.36	\$514.81	\$557.16	\$574.30	\$590.19	\$629.10	\$663.68
D6254	Interim Pontic	\$0.00							
D6545	Retainer-cast for resin bonded	\$0.00	\$430.79	\$447.49	\$497.13	\$505.71	\$523.70	\$556.49	\$575.76
D6548	Ret-porc/cer-resin bnd fxd pros	\$0.00	\$473.87	\$492.24	\$546.84	\$556.28	\$576.07	\$612.14	\$633.34
D6549	Ret-res - Res bnd fxd pros	\$0.00	\$310.69	\$322.74	\$358.54	\$364.73	\$377.70	\$401.35	\$415.25
D6600	Inlay-porcelain/ceramic, 2 surf	\$0.00	\$855.06	\$888.20	\$986.72	\$1,003.76	\$1,039.47	\$1,104.55	\$1,142.80
D6601	Inlay-porcelain/ceramic, 3+surf	\$0.00	\$896.83	\$931.59	\$1,034.93	\$1,052.80	\$1,090.26	\$1,158.51	\$1,198.64
D6602	Inlay-cast high noble met,2surf	\$0.00	\$913.80	\$949.22	\$1,054.52	\$1,072.72	\$1,110.89	\$1,180.43	\$1,221.32
D6603	Inlay-cast high nob met, 3+surf	\$0.00	\$1,005.18	\$1,044.14	\$1,159.97	\$1,179.99	\$1,221.97	\$1,298.47	\$1,343.45
D6604	Inlay-cast predomnt base, 2surf	\$0.00	\$895.52	\$930.24	\$1,033.42	\$1,051.27	\$1,088.67	\$1,156.82	\$1,196.89
D6605	Inlay-cast predomnt base,3+surf	\$0.00	\$949.05	\$985.83	\$1,095.19	\$1,114.10	\$1,153.73	\$1,225.96	\$1,268.43

Brumback Code	Brumback Procedure Description	Brumback Fee	50th Percentile	60th Percentile	75th Percentile	80th Percentile	85th Percentile	90th Percentile	95th Percentile
D6606	Inlay-cast noble metal, 2 surf	\$0.00	\$881.17	\$915.32	\$1,016.85	\$1,034.41	\$1,071.21	\$1,138.27	\$1,177.70
D6607	Inlay-cast noble metal, 3+ surf	\$0.00	\$977.77	\$1,015.67	\$1,128.33	\$1,147.81	\$1,188.65	\$1,263.06	\$1,306.81
D6608	Onlay-porcelain/ceramic, 2 surf	\$0.00	\$929.47	\$965.49	\$1,072.59	\$1,091.11	\$1,129.93	\$1,200.67	\$1,242.25
D6609	Onlay-porcelain/ceramic, 3+surf	\$0.00	\$969.93	\$1,007.53	\$1,119.29	\$1,138.62	\$1,179.13	\$1,252.94	\$1,296.34
D6610	Onlay-cast high noble met,2surf	\$0.00	\$985.60	\$1,023.80	\$1,137.37	\$1,157.01	\$1,198.17	\$1,273.18	\$1,317.28
D6611	Onlay-cast high nob met, 3+surf	\$0.00	\$1,078.29	\$1,120.08	\$1,244.33	\$1,265.81	\$1,310.85	\$1,392.91	\$1,441.16
D6612	Onlay-cast predomnt base, 2surf	\$0.00	\$980.38	\$1,018.38	\$1,131.34	\$1,150.88	\$1,191.82	\$1,266.43	\$1,310.30
D6613	Onlay-cast predomnt base,3+surf	\$0.00	\$1,024.76	\$1,064.48	\$1,182.56	\$1,202.98	\$1,245.78	\$1,323.77	\$1,369.62
D6614	Onlay-cast noble metal, 2 surf	\$0.00	\$959.49	\$996.68	\$1,107.24	\$1,126.36	\$1,166.43	\$1,239.45	\$1,282.38
D6615	Onlay-cast noble metal, 3+ surf	\$0.00	\$997.35	\$1,036.01	\$1,150.93	\$1,170.80	\$1,212.45	\$1,288.36	\$1,332.98
D6624	Inlay-titanium	\$0.00	\$913.80	\$949.22	\$1,054.52	\$1,072.72	\$1,110.89	\$1,180.43	\$1,221.32
D6634	Onlay-titanium	\$0.00	\$959.49	\$996.68	\$1,107.24	\$1,126.36	\$1,166.43	\$1,239.45	\$1,282.38
D6710	Retainer crn-indir res-bas comp	\$0.00	\$979.07	\$1,017.02	\$1,129.84	\$1,149.35	\$1,190.24	\$1,264.75	\$1,308.56
D6720	Retainer crn-res w/ hi nob met	\$0.00	\$1,142.25	\$1,186.53	\$1,318.14	\$1,340.90	\$1,388.61	\$1,475.54	\$1,526.65
D6721	Retainer crn-resin w/ base met	\$0.00	\$1,083.51	\$1,125.50	\$1,250.35	\$1,271.94	\$1,317.19	\$1,399.65	\$1,448.13
D6722	Retainer crn-resin w/ nob met	\$0.00	\$1,103.09	\$1,145.85	\$1,272.95	\$1,294.93	\$1,341.00	\$1,424.95	\$1,474.31
D6740	Crown-porcelain/ceramic	\$0.00	\$1,201.00	\$1,247.55	\$1,385.93	\$1,409.86	\$1,460.02	\$1,551.42	\$1,605.16
D6750	Retainer crn-porc fused-hi nob	\$0.00	\$1,169.67	\$1,215.00	\$1,349.78	\$1,373.08	\$1,421.93	\$1,510.95	\$1,563.29
D6751	Retainer crn-porc fuse-base met	\$0.00	\$1,091.34	\$1,133.64	\$1,259.39	\$1,281.14	\$1,326.72	\$1,409.77	\$1,458.60
D6752	Retainer crn-porc fused-nob met	\$0.00	\$1,117.45	\$1,160.76	\$1,289.52	\$1,311.79	\$1,358.45	\$1,443.50	\$1,493.50
D6780	Retainer crn-3/4 cast h nob met	\$0.00	\$1,103.09	\$1,145.85	\$1,272.95	\$1,294.93	\$1,341.00	\$1,424.95	\$1,474.31
D6781	Crown-3/4 cast most base metal	\$0.00	\$1,103.09	\$1,145.85	\$1,272.95	\$1,294.93	\$1,341.00	\$1,424.95	\$1,474.31
D6782	Crown-3/4 cast noble metal	\$0.00	\$1,024.76	\$1,064.48	\$1,182.56	\$1,202.98	\$1,245.78	\$1,323.77	\$1,369.62
D6783	Crown-3/4 porcelain/ceramic	\$0.00	\$1,135.72	\$1,179.75	\$1,310.61	\$1,333.24	\$1,380.67	\$1,467.11	\$1,517.92
D6790	Retainer crn-full cast hi nob	\$0.00	\$1,129.20	\$1,172.97	\$1,303.08	\$1,325.58	\$1,372.74	\$1,458.68	\$1,509.20
D6791	Retainer crn-full cast base	\$0.00	\$1,070.45	\$1,111.94	\$1,235.29	\$1,256.62	\$1,301.32	\$1,382.79	\$1,430.69
D6792	Retainer crn-full cast nob met	\$0.00	\$1,109.62	\$1,152.63	\$1,280.48	\$1,302.59	\$1,348.93	\$1,433.38	\$1,483.03
D6793	Provisional retainer crown	\$0.00	\$463.43	\$481.39	\$534.79	\$544.02	\$563.38	\$598.65	\$619.38
D6794	Retainer crown-titanium	\$0.00	\$1,109.62	\$1,152.63	\$1,280.48	\$1,302.59	\$1,348.93	\$1,433.38	\$1,483.03
D6795	Interim Retainer Crown	\$0.00							
D6920	Connector bar	\$0.00	\$224.71	\$259.02	\$281.47	\$285.20	\$303.75	\$338.46	\$392.31
D6930	Recement fixed partial denture	\$0.00	\$131.08	\$151.10	\$164.19	\$166.37	\$177.19	\$197.44	\$228.85
D6940	Stress breaker	\$0.00	\$297.11	\$342.48	\$372.16	\$377.10	\$401.63	\$447.53	\$518.72
D6950	Precision attachment	\$0.00	\$574.25	\$661.94	\$719.31	\$728.86	\$776.25	\$864.97	\$1,002.57
D6970	Cast post/core, + brdg retainer	\$0.00							
D6971	Cast post/part of brdg retainer	\$0.00							
D6972	Prefab post/core+ brdg retainer	\$0.00							
D6973	Core buildup for retain,inc pin	\$0.00							
D6975	Coping-metal	\$0.00							
D6976	Each add'l cast post-same tooth	\$0.00							
D6977	Each + prefab post-same tooth	\$0.00							
D6980	Fixed partial dent. repair, B/R	\$0.00							
D6999	Unspec fixed prosth proced, B/R	\$0.00							
D7251	Coronectomy-part tooth removal	\$0.00	\$579.70	\$616.47	\$685.44	\$727.25	\$744.61	\$807.90	\$888.14
D7272	Tooth transplantation	\$0.00	\$726.50	\$792.24	\$879.23	\$904.02	\$944.45	\$1,058.07	\$1,181.25

Brumback Code	Brumback Procedure Description	Brumback Fee	50th Percentile	60th Percentile	75th Percentile	80th Percentile	85th Percentile	90th Percentile	95th Percentile
D7282	Mobiliz erupt/malpos th-erupt	\$0.00	\$254.28	\$277.28	\$307.73	\$316.41	\$330.56	\$370.32	\$413.44
D7285	Biopsy of oral tissue-hard	\$0.00	\$1,017.10	\$1,109.13	\$1,230.92	\$1,265.63	\$1,322.23	\$1,481.29	\$1,653.75
D7286	Biopsy of oral tissue-soft	\$0.00	\$435.90	\$475.34	\$527.54	\$542.41	\$566.67	\$634.84	\$708.75
D7287	Exfoliative cyt sample collectn	\$0.00	\$174.36	\$190.14	\$211.02	\$216.96	\$226.67	\$253.94	\$283.50
D7288	Brush biopsy-transepith sample	\$0.00	\$174.36	\$190.14	\$211.02	\$216.96	\$226.67	\$253.94	\$283.50
D7290	Surgical reposition of teeth	\$0.00	\$435.90	\$475.34	\$527.54	\$542.41	\$566.67	\$634.84	\$708.75
D7291	T/SC Fiberotomy, B/R	\$0.00							
D7295	Bone Harvest for Grafting	\$0.00							
D7321	Alveoloplasty w/o ex 1-3 th/quad	\$0.00	\$325.89	\$375.15	\$498.40	\$534.60	\$578.99	\$633.67	\$755.76
D7340	Vestibuloplasty-ridge ext -2nd	\$0.00	\$1,629.46	\$1,875.73	\$2,492.02	\$2,673.00	\$2,894.93	\$3,168.36	\$3,778.79
D7350	Vestiplasty-ridge ext (inc)	\$0.00	\$4,740.24	\$5,456.68	\$7,249.52	\$7,776.00	\$8,421.60	\$9,217.04	\$10,992.84
D7410	Excision benign lesion<=1.25cm	\$0.00	\$711.04	\$818.50	\$1,087.43	\$1,166.40	\$1,263.24	\$1,382.56	\$1,648.93
D7411	Excision benign lesion>1.25 cm	\$0.00	\$1,125.81	\$1,295.96	\$1,721.76	\$1,846.80	\$2,000.13	\$2,189.05	\$2,610.80
D7412	Excision benign lesion,complic	\$0.00	\$1,244.31	\$1,432.38	\$1,903.00	\$2,041.20	\$2,210.67	\$2,419.47	\$2,885.62
D7413	Excision malig lesion<=1.25cm	\$0.00	\$829.54	\$954.92	\$1,268.67	\$1,360.80	\$1,473.78	\$1,612.98	\$1,923.75
D7414	Excision malig lesion>1.25cm	\$0.00	\$1,244.31	\$1,432.38	\$1,903.00	\$2,041.20	\$2,210.67	\$2,419.47	\$2,885.62
D7415	Excision malig lesion,complic	\$0.00	\$1,392.45	\$1,602.90	\$2,129.55	\$2,284.20	\$2,473.85	\$2,707.51	\$3,229.15
D7440	Ex malig tumor-diam <= 1.25 cm	\$0.00	\$1,125.81	\$1,295.96	\$1,721.76	\$1,846.80	\$2,000.13	\$2,189.05	\$2,610.80
D7441	Ex malig tumor-diam > 1.25 cm	\$0.00	\$1,659.08	\$1,909.84	\$2,537.33	\$2,721.60	\$2,947.56	\$3,225.96	\$3,847.49
D7450	Rem benign odont-diam<=1.25cm	\$0.00	\$711.04	\$818.50	\$1,087.43	\$1,166.40	\$1,263.24	\$1,382.56	\$1,648.93
D7451	Rem benign odont-diam>1.25 cm	\$0.00	\$971.75	\$1,118.62	\$1,486.15	\$1,594.08	\$1,726.43	\$1,889.49	\$2,253.53
D7460	Rem benign nonodont-di<=1.25cm	\$0.00	\$711.04	\$818.50	\$1,087.43	\$1,166.40	\$1,263.24	\$1,382.56	\$1,648.93
D7461	Rem benign nonodont-diam>1.25cm	\$0.00	\$971.75	\$1,118.62	\$1,486.15	\$1,594.08	\$1,726.43	\$1,889.49	\$2,253.53
D7465	Destruct lesion-phys/chem B/R	\$0.00	\$385.14	\$443.36	\$589.02	\$631.80	\$684.26	\$748.88	\$893.17
D7471	Removal of exostosis-per site	\$0.00	\$880.50	\$1,013.58	\$1,346.60	\$1,444.39	\$1,564.31	\$1,712.07	\$2,041.92
D7472	Removal of torus palatinus	\$0.00	\$1,046.41	\$1,204.56	\$1,600.33	\$1,716.55	\$1,859.07	\$2,034.66	\$2,426.67
D7473	Removal of torus mandibularis	\$0.00	\$987.15	\$1,136.35	\$1,509.71	\$1,619.35	\$1,753.80	\$1,919.45	\$2,289.26
D7485	Reduction of osseous tuberosity	\$0.00	\$880.50	\$1,013.58	\$1,346.60	\$1,444.39	\$1,564.31	\$1,712.07	\$2,041.92
D7490	Rad resectn-maxilla or mandible	\$0.00	\$7,110.36	\$8,185.02	\$10,874.28	\$11,664.00	\$12,632.40	\$13,825.56	\$16,489.26
D7511	Incis&drain absces-int soft comp	\$0.00	\$385.14	\$443.36	\$589.02	\$631.80	\$684.26	\$748.88	\$893.17
D7521	Incis&drain absces-ext soft comp	\$0.00	\$1,333.19	\$1,534.69	\$2,038.93	\$2,187.00	\$2,368.58	\$2,592.29	\$3,091.74
D7530	Remove foreign body from tissue	\$0.00	\$437.29	\$503.38	\$668.77	\$717.34	\$776.89	\$850.27	\$1,014.09
D7540	Remove foreign body from bone	\$0.00	\$484.69	\$557.95	\$741.26	\$795.10	\$861.11	\$942.44	\$1,124.02
D7550	Partial ostect/sequestrectomy	\$0.00	\$302.19	\$347.86	\$462.16	\$495.72	\$536.88	\$587.59	\$700.79
D7560	Maxill sinusotomy-rem foreign	\$0.00	\$2,399.75	\$2,762.44	\$3,670.07	\$3,936.60	\$4,263.44	\$4,666.13	\$5,565.13
D7610	Maxilla-open red (teeth immob)	\$0.00	\$3,881.07	\$4,467.66	\$5,935.54	\$6,366.60	\$6,895.19	\$7,546.45	\$9,000.39
D7620	Maxilla-closed red(teeth immob)	\$0.00	\$2,910.51	\$3,350.40	\$4,451.21	\$4,774.46	\$5,170.86	\$5,659.26	\$6,749.60
D7630	Mandible-open red (teeth immob)	\$0.00	\$5,045.99	\$5,808.64	\$7,717.11	\$8,277.55	\$8,964.79	\$9,811.54	\$11,701.88
D7640	Mandible-closed red (th immob)	\$0.00	\$3,202.03	\$3,685.99	\$4,897.05	\$5,252.69	\$5,688.79	\$6,226.11	\$7,425.66
D7650	Malar/zygomat arch-open reduc	\$0.00	\$2,425.82	\$2,792.46	\$3,709.94	\$3,979.37	\$4,309.75	\$4,716.82	\$5,625.59
D7660	Malar/zygo arch-closed reduc	\$0.00	\$1,430.37	\$1,646.55	\$2,187.54	\$2,346.41	\$2,541.22	\$2,781.24	\$3,317.09
D7670	Alveolus-closed reduction	\$0.00	\$1,116.33	\$1,285.05	\$1,707.26	\$1,831.25	\$1,983.29	\$2,170.61	\$2,588.81
D7671	Alveolus-open reduction	\$0.00	\$2,103.48	\$2,421.40	\$3,216.97	\$3,450.60	\$3,737.09	\$4,090.06	\$4,878.07
D7680	Facial bone-complicated reduct	\$0.00	\$7,277.45	\$8,377.37	\$11,129.83	\$11,938.10	\$12,929.26	\$14,150.46	\$16,876.76
D7710	Maxilla-open reduction	\$0.00	\$4,561.30	\$5,250.69	\$6,975.85	\$7,482.46	\$8,103.68	\$8,869.10	\$10,577.86

Brumback Code	Brumback Procedure Description	Brumback Fee	50th Percentile	60th Percentile	75th Percentile	80th Percentile	85th Percentile	90th Percentile	95th Percentile
D7720	Maxilla-closed reduction	\$0.00	\$3,202.03	\$3,685.99	\$4,897.05	\$5,252.69	\$5,688.79	\$6,226.11	\$7,425.66
D7730	Mandible-open reduction	\$0.00	\$6,598.41	\$7,595.70	\$10,091.33	\$10,824.19	\$11,722.87	\$12,830.12	\$15,302.03
D7740	Mandible-closed reduction	\$0.00	\$3,264.84	\$3,758.29	\$4,993.11	\$5,355.72	\$5,800.38	\$6,348.24	\$7,571.32
D7750	Malar/zygomatic arch-open red	\$0.00	\$4,152.45	\$4,780.05	\$6,350.58	\$6,811.78	\$7,377.32	\$8,074.13	\$9,629.73
D7760	Malar/zygomatic arch-close red	\$0.00	\$1,666.19	\$1,918.02	\$2,548.21	\$2,733.26	\$2,960.19	\$3,239.79	\$3,863.98
D7770	Alveolus-stabilize teeth, open	\$0.00	\$2,257.54	\$2,598.74	\$3,452.58	\$3,703.32	\$4,010.79	\$4,389.62	\$5,235.34
D7771	Alveolus-stabilize teeth,closed	\$0.00	\$1,742.04	\$2,005.33	\$2,664.20	\$2,857.68	\$3,094.94	\$3,387.26	\$4,039.87
D7780	Facial bones-complicated reduc	\$0.00	\$9,703.27	\$11,169.82	\$14,839.77	\$15,917.47	\$17,239.02	\$18,867.28	\$22,502.34
D7810	Open reduction of dislocation	\$0.00	\$4,268.59	\$4,913.74	\$6,528.19	\$7,002.29	\$7,583.65	\$8,299.94	\$9,899.05
D7820	Closed reduction of dislocate	\$0.00	\$699.19	\$804.86	\$1,069.30	\$1,146.96	\$1,242.19	\$1,359.51	\$1,621.44
D7830	Manipulation under anesthesia	\$0.00	\$400.55	\$461.09	\$612.58	\$657.07	\$711.63	\$778.84	\$928.89
D7840	Condylectomy	\$0.00	\$5,818.64	\$6,698.07	\$8,898.79	\$9,545.04	\$10,337.51	\$11,313.92	\$13,493.71
D7850	Surgical dissect:w/ w/o implant	\$0.00	\$5,024.65	\$5,784.08	\$7,684.49	\$8,242.56	\$8,926.90	\$9,770.06	\$11,652.41
D7852	Disc repair	\$0.00	\$5,753.47	\$6,623.05	\$8,799.10	\$9,438.12	\$10,221.72	\$11,187.18	\$13,342.56
D7854	Synovectomy	\$0.00	\$5,937.15	\$6,834.49	\$9,080.02	\$9,739.44	\$10,548.05	\$11,544.34	\$13,768.53
D7856	Myotomy	\$0.00	\$4,212.89	\$4,849.62	\$6,443.01	\$6,910.92	\$7,484.70	\$8,191.64	\$9,769.89
D7858	Joint reconstruction	\$0.00	\$12,008.21	\$13,823.13	\$18,364.85	\$19,698.55	\$21,334.02	\$23,349.07	\$27,847.61
D7860	Arthrotomy	\$0.00	\$5,118.27	\$5,891.85	\$7,827.67	\$8,396.14	\$9,093.22	\$9,952.10	\$11,869.52
D7865	Arthroplasty	\$0.00	\$8,248.02	\$9,494.62	\$12,614.16	\$13,530.24	\$14,653.58	\$16,037.65	\$19,127.54
D7870	Arthrocentesis	\$0.00	\$272.56	\$313.76	\$416.85	\$447.12	\$484.24	\$529.98	\$632.09
D7871	Non-arthroscopic lysis & lavage	\$0.00	\$545.13	\$627.52	\$833.69	\$894.24	\$968.48	\$1,059.96	\$1,264.18
D7872	Arthroscopy-diag, w/ w/o biopsy	\$0.00	\$2,909.32	\$3,349.04	\$4,449.39	\$4,772.52	\$5,168.76	\$5,656.96	\$6,746.86
D7873	Arthroscopy-lavage/lysis adhes	\$0.00	\$3,503.04	\$4,032.49	\$5,357.40	\$5,746.46	\$6,223.56	\$6,811.39	\$8,123.71
D7874	Arthroscopy-disc rpstn/stabil	\$0.00	\$5,024.65	\$5,784.08	\$7,684.49	\$8,242.56	\$8,926.90	\$9,770.06	\$11,652.41
D7875	Arthroscopy: Synovectomy	\$0.00	\$5,504.60	\$6,336.57	\$8,418.51	\$9,029.88	\$9,779.58	\$10,703.29	\$12,765.44
D7876	Arthroscopy: Dissectomy	\$0.00	\$5,934.78	\$6,831.76	\$9,076.40	\$9,735.55	\$10,543.84	\$11,539.73	\$13,763.04
D7877	Arthroscopy: Debridement	\$0.00	\$5,237.97	\$6,029.63	\$8,010.72	\$8,592.48	\$9,305.87	\$10,184.83	\$12,147.09
D7880	Occlusal orthotic device	\$0.00	\$654.15	\$753.02	\$1,000.43	\$1,073.09	\$1,162.18	\$1,271.95	\$1,517.01
D7881	Occlusal ortho device adjustmnt	\$0.00	\$71.10	\$81.85	\$108.74	\$116.64	\$126.32	\$138.26	\$164.89
D7899	Unspecified TMD therapy, B/R	\$0.00							
D7910	Suture of small wounds to 5cm	\$0.00	\$388.70	\$447.45	\$594.46	\$637.63	\$690.57	\$755.80	\$901.41
D7911	Complicated suture-up to 5 cm	\$0.00	\$970.56	\$1,117.26	\$1,484.34	\$1,592.14	\$1,724.32	\$1,887.19	\$2,250.78
D7912	Complicated suture-over 5 cm	\$0.00	\$1,746.78	\$2,010.79	\$2,671.45	\$2,865.46	\$3,103.36	\$3,396.48	\$4,050.86
D7920	Skin grafts, by report	\$0.00	\$2,861.92	\$3,294.47	\$4,376.90	\$4,694.76	\$5,084.54	\$5,564.79	\$6,636.93
D7940	Osteoplasty-orthognathic defor	\$0.00							
D7941	Osteotomy-mandibular rami	\$0.00	\$7,288.12	\$8,389.65	\$11,146.14	\$11,955.60	\$12,948.21	\$14,171.20	\$16,901.49
D7943	Osteotomy-mand rami w/ graft	\$0.00	\$6,695.59	\$7,707.56	\$10,239.95	\$10,983.60	\$11,895.51	\$13,019.07	\$15,527.39
D7944	Osteotomy-segment/subap-s/quad	\$0.00	\$5,966.78	\$6,868.60	\$9,125.33	\$9,788.04	\$10,600.69	\$11,601.95	\$13,837.24
D7945	Osteotomy-body of mandible	\$0.00	\$7,939.90	\$9,139.94	\$12,142.95	\$13,024.80	\$14,106.18	\$15,438.54	\$18,413.01
D7946	LeFort I (maxilla-total)	\$0.00							
D7947	LeFort I (maxilla-segmented)	\$0.00							
D7948	LeFort II/III-no bone graft	\$0.00							
D7949	LeFort II/III-with bone graft	\$0.00							
D7950	Osseous/cartilage graft-mandB/R	\$0.00							
D7953	Bone repl grft ridge prsv/site	\$0.00	\$402.92	\$463.82	\$616.21	\$660.96	\$715.84	\$783.45	\$934.39

Brumback Code	Brumback Procedure Description	Brumback Fee	50th Percentile	60th Percentile	75th Percentile	80th Percentile	85th Percentile	90th Percentile	95th Percentile
D7955	Rep maxillofacial sft/hrd tis	\$0.00							
D7960	Frenulectomy-separate procedur	\$0.00	\$325.89	\$375.15	\$498.40	\$534.60	\$578.99	\$633.67	\$755.76
D7963	Frenuloplasty	\$0.00	\$533.28	\$613.88	\$815.57	\$874.80	\$947.43	\$1,036.92	\$1,236.69
D7972	Surg reduc, fibrous tuberosity	\$0.00	\$663.63	\$763.94	\$1,014.93	\$1,088.64	\$1,179.02	\$1,290.39	\$1,539.00
D7980	Sialolithotomy	\$0.00	\$746.59	\$859.43	\$1,141.80	\$1,224.72	\$1,326.40	\$1,451.68	\$1,731.37
D7981	Excision of salivary gland, B/R	\$0.00	\$11,850.60	\$13,641.70	\$18,123.80	\$19,440.00	\$21,054.00	\$23,042.60	\$27,482.10
D7982	Sialodochoplasty	\$0.00	\$1,765.74	\$2,032.61	\$2,700.45	\$2,896.56	\$3,137.05	\$3,433.35	\$4,094.83
D7983	Closure of salivary fistula	\$0.00	\$1,694.64	\$1,950.76	\$2,591.70	\$2,779.92	\$3,010.72	\$3,295.09	\$3,929.94
D7990	Emergency tracheotomy	\$0.00							
D7991	Coronoidectomy	\$0.00							
D7995	Synthetic graft-mand/facial,B/R	\$0.00							
D7996	Implant-mandib/augmentation,B/R	\$0.00							
D7997	Appliance removal-incl archbar	\$0.00							
D7999	Unspecified oral surg proc, B/R	\$0.00							
D8010	Limited ortho trt, primary dent	\$0.00							
D8020	Limited ortho trt, transitional	\$0.00							
D8030	Limited ortho treat, adolescent	\$0.00							
D8040	Limited ortho treat, adult dent	\$0.00							
D8050	Intercep orth trt, primary dent	\$0.00							
D8060	Intercep orth trt, transitional	\$0.00							
D8680	Orthodontic retention	\$0.00							
D8681	Remov ortho retainer adjustment	\$0.00							
D8690	Ortho treatment (bill/contract)	\$0.00							
D8691	Repair of orthodontic appliance	\$0.00							
D8694	Repair/reattach fixed retainer	\$0.00							
D8999	Unspec ortho procedure, B/R	\$0.00							
D9210	Local anesthesia not op/surg	\$0.00	\$43.25	\$50.56	\$58.99	\$64.10	\$65.12	\$77.52	\$91.29
D9211	Regional block anesthesia	\$0.00	\$47.73	\$55.79	\$65.09	\$70.74	\$71.85	\$85.54	\$100.73
D9212	Trigeminal division blk anesth	\$0.00	\$74.57	\$87.17	\$101.71	\$110.53	\$112.27	\$133.66	\$157.39
D9215	Local anesthesia	\$0.00	\$35.79	\$41.84	\$48.82	\$53.05	\$53.89	\$64.16	\$75.55
D9219	Eval for deep sedat/gen anesth	\$0.00	\$85.01	\$99.37	\$115.95	\$126.00	\$127.99	\$152.37	\$179.43
D9223	Deep sedat/gen anesth-ea15m	\$0.00	\$193.89	\$226.64	\$264.45	\$287.37	\$291.91	\$347.52	\$409.22
D9243	IV conscious sed/analg-ea15m	\$0.00	\$164.06	\$191.77	\$223.76	\$243.16	\$247.00	\$294.05	\$346.26
D9311	Consult w/ medical professional	\$0.00	\$110.80	\$111.37	\$127.14	\$151.09	\$166.37	\$210.54	\$243.00
D9410	House/extended care facility	\$0.00	\$126.73	\$127.38	\$145.41	\$172.81	\$190.29	\$240.80	\$277.93
D9430	Office visit for observation	\$0.00	\$6,925.20	\$6,960.90	\$7,946.10	\$9,443.40	\$10,398.10	\$13,158.70	\$15,187.50
D9440	Office visit-after regular hrs	\$0.00	\$69.25	\$69.61	\$79.46	\$94.43	\$103.98	\$131.59	\$151.88
D9450	Case present,detailed/extens tx	\$0.00	\$34.63	\$34.80	\$39.73	\$47.22	\$51.99	\$65.79	\$75.94
D9610	Therapeutic drug injection, B/R	\$0.00							
D9630	Drugs/medicaments for home use	\$0.00							
D9910	Application of desensitize med	\$0.00	\$47.31	\$60.50	\$76.28	\$85.10	\$91.54	\$116.82	\$141.75
D9911	Apply desensitiz' resin, per th	\$0.00	\$66.23	\$84.70	\$106.80	\$119.14	\$128.15	\$163.55	\$198.45
D9931	Clean/insp of rmvbl appliance	\$0.00							
D9932	Clean/insp of maxl comp denture	\$0.00	\$116.25	\$148.65	\$187.44	\$209.10	\$224.92	\$287.05	\$348.30
D9933	Clean/insp of mand comp denture	\$0.00	\$116.25	\$148.65	\$187.44	\$209.10	\$224.92	\$287.05	\$348.30

Brumback Code	Brumback Procedure Description	Brumback Fee	50th Percentile	60th Percentile	75th Percentile	80th Percentile	85th Percentile	90th Percentile	95th Percentile
D9934	Clean/insp of maxl part denture	\$0.00	\$116.25	\$148.65	\$187.44	\$209.10	\$224.92	\$287.05	\$348.30
D9935	Clean/insp of mand part denture	\$0.00	\$116.25	\$148.65	\$187.44	\$209.10	\$224.92	\$287.05	\$348.30
D9940	Occlusal guards, by report	\$0.00	\$391.99	\$501.27	\$632.06	\$705.11	\$758.47	\$967.97	\$1,174.50
D9941	Fabricate athletic mouthguards	\$0.00	\$135.17	\$172.85	\$217.95	\$243.14	\$261.54	\$333.78	\$405.00
D9942	Repair/Reline of occlusal guard	\$0.00	\$162.20	\$207.42	\$261.54	\$291.77	\$313.85	\$400.54	\$486.00
D9943	Occlusal guard adjustment	\$0.00	\$81.10	\$103.71	\$130.77	\$145.88	\$156.92	\$200.27	\$243.00
D9950	Occlusal analysis-mounted case	\$0.00	\$256.82	\$328.42	\$414.11	\$461.97	\$496.93	\$634.19	\$769.50
D9952	Occlusal adjustment-complete	\$0.00	\$540.68	\$691.40	\$871.80	\$972.56	\$1,046.16	\$1,335.13	\$1,620.00
D9970	Enamel microabrasion	\$0.00	\$60.83	\$77.78	\$98.08	\$109.41	\$117.69	\$150.20	\$182.25
D9972	External bleaching-per arch	\$0.00	\$270.34	\$345.70	\$435.90	\$486.28	\$523.08	\$667.56	\$810.00
D9973	External bleaching-per tooth	\$0.00	\$44.61	\$57.04	\$71.92	\$80.24	\$86.31	\$110.15	\$133.65
D9974	Internal bleaching-per tooth	\$0.00	\$236.55	\$302.49	\$381.41	\$425.50	\$457.70	\$584.12	\$708.75
D9985	Sales Tax	\$0.00							
D9986	Missed appointment	\$0.00							
D9987	Cancelled Appointment	\$0.00							
D9991	DCM: appointment non-compliance	\$0.00	\$47.31	\$60.50	\$76.28	\$85.10	\$91.54	\$116.82	\$141.75
D9992	DCM: care coordination	\$0.00	\$47.31	\$60.50	\$76.28	\$85.10	\$91.54	\$116.82	\$141.75
D9993	DCM: motivational interviewing	\$0.00	\$47.31	\$60.50	\$76.28	\$85.10	\$91.54	\$116.82	\$141.75
D9994	DCM: oral health education	\$0.00	\$64.88	\$82.97	\$104.62	\$116.71	\$125.54	\$160.22	\$194.40
D9999	Unspecified adjunct. proced,B/R	\$0.00							

Brumback Code	This is the CPT Code you provided
Code	This is the matching CPT Code from the software
Modifier	This is the Modifier for the Matching CPT Code (Software), if available/applicable
Sub	This is the Sub-Modifier for the Matching CPT Code (Software), if available/applicable
Brumback Insurance Description	This is the Procedure Code Description you provided
Fee Software Description	This is the matching Procedure Code Description from the Software
Brumback Fee	This is the Fee you provided for the particular procedure
50th Percentile	This is the fee that falls within the 50th percentile of what those providing this service and reported data are charging for that same procedure
60th Percentile	This is the fee that falls within the 60th percentile of what those providing this service and reported data are charging for that same procedure
75th Percentile	This is the fee that falls within the 75th percentile of what those providing this service and reported data are charging for that same procedure
80th Percentile	This is the fee that falls within the 80th percentile of what those providing this service and reported data are charging for that same procedure
85th Percentile	This is the fee that falls within the 85th percentile of what those providing this service and reported data are charging for that same procedure
90th Percentile	This is the fee that falls within the 90th percentile of what those providing this service and reported data are charging for that same procedure
95th Percentile	This is the fee that falls within the 95th percentile of what those providing this service and reported data are charging for that same procedure
Medicare Fee	This is the Standard Medicare Fee being charged in your area for this procedure

DISTRICT CLINIC HOLDINGS, INC.
BOARD OF DIRECTORS
December 11, 2019

1. Description: Finance Policies Adoption

2. Summary:

This item presents the Grant Policy and the Budget Policy.

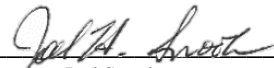
3. Substantive Analysis:

The Grant Policy was approved by the HCD Board on May 14, 2014 and the Budget Policy was approved by the HCD Board on April 30, 2018. These corporate policies are attached for reference.

4. Fiscal Analysis & Economic Impact Statement:

	Amount	Budget
Capital Requirements		Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>
Annual Net Revenue		Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>
Annual Expenditures		Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>

Reviewed for financial accuracy and compliance with purchasing procedure:



 Joel Snook
 VP & Chief Financial Officer

5. Reviewed/Approved by Committee:

N/A

 Committee Name

 Date Approved

DISTRICT CLINIC HOLDINGS, INC.
BOARD OF DIRECTORS
December 11, 2019

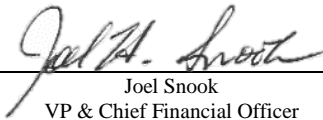
6. Recommendation:

Staff recommends the Board approve the adoption of the Health Care District's Grant and Budget policies.

Approved for Legal sufficiency:



Valerie Shahriari
VP & General Counsel



Joel Snook
VP & Chief Financial Officer



Dr. Belma Andric
Chief Medical Officer, VP & Executive Director
of Clinic Services

POLICY

Policy Title: **Budget Policy**

Effective Date: 02/27/18

Department: **Finance**

Policy #: 201610-BP

INTRODUCTION

All departments should participate in the responsibility of meeting policy goals and ensuring the long-term financial health of the Health Care District. The budget process is intended to weigh all competing requests for District resources, within existing fiscal restraints.

SCOPE

This policy applies to all District programs and affiliates.

POLICY

Budget development will use strategic multi-year fiscal planning, conservative revenue forecasts, and modified zero-base expenditure analysis that requires every program to be justified annually in terms of meeting intended objectives ("effectiveness criteria") and in terms of value received for dollars allocated ("efficiency criteria"). Requests for new, expanded, or modified services and eligibility guidelines shall be approved by the Board annually along with the budget process. The process will include a diligent review of programs by staff, management, and Boards. The public will be provided an opportunity for input during regular meetings and TRIM meetings.

Alternative means of service delivery will be evaluated to ensure that quality services are provided to our citizens at the most competitive and economical cost. Departments, in cooperation with their officer and the Chief Executive Officer, will identify all activities that could be provided by another source and review options/alternatives to current service delivery. The review of service delivery alternatives and the need for the service will be performed annually or as opportunities arise.

Fees and charges for enterprise funds (Healey, Healthy Palm Beaches, Primary Care Clinics and Lakeside Medical Center) will be examined annually to ensure that they maximize net reimbursement and fall within market rates.

Revenue and expenditure forecasts will be prepared on a three year time horizon to examine the District's ability to absorb operating costs due to changes in the economy, service demands, and capital improvements. These forecasts will be reviewed periodically throughout the year as industry conditions change and will be adjusted when appropriate.

POLICY

Policy Title: **Budget Policy**

Effective Date: 02/27/18

Department: **Finance**

Policy #: 201610-BP

Consistent with the Florida Special District Handbook, the following requirements will also be met regarding adoption of the initial budget:

- The governing body of the special taxing district shall adopt a budget by resolution each year.
- The total amount available from taxation and other sources, including balances brought forward from prior fiscal years, must equal the total appropriations for expenditures and reserves.
- The adopted budget must show for each fund, as required by law and sound financial practices, budgeted revenues and expenditures by organizational unit which are at least the level of detail required for the Annual Financial Report.
- The adopted budget must regulate expenditures of the special district, and an officer of a special district may not expend or contract for expenditures in any fiscal year except pursuant to the adopted budget.

The Board may amend its budget at any time within a fiscal year or within 60 days following the end of its fiscal year as follows:

- May increase or decrease appropriations for expenditures within a fund or program by motion recorded in the minutes, if the total appropriations of the fund do not increase.
- The Board may establish procedures by which the designated budget officer may authorize certain amendments within a fund or between programs for amounts less than \$250,000, as long as total appropriations of the fund do not increase.
- If a budget amendment is required for a purpose not specifically permitted by statute, the amendment must be adopted by a resolution of the Board, and posted on the official website of the District within 5 days after adoption.

REFERENCE: FS Chapter 189.016


POLICY

Policy Title: **Budget Policy**

Effective Date: 02/27/18

Department: **Finance**

Policy #: 201610-BP

APPROVED BY	DATE
 Darcy J. Davis, Chief Executive Officer	4-30-18
Health Care District Finance and Audit Committee	02/27/18
Health Care District Board	02/27/18

POLICY REVISION HISTORY

Original Policy Date

03/11/2009 –
Financial Policies

Revisions

11/14/2012 – Financial Policies	11/01/2013 – Financial Policies
10/01/2014	10/01/2015
02/27/2018	

POLICY

Policy Title: **Grant Policy**

Effective Date: 10/01/14

Department: **Finance**

Policy #: 201410-GP

INTRODUCTION

There are a number of ways in which the District and its affiliates receive funding. Grant funding will be considered to leverage District funds. The purpose of this policy is to establish a consistent understanding that will ensure that all grants are properly reviewed, documented, approved and maintained and that such arrangements are initiated/facilitated in accordance with District by-laws and applicable federal and state laws and regulations.

SCOPE

This policy applies to all District programs and affiliates.

DEFINITIONS

Grant/Contract – Award is from a federal, state, or municipal government or agency. Sponsor specifies desire to gain benefit as a result of activities to be conducted under the award. Award document stipulates method of payment as costs reimbursable, typically with a cost sharing commitment.

Private Foundations & Individual Donations – Donor is an individual corporation, foundation, or other private sector entity voluntarily transferring funds or other assets with the intent to treat the transfer as a charitable contribution. An unrestricted donation occurs when the donor makes the award without expecting benefit and does not participate in how the award is used. Any restrictions placed on the award by the donor should be reasonable and serve to direct the award to a broadly defined activity or specific program area of interest to the donor.

POLICY

Program Administrators or Management desiring to seek funding through a grant should coordinate with the executive team and Finance to coordinate efforts and verify support for grant requirements. Inconsistent and/or fluctuating grants should only be used to supplement ongoing programs.

In the event of reduced grant funding, District resources will be substituted only after all program priorities and alternatives are considered during the budget process. Positions that are added to support grant funded initiatives will be closed when the grant funding has ended.

POLICY

Policy Title: **Grant Policy**

Effective Date: 10/01/14

Department: **Finance**

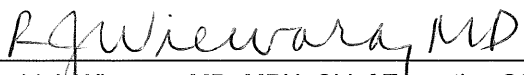
Policy #: 201410-GP

Program administrators who desire to pursue, or those who receive a grant award should be responsible for the following:

- Supplying initial grant funding information, including establishment of scope
- Submission of proposal to sponsor
- Receipt of award notice; negotiation of terms and preparation for acceptance by District
- Dissemination of award documents within the organization to affected departments
- Coordination with Finance to establish proper accounting controls and reporting
- Liaison between District and Sponsor
- Monitor timely submission of interim and final reports

The Finance team will be responsible for the following:

- Works with program administrator on proposal budgets
- Set up of grant accounts and reports
- Manages and processes all draws against grants or invoices for award
- Ensures capital expenditures required under each grant are processed in accordance with District capital acquisition policies
- Provides financial reports and data to support external reporting requirements

APPROVED BY	DATE
 _____ Ronald J. Wiewora, MD, MPH, Chief Executive Officer	_____ 9/4/14
_____ Health Care District Board	_____ 09/04/14

POLICY

Policy Title: **Grant Policy**

Effective Date: 10/01/14

Department: **Finance**

Policy #: 201410-GP

POLICY REVISION HISTORY

Original Policy Date

03/11/2009 – Financial Policies

Revisions

11/14/2012 – Financial Policies	11/01/2013 – Financial Policies

DISTRICT CLINIC HOLDINGS, INC.
BOARD OF DIRECTORS
December 11, 2019

1. Description: CMO, VP & Executive Director of Clinical Services Annual Evaluation by Board

2. Summary:

This agenda item presents the Board's annual evaluation of Dr. Belma Andric, CMO, VP & Executive Director of Clinical Services tally of results from November 2019.

3. Substantive Analysis:

The Bylaws and HRSA Compliance Manual indicate that the annual evaluation of the Executive Director of the Clinics are reviewed and approved by the Board. A tally of results from last month's completed Annual Evaluation Form is attached for your consideration.

4. Fiscal Analysis & Economic Impact Statement:

	Amount	Budget
Capital Requirements		Yes <input type="checkbox"/> No <input type="checkbox"/>
Annual Net Revenue		Yes <input type="checkbox"/> No <input type="checkbox"/>
Annual Expenditures		Yes <input type="checkbox"/> No <input type="checkbox"/>

Reviewed for financial accuracy and compliance with purchasing procedure:

N/A

 Joel H. Snook, CPA
 VP & Chief Financial Officer

5. Reviewed/Approved by Committee:

N/A

 Committee Name

 Date Approved

DISTRICT CLINIC HOLDINGS, INC.
BOARD OF DIRECTORS
December 11, 2019

6. Recommendation:

Staff recommends the Board receive and file Dr. Andric's Annual Evaluation by the Board.

Approved for Legal sufficiency:



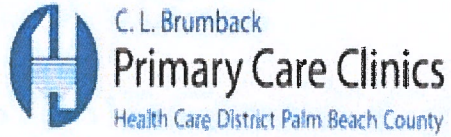
Valerie Shahriari
VP & General Counsel



Thomas Cleare
VP of Strategy



Darcy J. Davis
Chief Executive Officer



**Leadership Performance 2019
Executive Director**

	BM1	BM2	BM3	BM4	BM5	BM6	BM7	BM8	BM9	BM10
Leadership	3	3	3	3	3	3	3	No evaluation turned in		
Cooperation	3	3	3	3	3	3	3			
Communication	3	3	3	3	3	3	3			
Decision Making	3	3	3	3	3	3	3			
Job Knowledge	3	3	3	3	3	3	3			
Compliance	3	3	3	3	3	3	3			
FQHC Knowledge	3	3	3	3	3	3	3			
FQHC Funding	3	3	3	3	3	3	3			
Staff Supervision	3	2	3	3	3	3	3			
Board Support and Relations	3	2	3	3	3	3	3			
Total	30	28	30	30	30	30	30			

Total

29.71

COMMENTS

Dr. Andric has been very welcoming and informative throughout my transition as a new board member.

Dr. Andric displays professional character at all times. Very helpful to Board Members and always available.

DISTRICT CLINIC HOLDINGS, INC.
BOARD OF DIRECTORS
December 11, 2019

1. Description: Summary of Board Member Self-Evaluations

2. Summary:

This agenda item presents the Board’s annual self-evaluation tally of results from November 2019.

3. Substantive Analysis:

The C. L. Brumback Primary Care Clinics Board completes an annual self-evaluation yearly. Attached you will find the tally of results for 2019.

4. Fiscal Analysis & Economic Impact Statement:

	Amount	Budget
Capital Requirements		Yes <input type="checkbox"/> No <input type="checkbox"/>
Annual Net Revenue		Yes <input type="checkbox"/> No <input type="checkbox"/>
Annual Expenditures		Yes <input type="checkbox"/> No <input type="checkbox"/>

Reviewed for financial accuracy and compliance with purchasing procedure:

N/A

 Joel H. Snook, CPA
 VP & Chief Financial Officer

5. Reviewed/Approved by Committee:

N/A

 Committee Name

 Date Approved

6. Recommendation:

Staff recommends the Board receive and file the Summary of Board Member Self-Evaluations.

DISTRICT CLINIC HOLDINGS, INC.
BOARD OF DIRECTORS
December 11, 2019

Approved for Legal sufficiency:



Valerie Shahriari
VP & General Counsel



Thomas Cleare
VP of Strategy



Belma Andric, MD
CMP, VP and Executive Director
of Clinical Services

C. L. BRUMBACK PRIMARY CARE CLINICS

BOARD OF DIRECTORS

SELF-EVALUATION TALLY SHEET 2019

Criteria or Measures of:	YES	NO	Need to Work on
Our Board Prepares to do its job by:			
<u>SELECTION AND COMPOSITION</u>	8		
Ensuring that the Board is composed of persons vitally interested in the work of the organization.	8		
Ensuring that the Board is widely representative of the community.	8		
Ensuring that there is a satisfactory combination of experience and new Board members to guarantee both continuity and new thinking.	8		
<u>ORIENTATION AND TRAINING</u>	8		
Ensuring that the organization has a Board Member manual, which it supplies to all Board members. The manual is revised periodically.	8		
Ensuring that Board members participate in community, state regional and national training opportunities.	7		1
Conducting a thorough orientation of all new Board members.	8		
Integrating new members into the team as quickly as possible.	8		
Attending Board development activities for all Board members.	8		
Providing Board development activities for all Board members.	8		
Performing an annual evaluation of Board and organization operations.	8		
Providing all Board members with copies of the mission statement, by-laws, and all other important documents of the organization.	8		
Touring all facilities on a regular basis.	7		1 – need to tour facilities
Ensuring that Board members understand their legal responsibilities	8		
Ensuring that Board activities are confined to policy issues rather than management issues.	8		
<u>OUR BOARD ENSURES GOOD MEETINGS BY</u>	8		
Ensuring that the minutes of the Board and committee meetings are written and circulated to members.	8		
Limiting most meeting to two (2) hours or less.	8		
Providing a comfortable meeting room conducive to business.	8		
Convening and adjourning on time.	8		
Sticking to the prepared agenda and are businesslike.	8		
Working for consensus rather than fighting for a majority.	8		
Following a businesslike system of parliamentary rules.	8		
Including the Executive Director and/or other appropriate staff.	8		
Confining all discussion to policy issues and avoiding management issues.	8		
Allowing/encouraging all Board members to participate in discussion.	8		

Criteria or Measures of:	YES	NO	Need to Work on
<u>INDIVIDUAL BOARD MEMBERS</u>	8		
Attend at least 80% of all Board meetings and committee meetings to which they are assigned.	8		
Come to meetings prepared to discuss agenda issues.	8		
Come to meetings on time.	8		
See themselves as a part of a team effort.	8		
Act as lobbyists for the organization, as required and/or needed.	8		
Know their responsibility as trustees of the organization.	8		
Attempt to exercise authority only during official meetings of a Board.	8		
Represent the Board interest of the organization and all constituents, not special interests.	8		
Understand that the most efficient way to govern is to delegate management to the Executive Director.	8		
<u>OUR BOARD PLANS FOR THE FUTURE OF THE ORGANIZATION BY:</u>	8		
Annually reviewing and approving the mission statement.			
Criteria or Measures of:	YES	NO	Need to Work on
Operating from opportunity to opportunity rather than crisis to crisis.	7		

REINFORCEMENTS AND SOLUTIONS

In which of the major categories above does our Board show real strength?

- Support the staff.
- In the diversity of its members. Also, a board made-up of new and experienced members.
- Great communication and teamwork.
- Interest, teamwork, commitment.

In which of the major categories above does our Board need improvement?

- In Board training activities.

DISTRICT CLINIC HOLDINGS, INC.
BOARD OF DIRECTORS
December 11, 2019

1. Description: 2019 Palm Beach County Community Health Assessment and Lakeside Medical Center Community Health Needs Assessment

2. Summary:

This agenda item presents the Board with the 2019 Palm Beach County Community Health Assessment, draft Lakeside Medical Center Community Health Needs Assessment.

3. Substantive Analysis:

The HRSA Compliance Manual requires that the health center completes or updates a needs assessment of the current or proposed population at least once every three years, for the purposes of informing and improving the delivery of health center services. The needs assessment utilizes the most recently available data for the service area and, if applicable, special populations and addresses the following:

- Factors associated with access to care and health care utilization (for example, geography, transportation, occupation, transience, unemployment, income level, educational attainment);
- The most significant causes of morbidity and mortality (for example, diabetes, cardiovascular disease, cancer, low birth weight, behavioral health) as well as any associated health disparities; and
- Any other unique health care needs or characteristics that impact health status or access to, or utilization of, primary care (for example, social factors, the physical environment, cultural/ethnic factors, language needs, housing status).

The 2019 Palm Beach County Community Health Assessment outcome identified three key strategies that will be the focus of C. L. Brumback Primary Care Clinics Implementation Strategy:

1. Increase patient awareness on maintaining a healthy and active lifestyle
2. Continue integrating behavioral health into all service-lines and ensure consistent reporting of social determinants of health (PRAPARE)
3. Continue increasing access to care

The Lakeside Medical Center Community Health Needs Assessment outcome identified three key strategies that will be the focus of Belle Glade Clinic's Implementation Strategy. Those strategies are:

1. Increase patient awareness on maintaining a healthy lifestyle to include obesity and cardiovascular disease
2. Increase patient knowledge of diabetes and diabetes resources
3. Enhance marketing in the community

**DISTRICT CLINIC HOLDINGS, INC.
BOARD OF DIRECTORS
December 11, 2019**

4. Fiscal Analysis & Economic Impact Statement:

	Amount	Budget
Capital Requirements	N/A	Yes <input type="checkbox"/> No <input type="checkbox"/>
Annual Net Revenue	N/A	Yes <input type="checkbox"/> No <input type="checkbox"/>
Annual Expenditures	N/A	Yes <input type="checkbox"/> No <input type="checkbox"/>

Reviewed for financial accuracy and compliance with purchasing procedure:

N/A

Joel H. Snook, CPA
VP & Chief Financial Officer

5. Reviewed/Approved by Committee:

N/A

Committee Name

Date Approved

6. Recommendation:

Staff recommends the Board receive and file the 2019 Palm Beach County Community Health Assessment and Lakeside Medical Center Community Health Needs Assessment.

Approved for Legal sufficiency:



Valerie Shahriari
VP & General Counsel



Thomas Cleare
VP of Strategy



Belma Andric
CMO, VP and Executive Director
of Clinical Services

DISTRICT CLINIC HOLDINGS, INC.
BOARD OF DIRECTORS
December 11, 2019

1. Description: Executive Director Informational Update

2. Summary:

Updates on key changes within C. L. Brumback Primary Care Clinics:

- Mock FTCA Audit
- HRSA Operational Site Visit

3. Substantive Analysis:

Mock FTCA Audit

Mock FTCA Audit is scheduled for the week of January 27-31.

HRSA Operational Site Visit

Operational Site Visit is scheduled for the week of March 23-27. As a reminder, the Mock HRSA Audit is scheduled for December 11-13.

4. Fiscal Analysis & Economic Impact Statement:

	Amount	Budget
Capital Requirements	N/A	Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>
Annual Net Revenue	N/A	Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>
Annual Expenditures	N/A	Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>

Reviewed for financial accuracy and compliance with purchasing procedure:

N/A

 Joel Snook
 Chief Financial Officer

5. Reviewed/Approved by Committee:

N/A

 Committee Name

 Date Approved

DISTRICT CLINIC HOLDINGS, INC.
BOARD OF DIRECTORS
December 11, 2019

6. Recommendation:

Staff recommends Board receive and file the Executive Director Informational Update.

Approved for Legal sufficiency:



Valerie Shahriari
General Counsel



Dr. Belma Andric
Chief Medical Officer, VP & Executive Director
of Clinic Services

DISTRICT CLINIC HOLDINGS, INC.
BOARD OF DIRECTORS
December 11, 2019

1. Description: Operations Reports – November 2019

2. Summary:

This agenda item provides the following operations reports for November 2019:

- Productivity Summary Report
- Productivity Detail Report by Clinic

3. Substantive Analysis:

Overall visits year to date is 138,842. Number of encounters in November across all categories is significantly lower than the previous month due to three less workdays in the month. Belle Glade Medical and Dental Clinics moved into the new primary care suite at Lakeside Medical Center in early November, which slightly affected encounters at these locations.

Enhancements to the Operations report includes prior year comparison reporting beginning May 15, 2018, when clinics transitioned to Athena EHR. NOTE the specific clinic 2018 data is only for 7.5 months. During those 7.5 months in 2019 clinics are trending higher.

4. Fiscal Analysis & Economic Impact Statement:

	Amount	Budget
Capital Requirements	N/A	Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>
Annual Net Revenue	N/A	Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>
Annual Expenditures	N/A	Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>

Reviewed for financial accuracy and compliance with purchasing procedure:

N/A

Darcy J. Davis
Chief Executive Officer

5. Reviewed/Approved by Committee:

N/A

Committee Name

Date Approved

DISTRICT CLINIC HOLDINGS, INC.
BOARD OF DIRECTORS
December 11, 2019

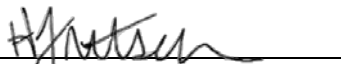
6. Recommendation:

Staff recommends the Board Approve the Operations Reports for November 2019.

Approved for Legal sufficiency:



Valerie Shahriari
General Counsel



Dr. Hyla Fritsch
Director of Clinic Operations and Pharmacy
Services



Dr. Belma Andric
Chief Medical Officer, VP & Executive Director
of Clinic Services



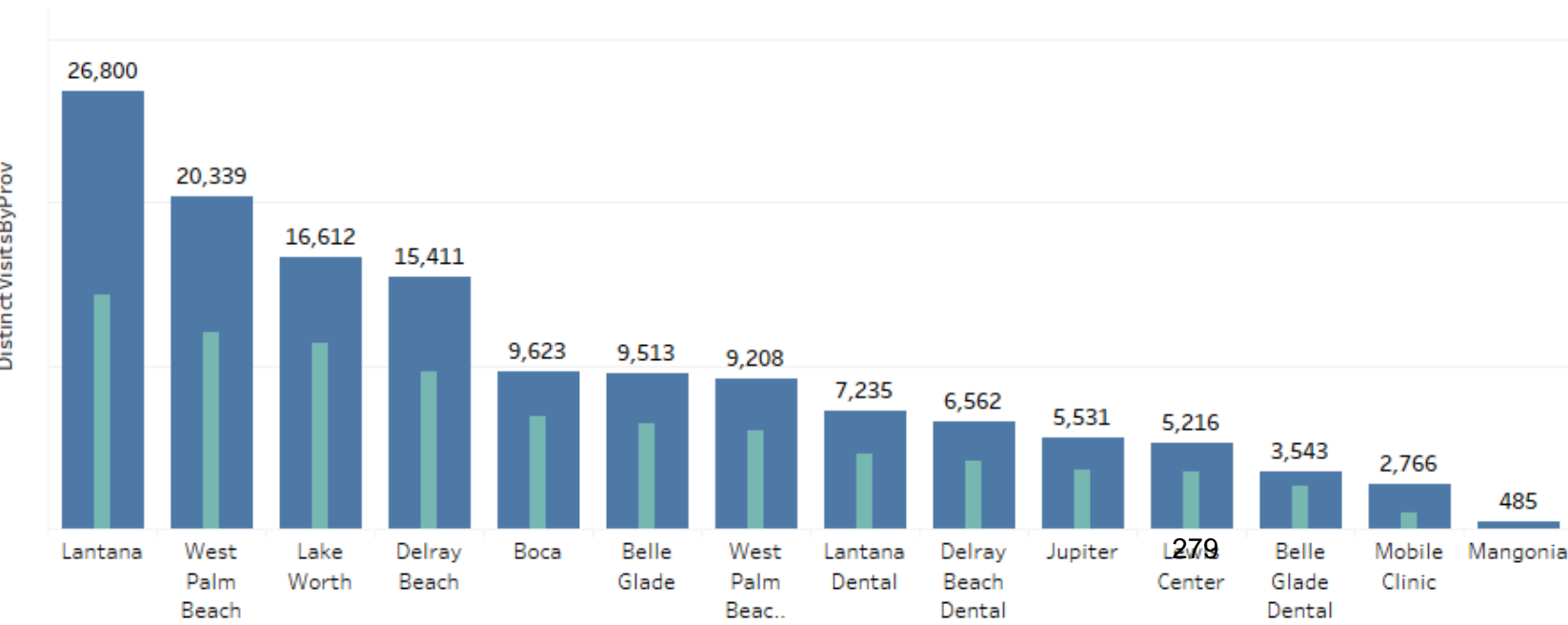
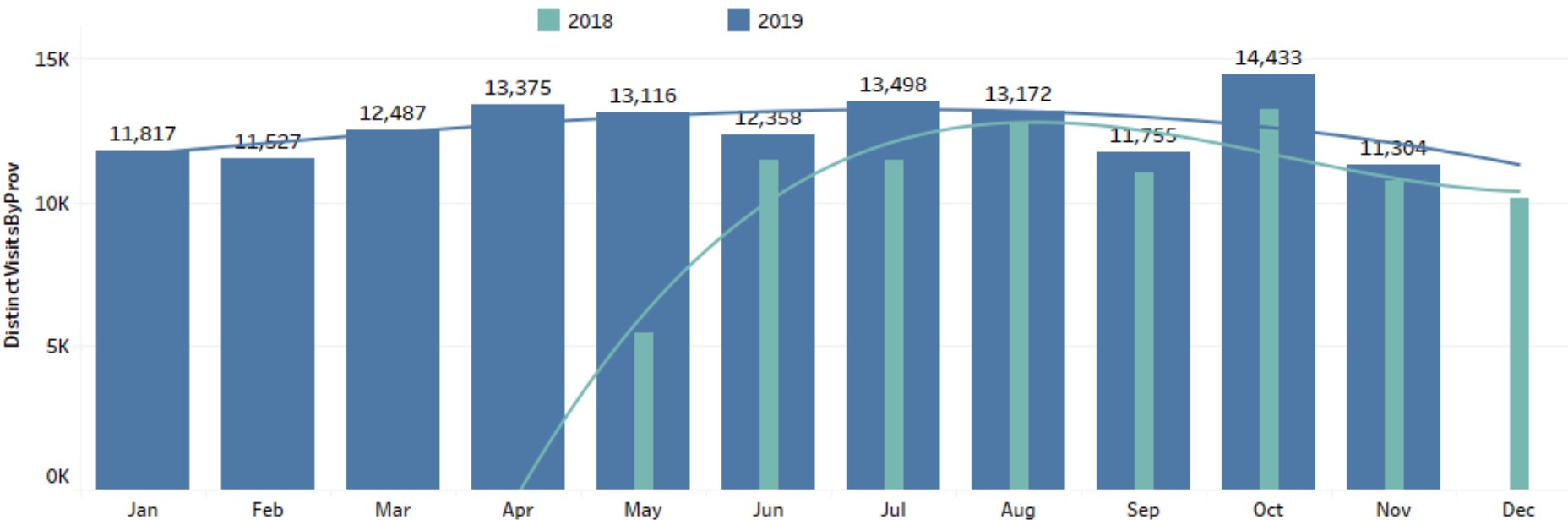
2019 Visits

138,842

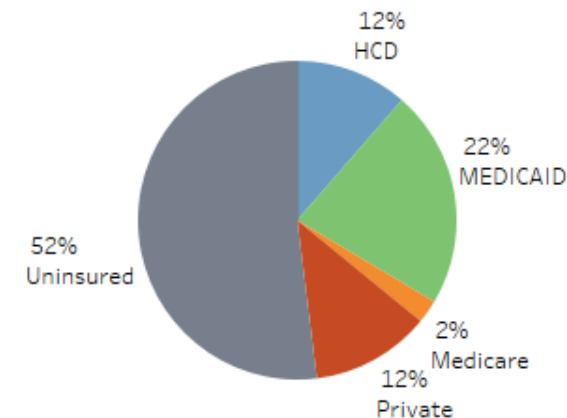
Service Date
 5/15/2018 to 11/27/2019

Category

- Adult Care
- Dental
- Dental Hygiene
- Mental Health
- Pediatric Care
- Substance Abuse
- Women's Care



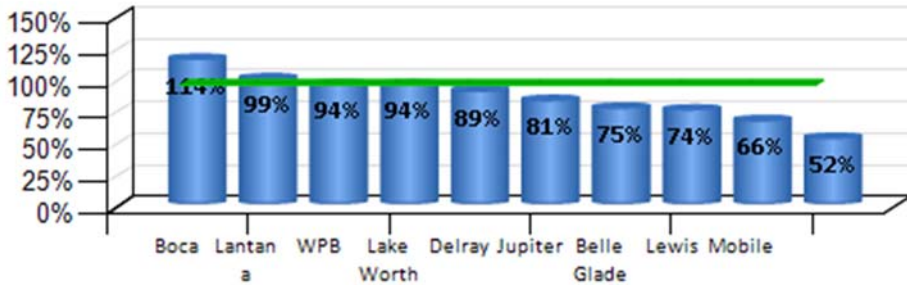
Payer Mix



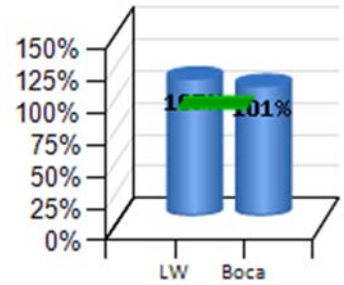
ALL CLINICS PRODUCTIVITY NOVEMBER 2019

	Target	Total seen	% Monthly Target
ADULT CARE	6478	5736	89%
DENTAL	2017	1752	87%
DENTAL HYGIENE	536	392	73%
MENTAL HEALTH	1790	1296	72%
PEDIATRIC CARE	1255	1296	103%
SUBSTANCE ABUSE	535	497	93%
WOMEN'S HEALTH CARE	343	360	105%

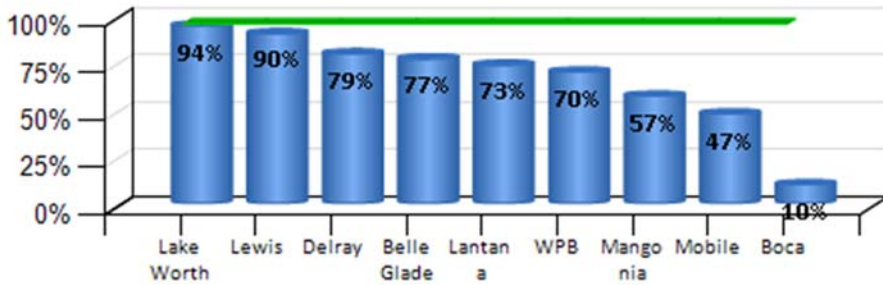
Adult care



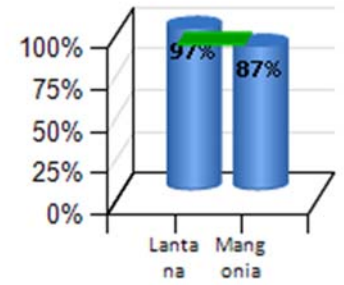
Women's Health



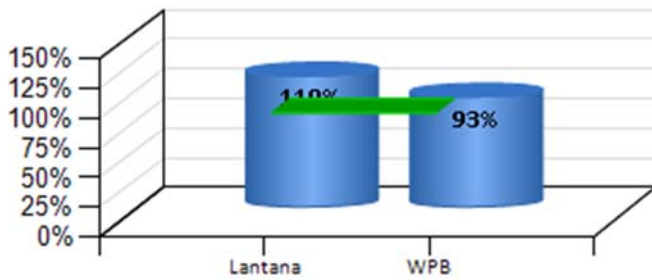
Mental Health



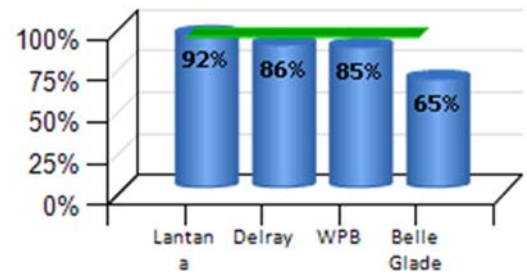
Substance Abuse



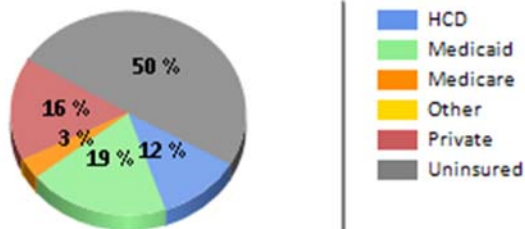
Pediatric Care



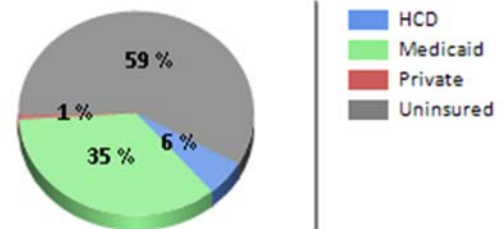
Dental & Dental Hygiene



Medical Payer Mix YTD



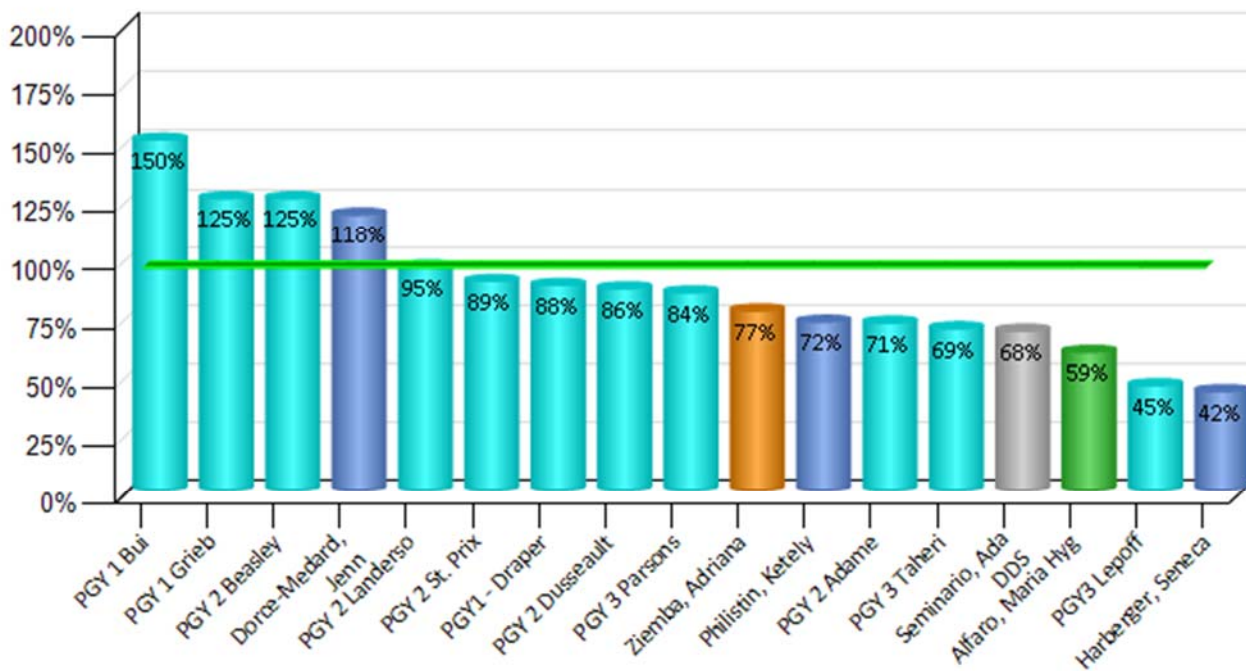
Dental Payer Mix YTD



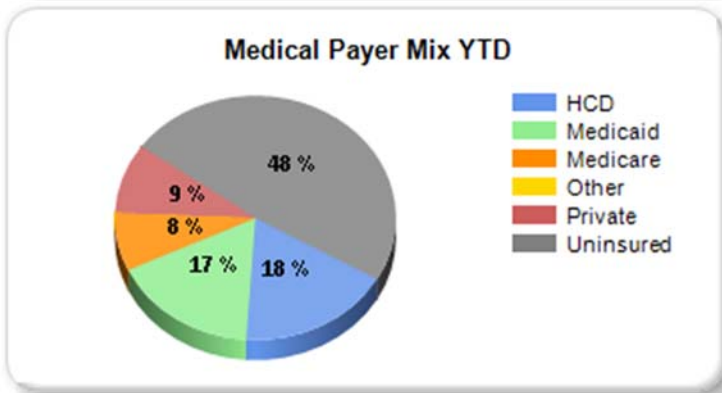
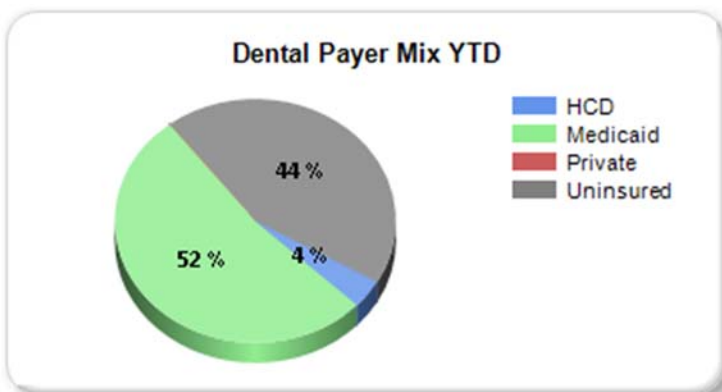
BELLE GLADE TOTALS FOR NOVEMBER 2019

	Daily Target	Days Worked	Target for the month	Total for month seen	% Monthly Target Achieved	Daily Average
RESIDENT						
PGY 1 Bui	8	1.0	8	12	150%	12.0
PGY 1 Grieb	8	0.5	4	5	125%	10.0
PGY 2 Beasley	12	1.0	12	15	125%	15.0
PGY 2 Landerso	12	5.5	66	63	95%	11.5
PGY 2 St. Prix	12	8.5	102	91	89%	10.7
PGY1 - Draper	8	2.0	16	14	88%	7.0
PGY 2 Dusseault	12	6.0	72	62	86%	10.3
PGY 3 Parsons	16	2.0	32	27	84%	13.5
PGY 2 Adame	12	3.5	42	30	71%	8.6
PGY 3 Taheri	16	10.5	168	116	69%	11.0
PGY3 Lepoff	16	2.5	40	18	45%	7.2
BELLE GLADE RESIDENT TOTALS		43.0	562	453	81%	
ADULT CARE						
Dorce-Medard, Jennifer DO Resident Preceptor	3	13.0	39	46	118%	3.5
Philistin, Ketely ARNP	16	17.5	280	201	72%	11.5
Harberger, Seneca MD Resident Preceptor	7	15.5	109	46	42%	3.0
BELLE GLADE ADULT CARE TOTALS		46.0	428	293	69%	
MENTAL HEALTH						
Ziemba, Adriana	8	15.5	124	95	77%	6.1
BELLE GLADE MENTAL HEALTH TOTALS		15.5	124	95	77%	
DENTAL						
Seminario, Ada DDS	16	17.0	272	185	68%	10.9
BELLE GLADE DENTAL TOTALS		17.0	272	185	68%	
DENTAL HYGIENE						
Alfaro, Maria Hyg	8	14.0	112	66	59%	4.7
BELLE GLADE DENTAL HYGIENE TOTALS		14.0	112	66	59%	
BELLE GLADE TOTALS		135.5	1498	1092	73%	

BELLE GLADE PROVIDER PRODUCTIVITY NOVEMBER 2019



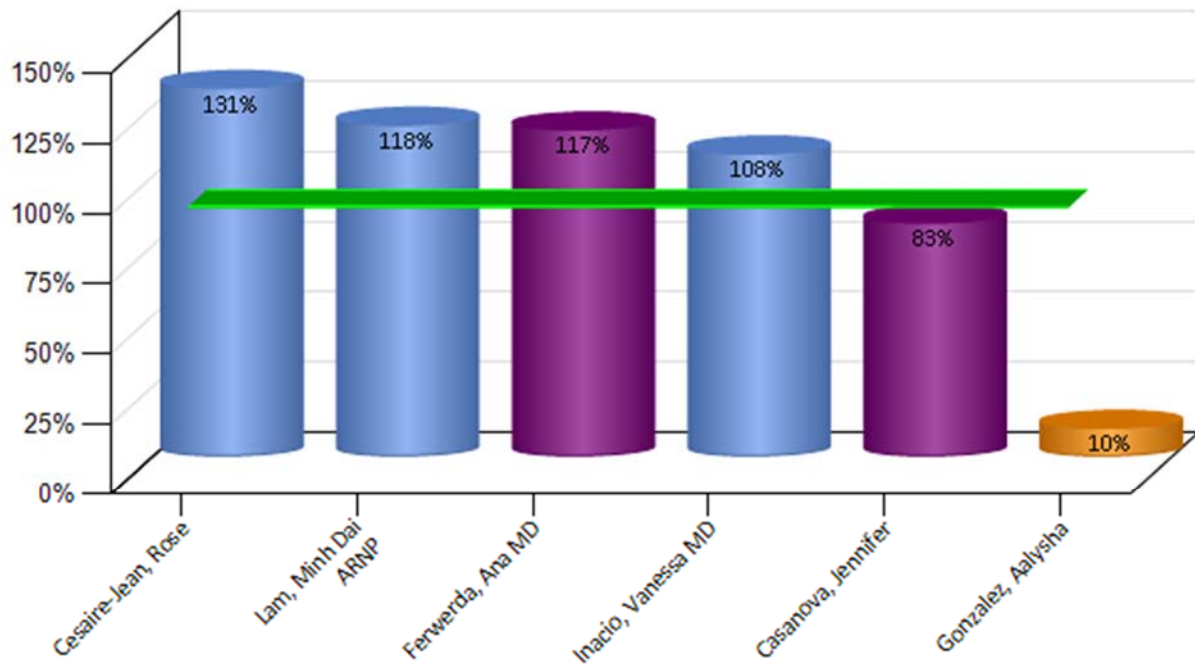
■ Mental Health
 ■ Adult Care
 ■ Dental
 ■ Dental Hyg.



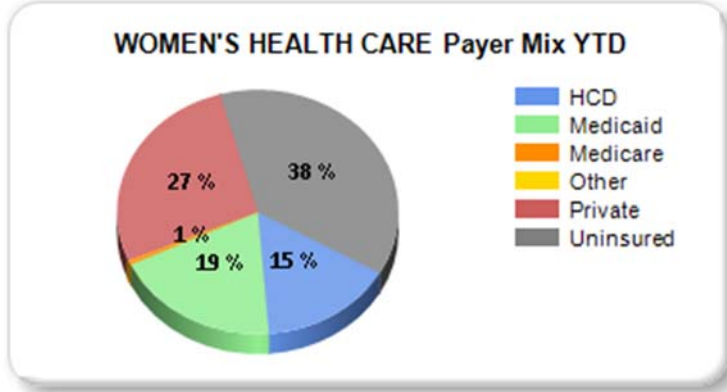
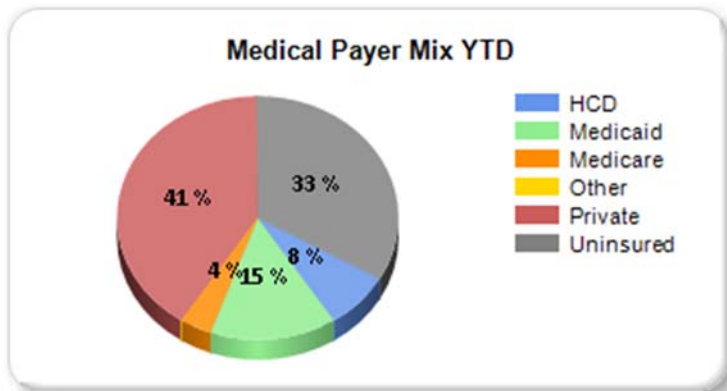
BOCA TOTALS FOR NOVEMBER 2019

	Daily Target	Days Worked	Target for the month	Total for month seen	% Monthly Target Achieved	Daily Average
ADULT CARE						
Cesaire-Jean, Rose Carline ARNP	16	1.0	16	21	131%	21.0
Lam, Minh Dai ARNP	16	16.0	256	303	118%	18.9
Inacio, Vanessa MD	18	13.0	234	253	108%	19.5
BOCA ADULT CARE TOTALS		30.0	506	577	114%	
WOMEN'S HEALTH CARE						
Ferwerda, Ana MD	18	3.0	54	63	117%	21.0
Casanova, Jennifer, ARNP	16	3.0	48	40	83%	13.3
BOCA WOMEN'S HEALTH CARE TOTALS		6.0	102	103	101%	
MENTAL HEALTH						
Gonzalez, Aalysha LCSW	10	1.0	10	1	10%	1.0
BOCA MENTAL HEALTH TOTALS		1.0	10	1	10%	
BOCA TOTALS		37.0	618	681	110%	

BOCA PROVIDER PRODUCTIVITY NOVEMBER 2019



■ Pediatrics
 ■ Adult Care
 ■ Women's Health



DELRAY BEACH TOTALS FOR NOVEMBER 2019

	Daily Target	Days Worked	Target for the month	Total for month seen	% Monthly Target Achieved	Daily Average
ADULT CARE						
Lam, Minh Dai ARNP	16	1.0	16	20	125%	20.0
St. Vil-Joseph, Carline ARNP	16	17.0	272	258	95%	15.2
Cesaire-Jean, Rose Carline ARNP	16	15.5	248	225	91%	14.5
Montenegro, Claudia DO	18	14.0	252	217	86%	15.5
Duthil, Marie MD	18	16.0	288	237	82%	14.8
DELRAY BEACH ADULT CARE TOTALS		63.5	1076	957	89%	

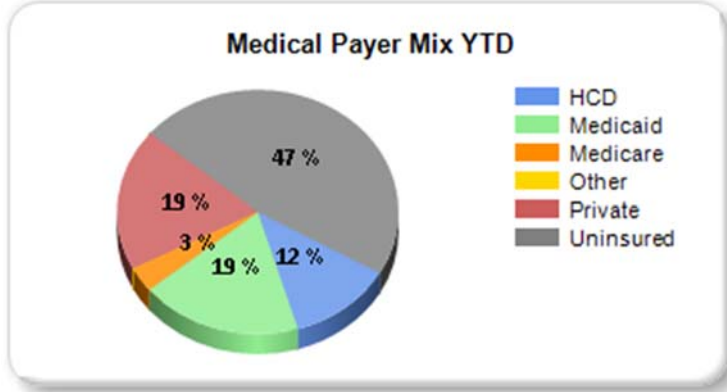
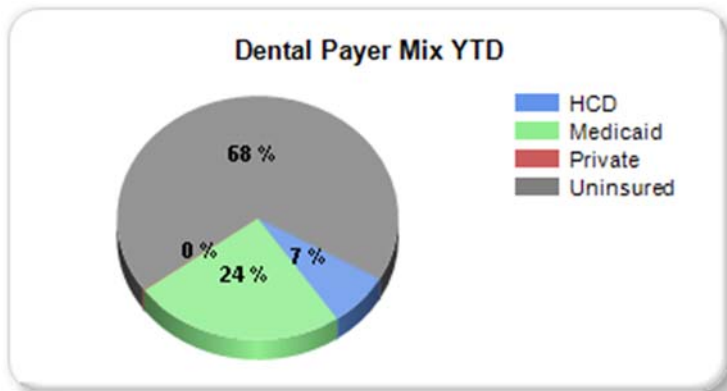
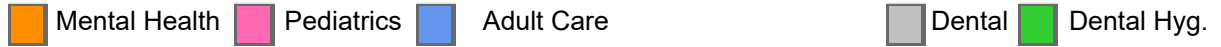
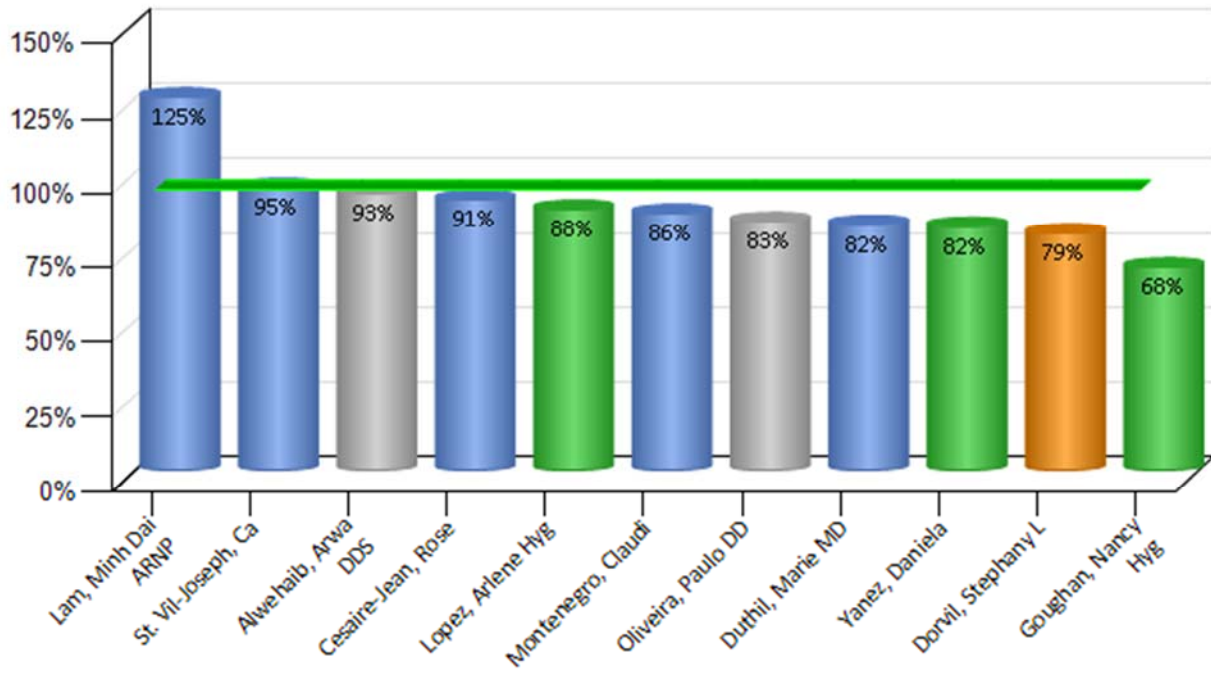
MENTAL HEALTH						
Dorvil, Stephany LCSW	10	15.0	150	119	79%	7.9
DELRAY BEACH MENTAL HEALTH TOTALS		15.0	150	119	79%	

DENTAL						
Alwehaib, Arwa DDS	16	17.0	272	253	93%	14.9
Oliveira, Paulo DDS	16	15.0	240	200	83%	13.3
DELRAY BEACH DENTAL TOTALS		32.0	512	453	88%	

DENTAL HYGIENE						
Lopez, Arlene Hyg	8	1.0	8	7	88%	7.0
Yanez, Daniela	8	7.5	60	49	82%	6.5
Goughan, Nancy Hyg	8	7.0	56	38	68%	5.4
DELRAY BEACH DENTAL HYGIENE TOTALS		15.5	124	94	76%	

DELRAY BEACH TOTALS		126.0	1862	1623	87%	
----------------------------	--	--------------	-------------	-------------	------------	--

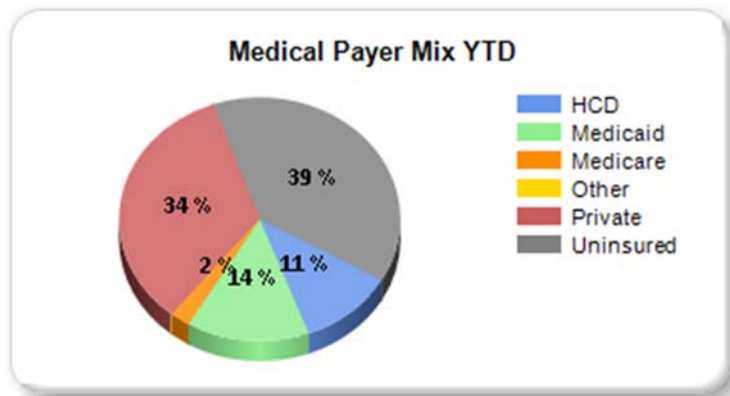
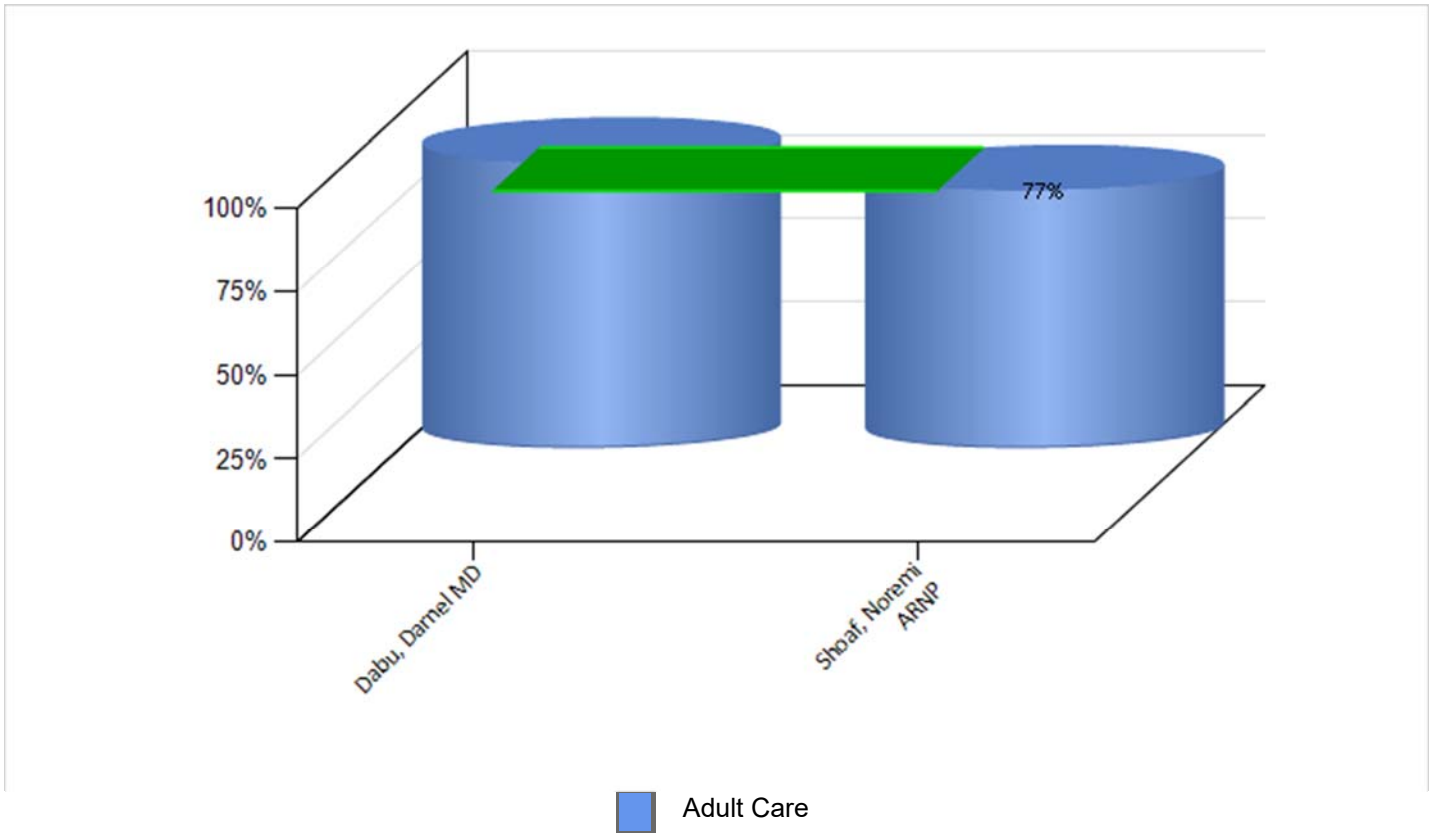
DELRAY BEACH PROVIDER PRODUCTIVITY NOVEMBER 2019



JUPITER TOTALS FOR NOVEMBER 2019

	Daily Target	Days Worked	Target for the month	Total for month seen	% Monthly Target Achieved	Daily Average
ADULT CARE						
Dabu, Darnel MD	18	17.0	306	261	85%	15.4
Shoaf, Noremi ARNP	16	17.0	272	210	77%	12.4
JUPITER ADULT CARE TOTALS		34.0	578	471	81%	
JUPITER TOTALS		34.0	578	471	81%	

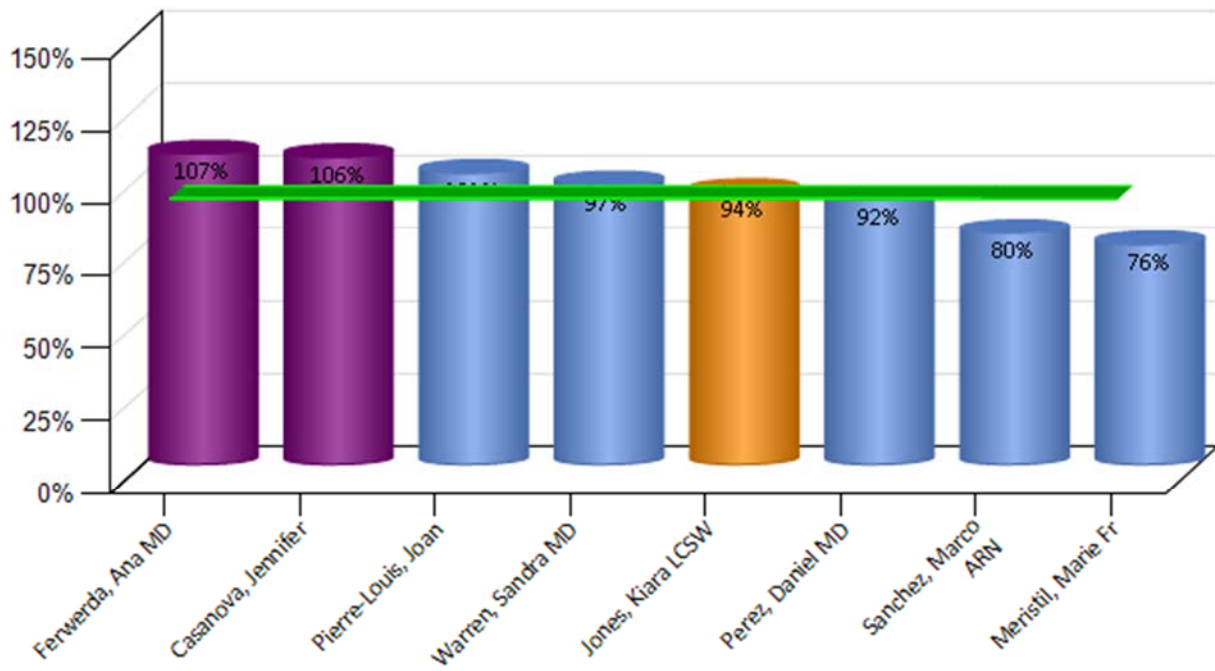
JUPITER PROVIDER PRODUCTIVITY NOVEMBER 2019



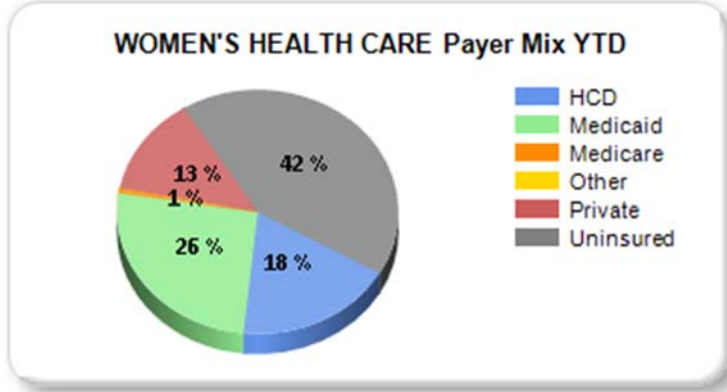
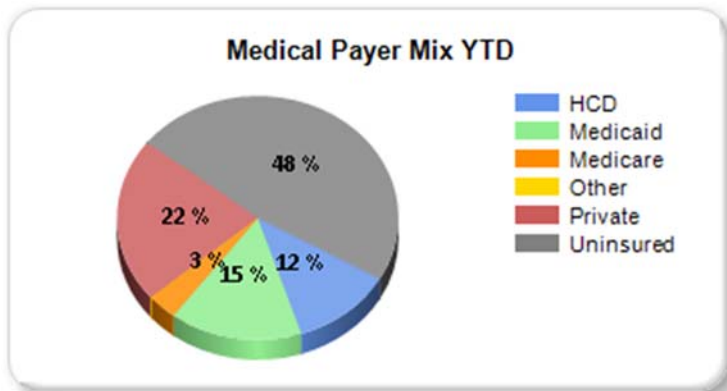
LAKE WORTH TOTALS FOR NOVEMBER 2019

	Daily Target	Days Worked	Target for the month	Total for month seen	% Monthly Target Achieved	Daily Average
ADULT CARE						
Pierre-Louis, Joanne ARNP	16	15.5	248	250	101%	16.1
Warren, Sandra MD	18	17.5	315	305	97%	17.4
Perez, Daniel MD	18	15.5	279	256	92%	16.5
Sanchez, Marco ARNP	10	1.0	10	8	80%	8.0
Meristil, Marie Frantzcia ARNP	16	7.0	112	85	76%	12.1
LAKE WORTH ADULT CARE TOTALS		56.5	964	904	94%	
WOMEN'S HEALTH CARE						
Ferwerda, Ana MD	18	4.5	81	87	107%	19.3
Casanova, Jennifer, ARNP	16	10.0	160	170	106%	17.0
LAKE WORTH WOMEN'S HEALTH CARE TOTALS		14.5	241	257	107%	
MENTAL HEALTH						
Jones, Kiara LCSW	10	15.5	155	146	94%	9.4
LAKE WORTH MENTAL HEALTH TOTALS		15.5	155	146	94%	
LAKE WORTH TOTALS		86.5	1360	1307	96%	

LAKE WORTH PROVIDER PRODUCTIVITY NOVEMBER 2019



■ Mental Health
 ■ Pediatrics
 ■ Adult Care
 ■ Women's Health



LANTANA TOTALS FOR NOVEMBER 2019

	Daily Target	Days Worked	Target for the month	Total for month seen	% Monthly Target Achieved	Daily Average
ADULT CARE						
Fernique Jean-Jacques, ARNP	10	16.5	165	181	110%	11.0
Navarro, Elsy ARNP	16	11.0	176	172	98%	15.6
Meristil, Marie Frantzcia ARNP	16	5.0	80	77	96%	15.4
Alfonso-Puentes, Ramiro MD	18	13.5	243	228	94%	16.9
Perez, Daniel MD	18	0.5	9	6	67%	12.0
LANTANA ADULT CARE TOTALS		46.5	673	664	99%	

PEDIATRIC CARE						
Lazaro, Nancy MD	18	14.0	252	296	117%	21.1
Dessalines, Duclos MD	18	12.0	216	241	112%	20.1
Normil-Smith, Sherloune MD	18	15.5	279	288	103%	18.6
LANTANA PEDIATRIC CARE TOTALS		41.5	747	825	110%	

MENTAL HEALTH						
Bell, Emily	16	8.5	136	136	100%	16.0
Rivera-Pullen, Valerie LCSW	10	14.5	145	141	97%	9.7
Alvarez, Franco MD	16	6.0	96	56	58%	9.3
Calderon, Nylsa LMHC	10	17.5	175	88	50%	5.0
Rowling, Courtney MD	16	3.0	48	19	40%	6.3
LANTANA MENTAL HEALTH TOTALS		49.5	600	440	73%	

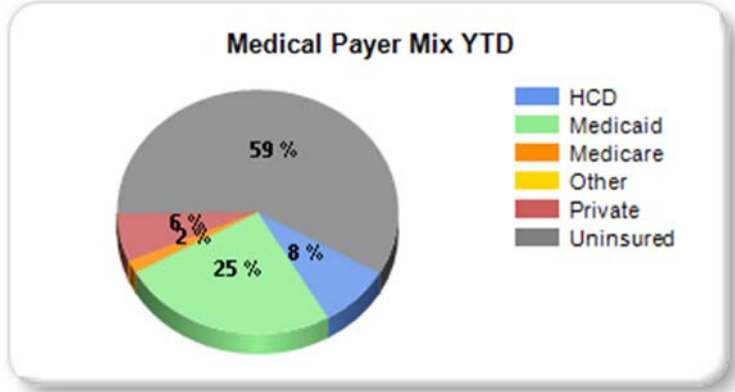
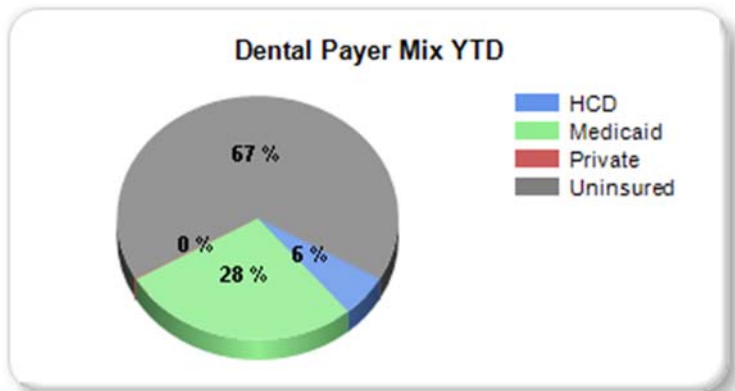
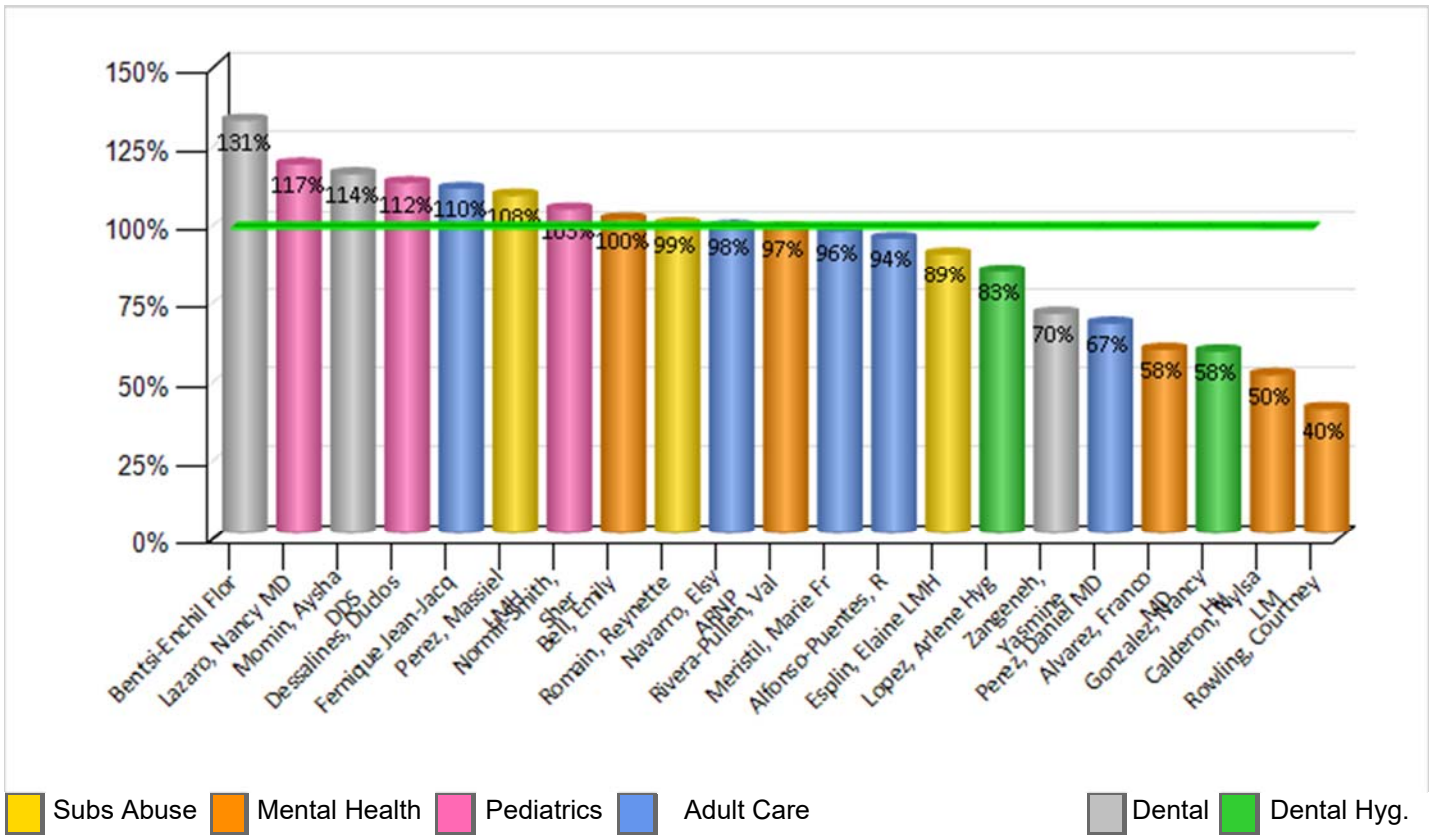
SUBSTANCE ABUSE						
Perez, Massiel LMHC	10	10.5	105	113	108%	10.8
Romain, Reynette	10	7.0	70	69	99%	9.9
Esplin, Elaine LMHC	10	13.5	135	120	89%	8.9
LANTANA SUBSTANCE ABUSE TOTALS		31.0	310	302	97%	

DENTAL						
Bentsi-Enchil Flora DDS	16	2.0	32	42	131%	21.0
Momin, Aysha DDS	16	16.0	256	293	114%	18.3
Zangeneh, Yasmine DDS	13	13.0	169	118	70%	9.1
LANTANA DENTAL TOTALS		31.0	457	453	99%	

DENTAL HYGIENE						
Lopez, Arlene Hyg	8	12.0	96	80	83%	6.7
Gonzalez, Nancy Hyg	8	8.0	64	37	58%	4.6
LANTANA DENTAL HYGIENE TOTALS		20.0	160	117	73%	

LANTANA TOTALS		219.5	2947	2801	95%	
-----------------------	--	--------------	-------------	-------------	------------	--

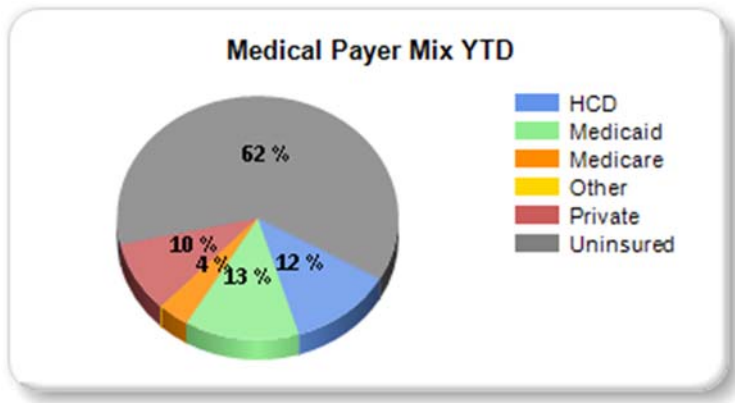
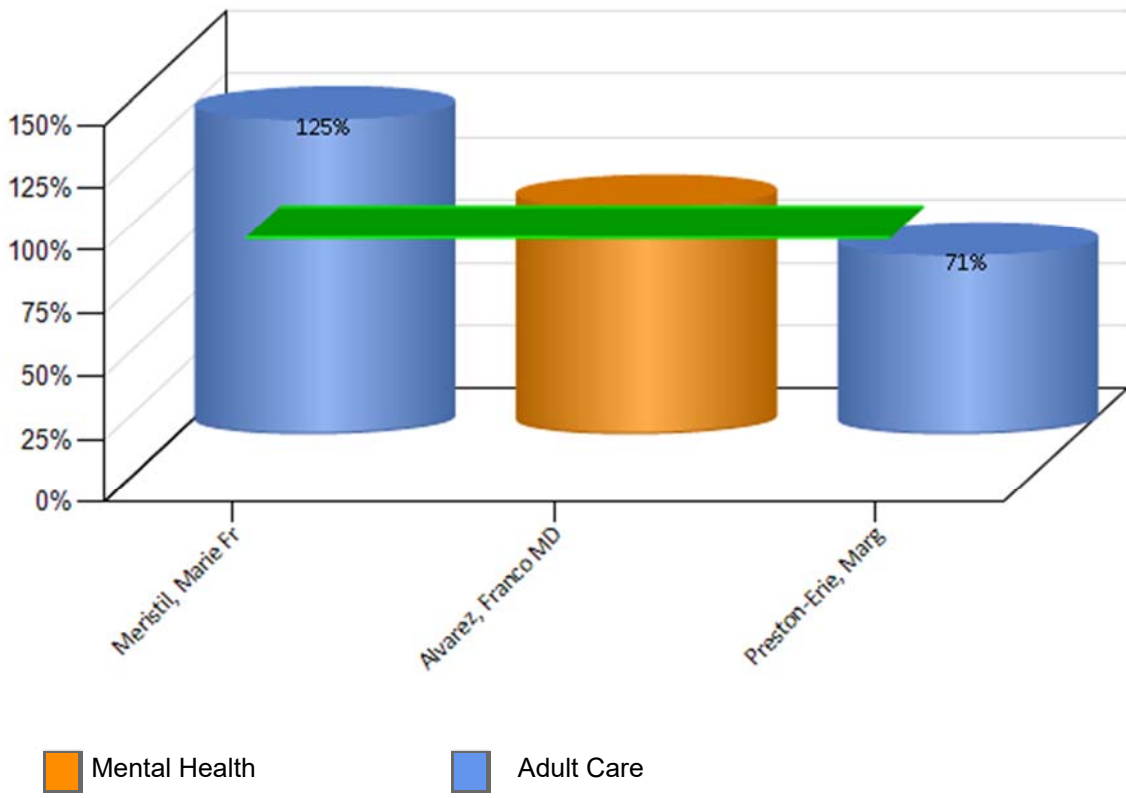
LANTANA PROVIDER PRODUCTIVITY NOVEMBER 2019



LEWIS CENTER TOTALS FOR NOVEMBER 2019

	Daily Target	Days Worked	Target for the month	Total for month seen	% Monthly Target Achieved	Daily Average
ADULT CARE						
Meristil, Marie Frantzcia ARNP	16	1.0	16	20	125%	20.0
Preston-Erie, Margareth ARNP	16	17.0	272	193	71%	11.4
LEWIS CENTER ADULT CARE TOTALS		18.0	288	213	74%	
MENTAL HEALTH						
Alvarez, Franco MD	16	12.0	192	173	90%	14.4
LEWIS CENTER MENTAL HEALTH TOTALS		12.0	192	173	90%	
LEWIS CENTER TOTALS		30.0	480	386	80%	

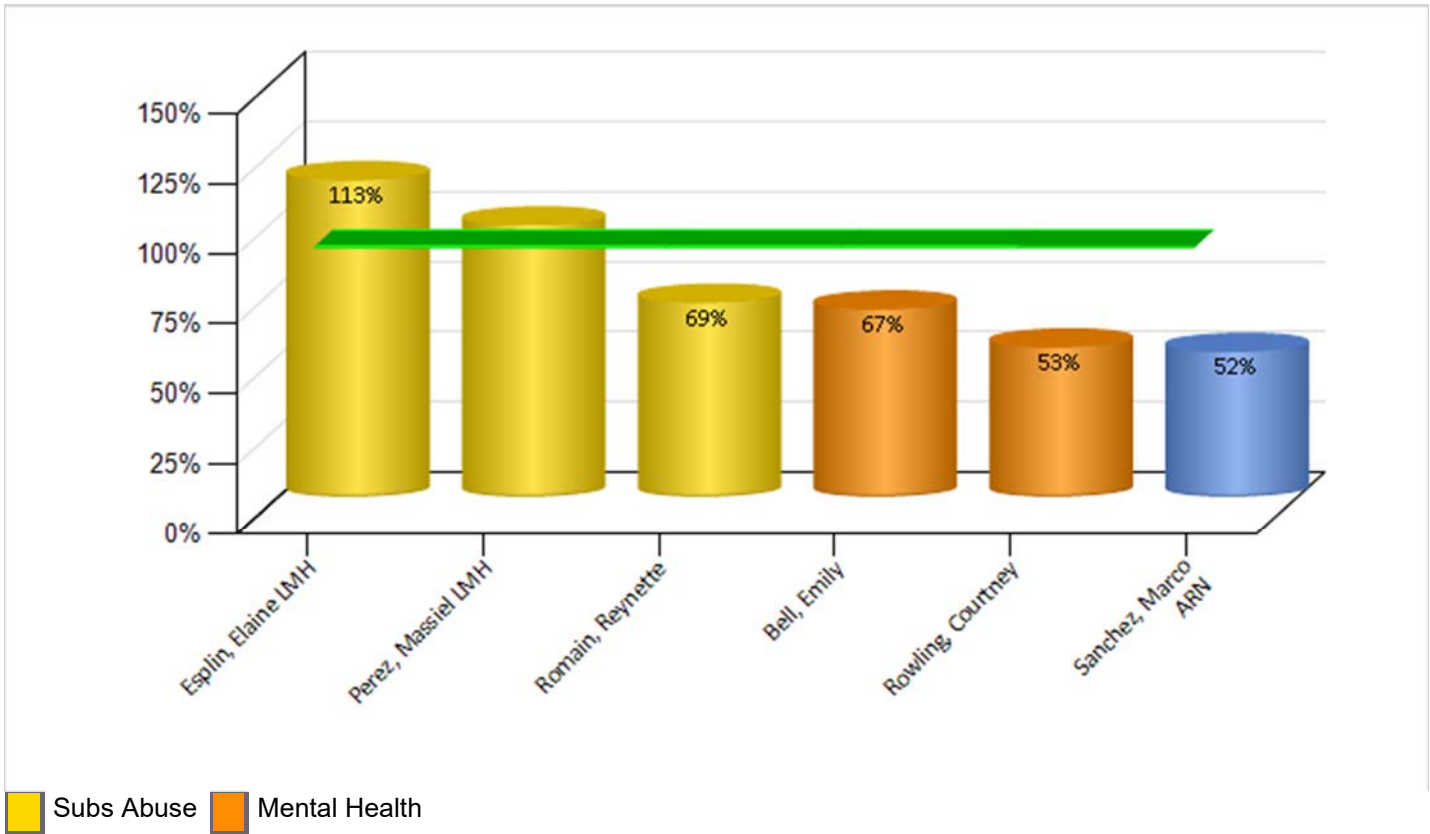
LEWIS CENTER PROVIDER PRODUCTIVITY NOVEMBER 2019



MANGONIA PARK TOTALS FOR NOVEMBER 2019

	Daily Target	Days Worked	Target for the month	Total for month seen	% Monthly Target Achieved	Daily Average
ADULT CARE						
Sanchez, Marco ARNP	10	13.0	130	67	52%	5.2
MANGONIA PARK ADULT CARE TOTALS		13.0	130	67	52%	
MENTAL HEALTH						
Bell, Emily	16	4.5	72	48	67%	10.7
Rowling, Courtney MD	16	12.0	192	102	53%	8.5
MANGONIA PARK MENTAL HEALTH TOTALS		16.5	264	150	57%	
SUBSTANCE ABUSE						
Esplin, Elaine LMHC	10	4.5	45	51	113%	11.3
Perez, Massiel LMHC	10	7.0	70	68	97%	9.7
Romain, Reynette	10	11.0	110	76	69%	6.9
MANGONIA PARK SUBSTANCE ABUSE TOTALS		22.5	225	195	87%	
MANGONIA PARK TOTALS			52.0	619	412	67%

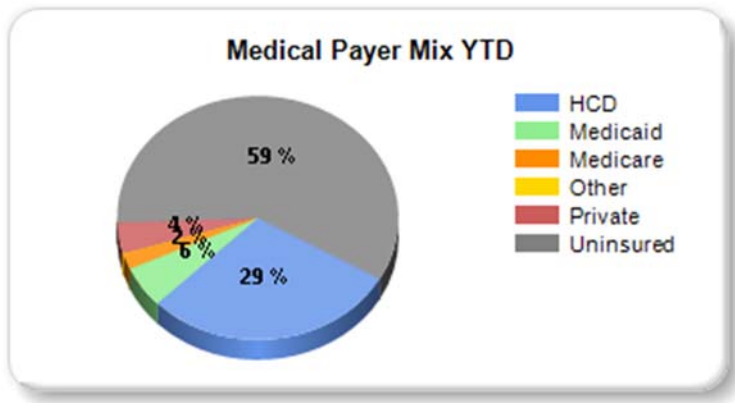
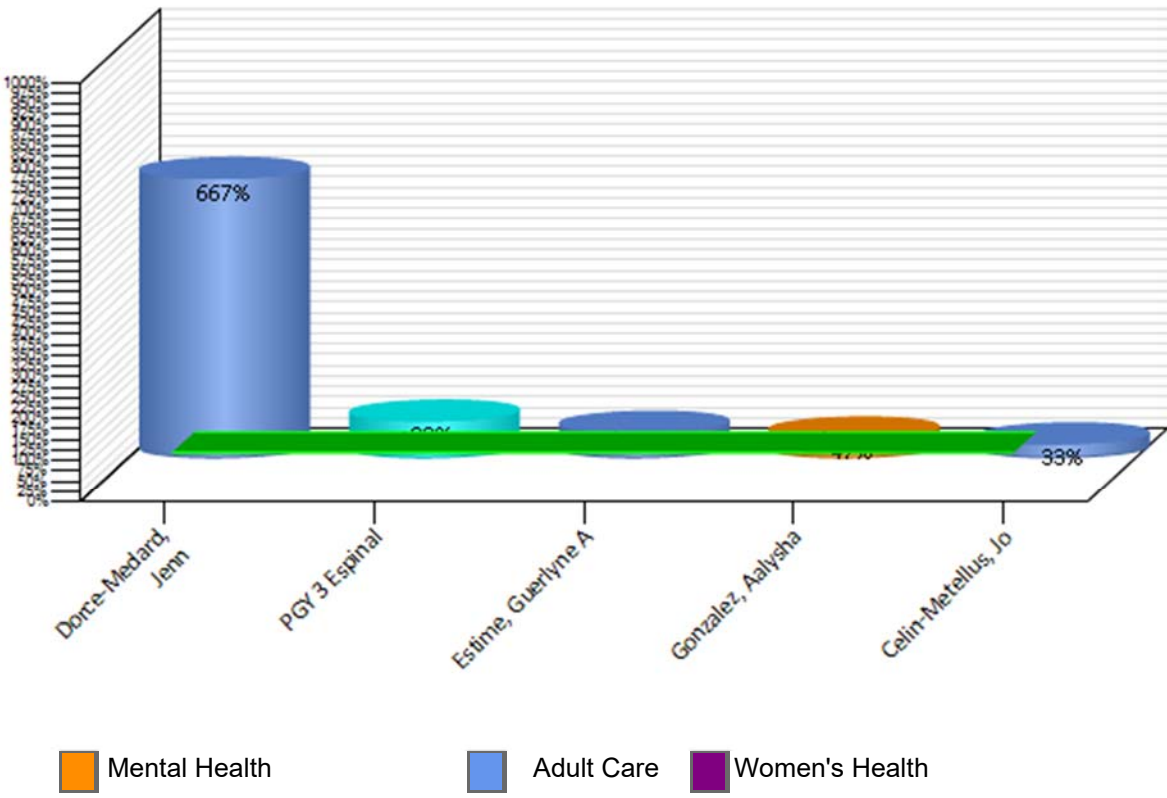
MANGONIA PARK PROVIDER PRODUCTIVITY NOVEMBER 2019



MOBILE CLINIC TOTALS FOR NOVEMBER 2019

	Daily Target	Days Worked	Target for the month	Total for month seen	% Monthly Target Achieved	Daily Average
RESIDENT						
PGY 3 Espinal	16	0.5	8	7	88%	14.0
MOBILE CLINIC RESIDENT TOTALS		0.5	8	7	88%	
ADULT CARE						
Dorce-Medard, Jennifer DO Resident Preceptor	3	0.5	2	10	667%	20.0
Estime, Guerlyne ARNP	12	16.0	192	117	61%	7.3
Celin-Metellus, Jourdine ARNP	12	0.5	6	2	33%	4.0
MOBILE CLINIC ADULT CARE TOTALS		17.0	200	129	65%	
MENTAL HEALTH						
Gonzalez, Aalysha LCSW	10	15.0	150	71	47%	4.7
MOBILE CLINIC MENTAL HEALTH TOTALS		15.0	150	71	47%	
MOBILE CLINIC TOTALS			32.5	358	207	58%

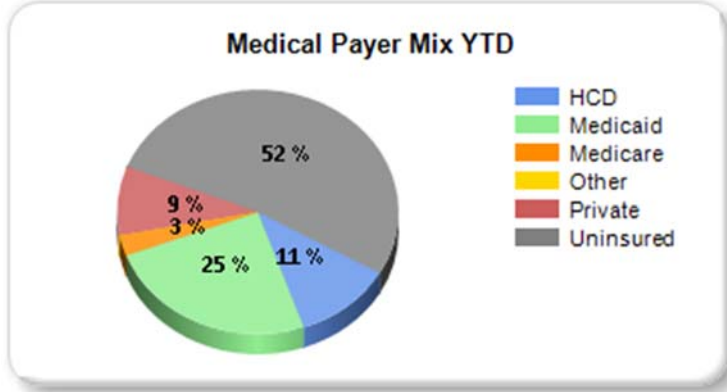
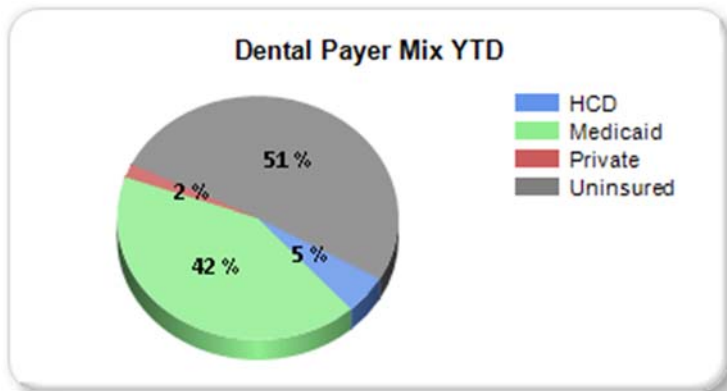
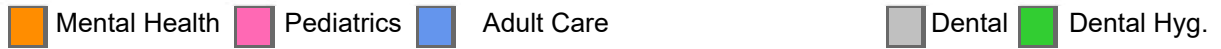
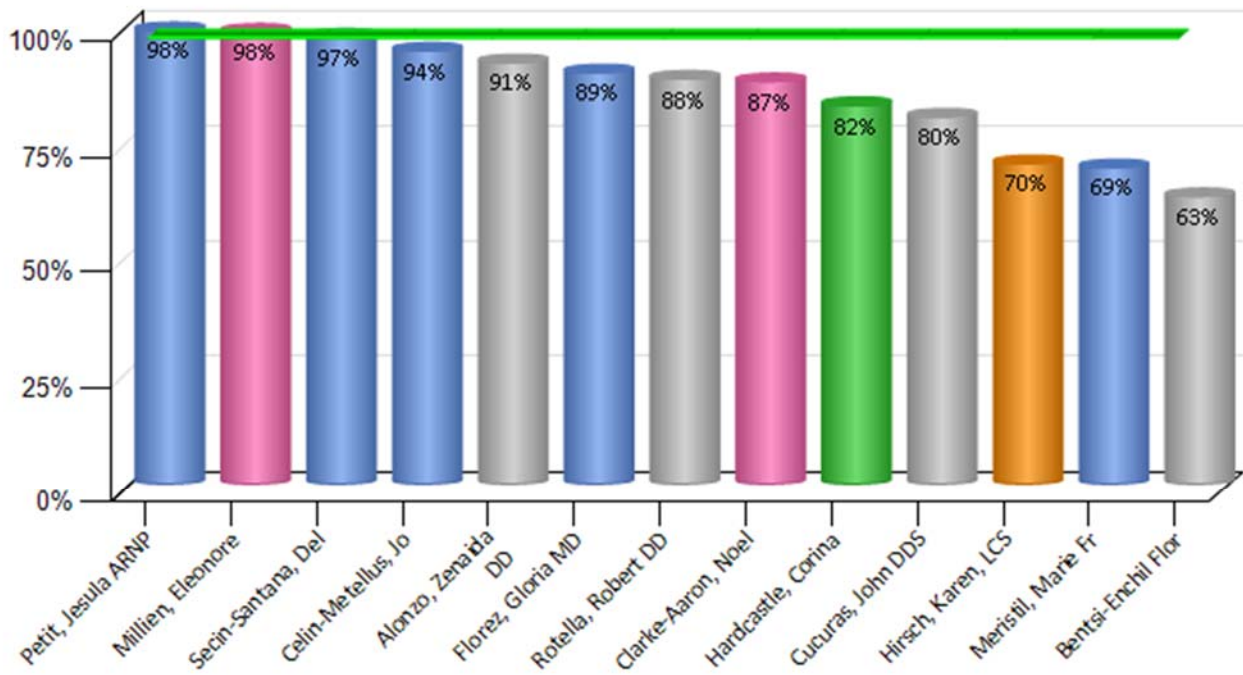
MOBILE CLINIC PROVIDER PRODUCTIVITY NOVEMBER 2019



WEST PALM BEACH TOTALS FOR NOVEMBER 2019

	Daily Target	Days Worked	Target for the month	Total for month seen	% Monthly Target Achieved	Daily Average
ADULT CARE						
Petit, Jesula ARNP	16	15.5	248	244	98%	15.7
Secin-Santana, Delvis MD	16	14.5	232	225	97%	15.5
Celin-Metellus, Jourdine ARNP	16	16.5	264	248	94%	15.0
Florez, Gloria MD	18	17.0	306	273	89%	16.1
Meristil, Marie Frantzcia ARNP	16	1.0	16	11	69%	11.0
WEST PALM BEACH ADULT CARE TOTALS		64.5	1066	1001	94%	
PEDIATRIC CARE						
Millien, Eleonore ARNP	16	16.0	256	251	98%	15.7
Clarke-Aaron, Noella MD	18	14.0	252	220	87%	15.7
WEST PALM BEACH PEDIATRIC CARE TOTALS		30.0	508	471	93%	
MENTAL HEALTH						
Hirsch, Karen, LCSW	10	14.5	145	101	70%	7.0
WEST PALM BEACH MENTAL HEALTH TOTALS		14.5	145	101	70%	
DENTAL						
Alonzo, Zenaida DDS	16	16.0	256	234	91%	14.6
Rotella, Robert DDS	16	18.0	288	253	88%	14.1
Cucuras, John DDS	16	10.5	168	134	80%	12.8
Bentsi-Enchil Flora DDS	16	4.0	64	40	63%	10.0
WEST PALM BEACH DENTAL TOTALS		48.5	776	661	85%	
DENTAL HYGIENE						
Hardcastle, Corina	8	17.5	140	115	82%	6.6
WEST PALM BEACH DENTAL HYGIENE TOTALS		17.5	140	115	82%	
WEST PALM BEACH TOTALS		175.0	2635	2349	89%	

WEST PALM BEACH PROVIDER PRODUCTIVITY NOVEMBER 2019



DISTRICT CLINIC HOLDINGS, INC.
BOARD OF DIRECTORS
December 10, 2019

1. Description: Licensed Independent Practitioner Credentialing and Privileging

2. Summary:

The agenda item represents the licensed independent practitioner(s) recommended for credentialing and privileging by the FQHC Medical Director and Dental Director.

3. Substantive Analysis:

The LIP(s) listed below satisfactorily completed the credentialing and privileges process and met the standards set forth within the approved Credentialing and Privileging Policy. The credentialing and privileging process ensures that all health center practitioners meet specific criteria and standards of professional qualifications. This criterion includes, but is not limited to:

- Current licensure, registration or certification
- Relevant education, training and experience
- Current clinical competence
- Health fitness, or ability to perform the requested privileges
- Malpractice history (NPDB query)
- Immunization and PPD status; and
- Life support training (BLS)

Last Name	First Name	Degree	Specialty	Credentialing
Kaloglian Silva	Michelle	DDS	General Dentistry	Initial Credentialing
Alvarez	Franco	MD	Psychiatry	Recredentialing
Celin-Metellus	Jourdine	APRN	Family Medicine Nurse Practitioner	Recredentialing
Meristil	Marie	APRN	Family Medicine Nurse Practitioner	Recredentialing

Primary source and secondary source verifications were performed for credentialing and privileging elements in accordance with state, federal and HRSA requirements. A Nationally accredited Credentials Verification Organization (CVO) was utilized to verify the elements requiring primary source verification.

The C.L. Brumback Primary Care Clinics utilized internal Credentialing staff and the FQHC Medical Director and Dental Director to support the credentialing and privileging process.

Michelle Kaloglian Silva, DDS is joining the West Palm Beach Clinic specializing in General Dentistry. She attended Sao Francisco University in Brazil and completed her residency program at the University of Florida. Dr. Kaloglian Silva has been in practice for over a year and is fluent in Portuguese and conversant in Spanish.

DISTRICT CLINIC HOLDINGS, INC.
BOARD OF DIRECTORS
December 10, 2019

Franco Alvarez, MD joined the Lewis Center in 2017 specializing in Psychiatry. He attended the University of Puerto Rico School of Medicine and completed his residency program at Wright State University. Dr. Alvarez is certified in Psychiatry by the American Board of Psychiatry and Neurology. He has been in practice for five years and is fluent in Spanish.

Jourdine Celin-Metellus, APRN joined the West Palm Beach Clinic in 2018 as a Nurse Practitioner specializing in Family Medicine. She attended South University and is certified as Family Nurse Practitioner by the American Nurses Credentialing Center. Ms. Celin-Metellus has been in practice for nearly two years and is fluent in French Creole.

Marie Meristil, APRN joined the Lake Worth Clinic in 2018 as a Nurse Practitioner specializing in Family Medicine. She attended Florida International University and is certified as an Adult-Gerontology Primary Care Nurse Practitioner by the American Academy of Nurse Practitioners. Ms. Meristil has been in practice for nearly two years and is fluent in French Creole and Spanish.

4. Fiscal Analysis & Economic Impact Statement:

	Amount	Budget
Capital Requirements		Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>
Annual Net Revenue		Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>
Annual Expenditures		Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>

Reviewed for financial accuracy and compliance with purchasing procedure:

N/A

 Joel H. Snook, CPA
 Chief Financial Officer

5. Reviewed/Approved by Committee:

N/A

 Committee Name

_____ Date Approved

6. Recommendation:

Staff recommends the Board approve the initial credentialing and privileging of Michelle Kaloglian Silva, DDS, General Dentistry.

Staff recommends the Board approve the recredentialing and renewal of privileges of Franco Alvarez, MD, Psychiatry.

DISTRICT CLINIC HOLDINGS, INC.
BOARD OF DIRECTORS
December 10, 2019


Staff recommends the Board approve the recredentialing and renewal of privileges of Jourdine Celin-Metellus, APRN, Family Medicine Nurse Practitioner.

Staff recommends the Board approve the recredentialing and renewal of privileges of Marie Meristil, APRN, Family Medicine Nurse Practitioner.

Approved for Legal sufficiency:



Valerie Shahriari
VP & General Counsel



Sarah Gonzalez, CPMSM, CPC
Director, Credentialing & Provider Services



Dr. Belma Andric
Chief Medical Officer, VP & Executive Director
of Clinic Services

DISTRICT CLINIC HOLDINGS, INC.
BOARD OF DIRECTORS
December 10, 2019

1. Description: Patient Relations Reports

2. Summary:

This agenda item provides the following:

- Quarterly Patient Relations Dashboard Q3

3. Substantive Analysis:

- See attached Quarterly Patient Relations Dashboard.

4. Fiscal Analysis & Economic Impact Statement:

	Amount	Budget
Capital Requirements	N/A	Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>
Annual Net Revenue	N/A	Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>
Annual Expenditures	N/A	Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>

Reviewed for financial accuracy and compliance with purchasing procedure:

N/A

 Joel Snook
 Chief Financial Officer

5. Reviewed/Approved by Committee:

N/A

 Committee Name

 Date Approved

DISTRICT CLINIC HOLDINGS, INC.
BOARD OF DIRECTORS
December 10, 2019

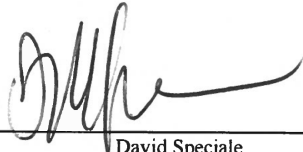
6. Recommendation:

Staff recommends the board approve the Patient Relations Reports.

Approved for Legal sufficiency:



Valerie Shahriari
General Counsel



David Speciale
Patient Relations Manager



Dr. Belma Andric
Chief Medical Officer, VP & Executive Director
of Clinic Services

PATIENT RELATIONS DASHBOARD

2019

January - September

COMPLAINTS/GRIEVANCES

CATEGORY	JAN	FEB	MAR	Q1 2019	APR	MAY	JUN	Q2 2019	JULY	AUG	SEPT	Q3 2019	OCT	NOV	DEC	Q4 2019	2019	2018
	#	#	#	TOTAL	#	#	#	TOTAL	#	#	#	TOTAL	#	#	#	TOTAL	TOTAL	TOTAL
Care & Treatment	7	6	2	15	6	3	3	12	4	5	5	14					41	23
Communication	2	3	2	7	3			3	1	1	2	4					14	11
Discharge				0	0			0				0					0	0
Environmental		1		1	0			0				0					1	1
Finance	1			1	0	1		1		2	1	3					5	2
Medical Records			1	1	0			0				0					1	2
Nursing Related				0	0			0				0					0	1
Clinical Support Staff				0	0			0				0					0	0
Other			1	1	0		1	1	3			3					5	21
Pharmacy Related	2			2	2			2				0					4	6
Physician Related			2	2	0			0	1			1					3	5
Respect Related	1	2		3	2	1	1	4			1	1					8	8
TOTAL:	13	12	8	33	13	5	5	23	9	8	9	26					82	80
Complaints/No Letter Required	5	7	4	16	5	2	2	9	5	6	4	15					40	43
Grievances/Letter Sent ≤ 7 days	8	5	4	17	8	3	3	14	4	2	5	11					42	44
Grievances/Letter Sent > 7 days	0	0	0	0	0	0	0	0	0	0	0	0					0	0
LETTERS NOT SENT FOR GRIEVANCES	0	0	0	0	0	0	0	0	0	0	0	0					0	4

Q1 encounters: 35,625

Q2 encounters: 37,071

Q3 encounters: 38,358

Q4 encounters:

SUMMARY OF TOP COMPLAINT/GRIEVANCE CATEGORIES

JUL:	Of the 9 occurrences there were 5 complaints and 4 grievances. There was 1 Dental complaint about a Dentist care in Delray, 1 Women's Health complaint from a patient concerning the wait time for receiving a lab result (over 30 days), and 7 Primary Care occurrences of which there were 3 complaints and 4 grievances. The 3 complaints included 2 for Quest Lab services and billing, and was 1 related to the District Cares authorization process. The 4 grievances included: receiving a lab result letter in the mail for a lab the patient did not receive, poor care & treatment by a provider at the Lewis Center, confusion with the referral process for a Humana patient, and a patient feeling disrespected by a Certified Application Counselor in Lantana. The Patient Experience Manager completed a "walk in your shoes" with patient to learn more about the patient experience. All complaints resolved to the patient's satisfaction and grievances resolved according to policy and procedure.
AUG:	Of the 8 occurrences there were 6 complaints and 2 grievances reported. There were 5 complaints for Primary Care services of which: 2 from the Delray Beach clinic for a delay in processing a patient referral and another related to a billing issue; 2 related to wait times at the Lantana and West Palm Beach clinics; and 1 from a Jupiter patient who was turned away from Quest labs for an outstanding balance. The last complaint was from a Delray Beach Dental patient who refused the Hygienist recommendation to receive an SRP (deep cleaning) instead of a one-visit, full-mouth cleaning. Of the 2 grievances, 1 was from a WPB patient related to the wait time for a Primary Care Visit, and 1 was from a Delray Beach Dental Clinic patient who felt the hygienist was "too rough" during her teeth cleaning. All complaints resolved to the patient's satisfaction and grievances resolved according to policy and procedure.
SEP:	Of the 9 occurrences there were 4 complaints and 5 grievances. All 4 complaints were submitted by patients of the West Boca Clinic. Of these 4: one (1) was related to the sliding fee scale policy, 1 related to frustrations with contacting clinic staff directly, 1 was related to an issue with the security guard, and 1 was regarding a denied request for a patient to be seen by a medical provider via telephone / telemedicine. Of the 5 grievances, 4 were for Primary Care Services of which one (1) was related to care and treatment of a parathyroid issue at the Delray Beach Clinic, 1 was related to the incorrect processing of an authorization at the Home Office, and 2 were submitted by Lake Worth patient: 1 regarding the patients inability to reach the clinic directly by phone, and 1 was regarding an incorrect lab result. The 1 Dental grievance was submitted by a WPB patient who reported she was denied for service. The Patient Experience Manager completed a "walk in your shoes" with patient to learn more about the patient experience. All complaints resolved to the patient's satisfaction and grievances resolved according to policy and procedure.

COMPLIMENTS

	<u>JAN</u>	<u>FEB</u>	<u>MAR</u>	<u>Q1</u> <u>2019</u> <u>TOTAL</u>	<u>APR</u>	<u>MAY</u>	<u>JUN</u>	<u>Q2</u> <u>2019</u> <u>TOTAL</u>	<u>JULY</u>	<u>AUG</u>	<u>SEPT</u>	<u>Q3</u> <u>2019</u> <u>TOTAL</u>	<u>OCT</u>	<u>NOV</u>	<u>DEC</u>	<u>Q4</u> <u>2019</u> <u>TOTAL</u>	<u>2019</u> <u>TOTAL</u>	<u>2018</u> <u>TOTAL</u>
# COMPLIMENTS RECEIVED	1	9	13	23	8	5	14	27	11	5	27	43					93	316

SUMMARY OF COMPLIMENTS

<u>JUL:</u>	There were 11 compliments of which 7 were for staff and services for Primary Care, 2 were for dental providers Dr. Flora Bentsi-Enchill, 1 for the Delray Dental Team, and 1 compliment was for Substance Abuse Services Program.
<u>AUG:</u>	There were 5 compliments for the month. One was made by a clinic partner "Fyzical Therapy Palm Beach" to the FQHC Referral Team for their hard work and dedication to the patients they serve. One made to Rochelle Francois, Registration Specialist at WPB for excellent service. One was made on behalf of Keisha Pittman, MA/ Registrations Specialist at the Lewis Center for being professional. One for Irlande Polynice, MA at the WPB Clinic for being helpful and nice. One made for Dr. Delvis Secin Santana, WPB provider for being a compassionate, thorough, and caring doctor.
<u>SEP:</u>	There were 27 Primary Care Service compliments for the month. Of these compliments: 16 were for WPB registration and nursing staff, 5 were for West Boca Staff, 5 for the Lewis Center, and 1 for Belle Glade staff. Some of the compliments are: "I couldn't have a better healthcare experience. Thanks so much for all staff members", "patient stated to staff that she loved how she is treated every time she comes to the clinic and that she enjoys the friendly staff and the provider", "the staff sincerely care about our patients", "Excellent, polite, good respectful, speedy", "My experience with my visit today was amazing. I received exceptional service from the doctor and staff. Thank you!".

DISTRICT CLINIC HOLDINGS, INC.
BOARD OF DIRECTORS
December 11, 2019

1. Description: Quality Report

2. Summary:

This agenda item provides the following:

- UDS Report – YTD November 2019

3. Substantive Analysis:

PATIENT SAFETY & ADVERSE EVENTS

Patient safety and risk, including adverse events, peer review and chart review are brought to the board “under separate cover” on a quarterly basis.

PATIENT SATISFACTION & GRIEVANCES

The patient satisfaction surveys are currently being administered in all the clinics. At the end of 2019 a roll-up report will be presented. We have added several platforms that will allow us to survey our patients in more convenient ways such as by cell phone app.

The clinics are increasing the amount and variety of patient educational materials available before and after their appointments. Content will be streamed to the screens present in the waiting rooms in order to provide education via SnapComm and video platforms. Educational brochures will also be provided for patients who prefer written content.

QUALITY ASSURANCE & IMPROVEMENT

Of the 14 UDS Measures: 7 exceeded the HRSA Goal and 7 were short of the HRSA Goal.

Currently the cervical cancer screening and CAD measures are within 2% of the goal. Appropriate use of Asthma Medications is not within 1% of our target. Weight screening and counseling for children and adolescents, although not yet met is 7% higher this year than last year and is not within 4% of our goal. HIV linkage to care is 100% for 2019.

It is important to keep in mind that although some measures such as childhood immunizations have not reached our goal, the numbers have improved substantially over 2018. Changes to the pediatric workflow are in progress as well as a more substantial tracking system to identify patients who are close to compliance and schedule them for services.

HRSA as well as The C.L. Brumback Primary Care Clinic recognize the global diabetes epidemic as an area of specific concern. The Clinics plan on implementing in house HgbA1c screening and a robust patient education program in order to increase

DISTRICT CLINIC HOLDINGS, INC.
BOARD OF DIRECTORS
December 11, 2019

compliance and self-management of diabetic patients as well as promote early diagnosis of pre-diabetics with the aim of decreasing conversion.

UTILIZATION OF HEALTH CENTER SERVICES

The Clinics are evaluating and improving the patient outreach process. MOUs have been initiated and updated depending on need. In order to measure the need and success of our outreach efforts a new “outreach” option has been added to the quick view in the EHR. The goal of patient outreach is to identify patients who would benefit from our services and increase their presence in our clinics.

4. Fiscal Analysis & Economic Impact Statement:

	Amount	Budget
Capital Requirements	N/A	Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>
Annual Net Revenue	N/A	Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>
Annual Expenditures	N/A	Yes <input type="checkbox"/> No <input checked="" type="checkbox"/>

Reviewed for financial accuracy and compliance with purchasing procedure:

N/A

 Joel Snook
 Chief Financial Officer

5. Reviewed/Approved by Committee:

N/A

 Committee Name

 Date Approved

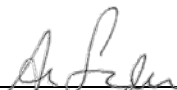
6. Recommendation:

Staff recommends the Board Approve the Quality Report.

Approved for Legal sufficiency:



 Valerie Shahriari
 General Counsel

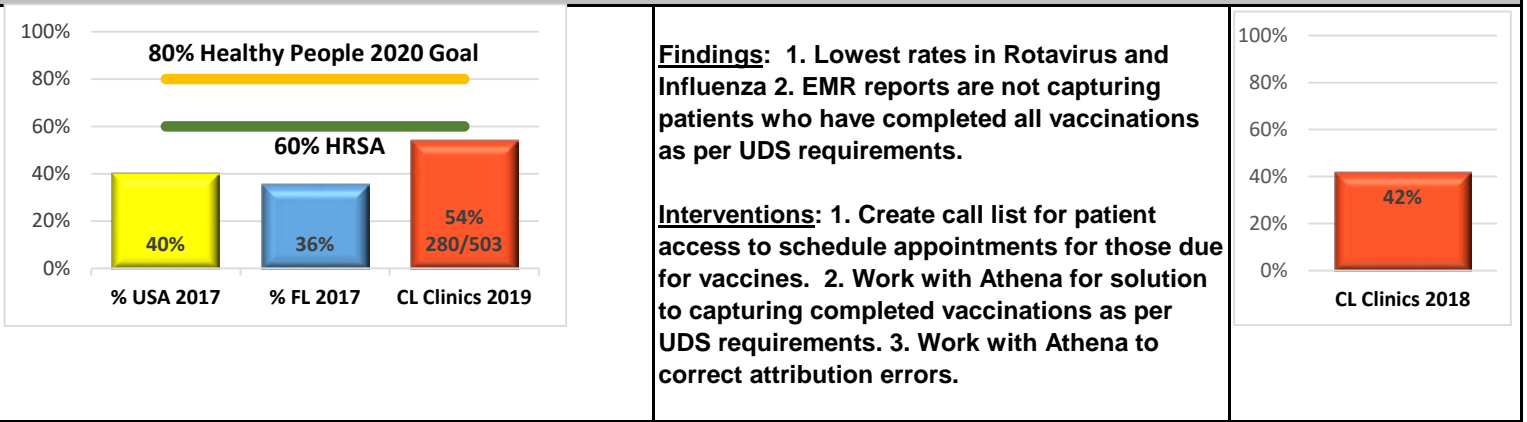


 Dr. Ana Ferwerda
 FQHC Medical Director

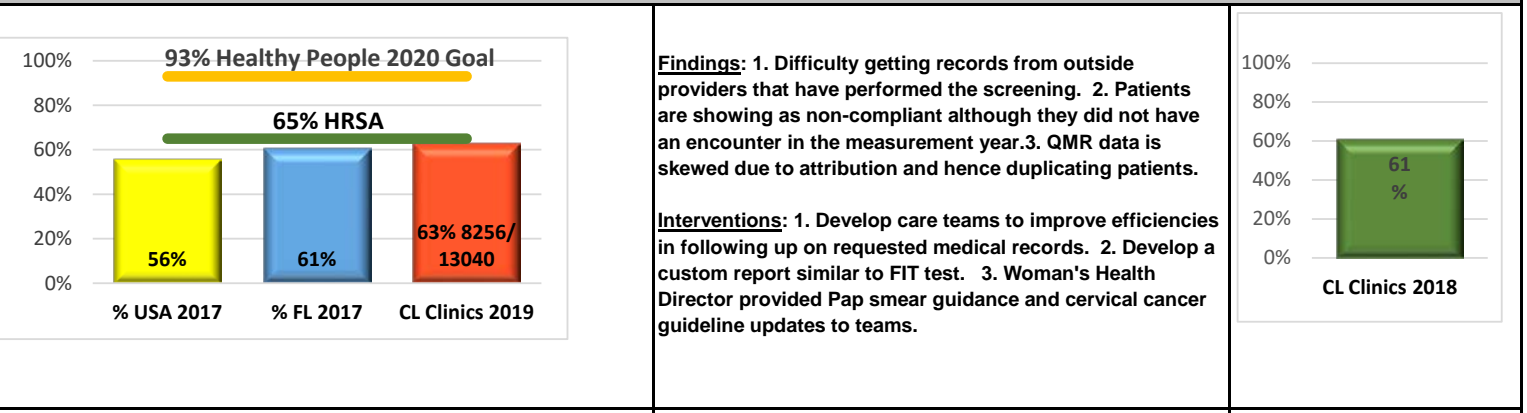


 Dr. Belma Andric
 Chief Medical Officer, VP & Executive Director
 of Clinic Services

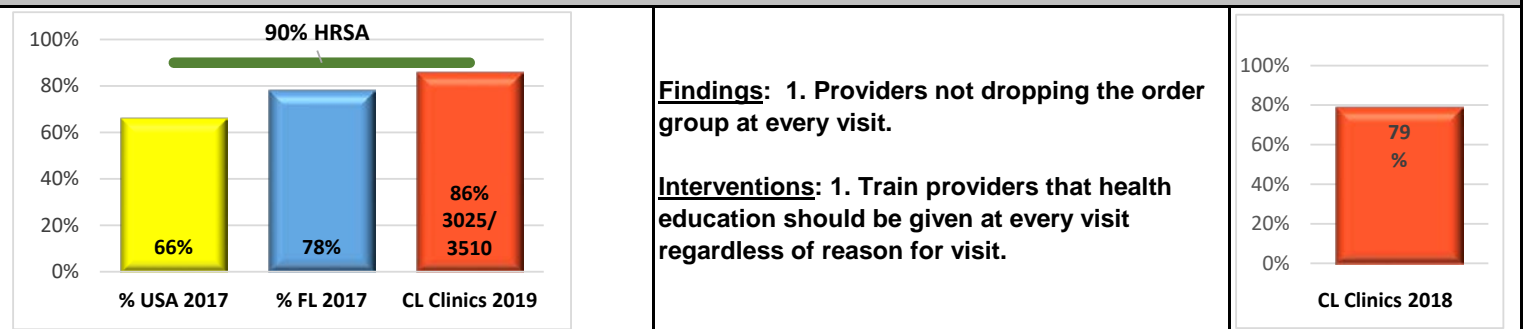
CHILDHOOD IMMUNIZATION



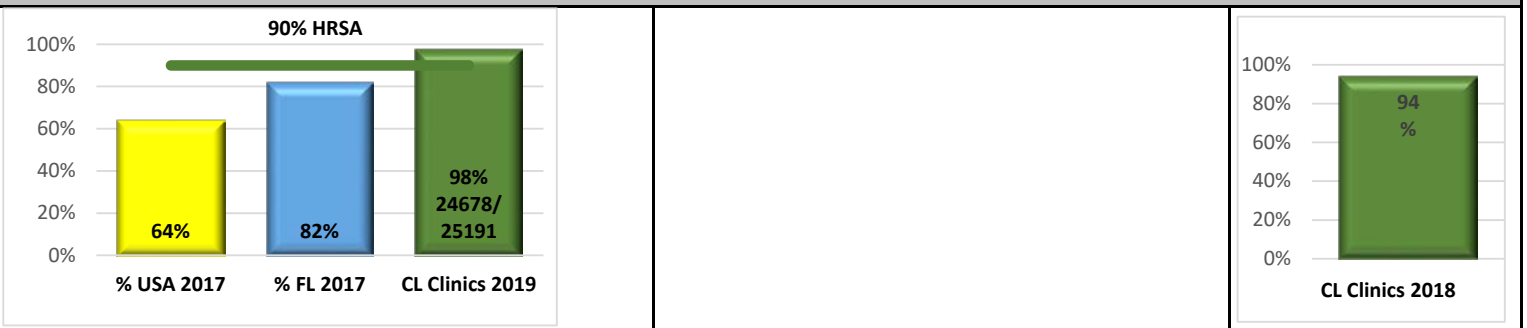
CERVICAL CANCER SCREENING



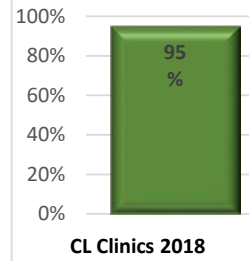
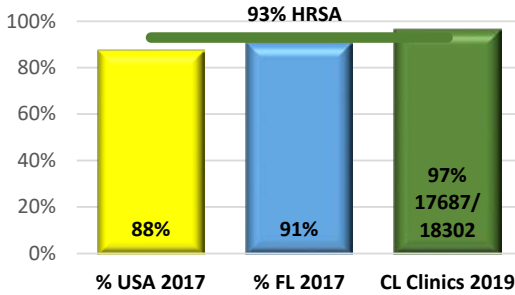
WEIGHT SCREENING AND COUNSELING FOR CHILDREN AND ADOLESCENTS



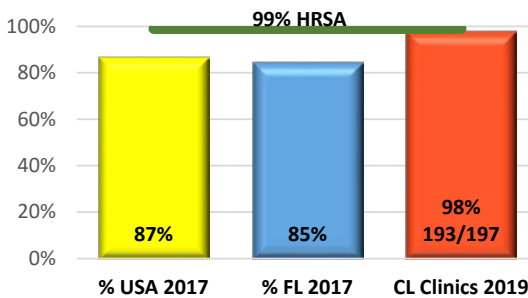
ADULT WEIGHT SCREENING AND FOLLOW UP



TOBACCO USE SCREENING AND CESSATION INTERVENTION

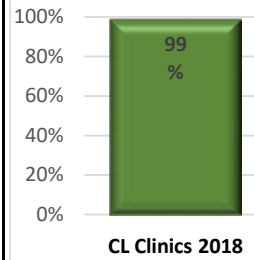


ASTHMA PHARMACOLOGIC THERAPY

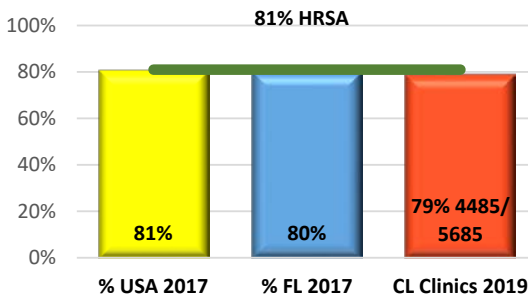


Findings: 1. Asthma medication must dated as active in 2019 to be compliant and some therapies that were first prescribed in 2018 may not have updated dates.

Interventions: 1. Providers have been trained to update the dates. 2. Send cases to individual providers to update medication list if still active.



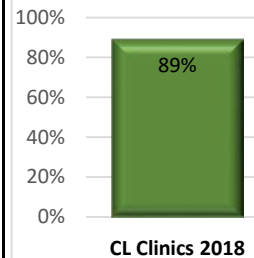
CORONARY ARTERY DISEASE (CAD): LIPID THERAPY



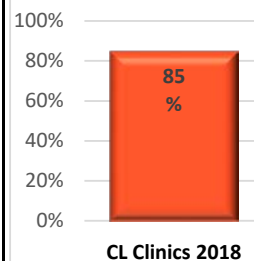
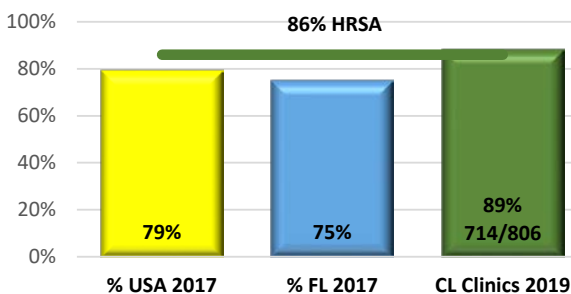
Findings: There are patients who have been recognized as meeting exclusion criteria for measure, however are still presenting as requiring statin on quality tab.

This measure covers 3 populations. It is the theory that the diabetic patients are what is holding us back.

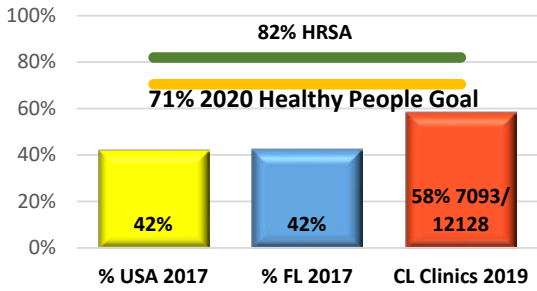
Interventions: (1) Send ticket to Athena for review of exclusion criteria. (2) Measure validation and audit to be completed.



ISCHEMIC VASCULAR DISEASE (IVD): Antiplatelet Therapy

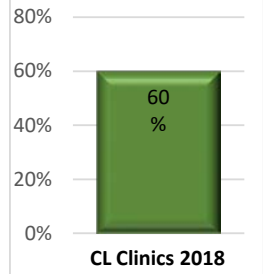


COLORECTAL CANCER SCREENING

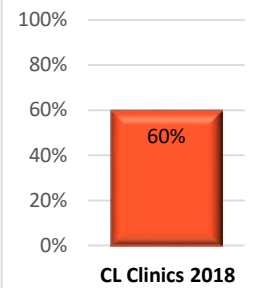
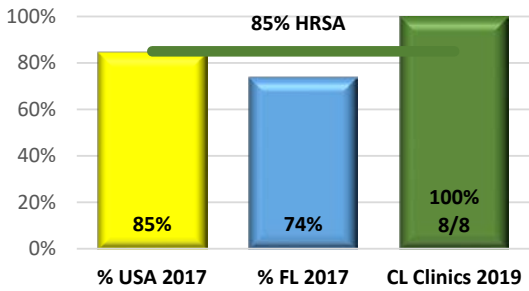


Findings: 1. Difficulty in getting FIT test returned from patient. 2. Some patients may have colonoscopies in Allscripts that have not been updated in Athena.

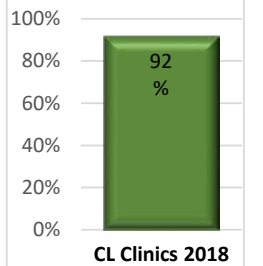
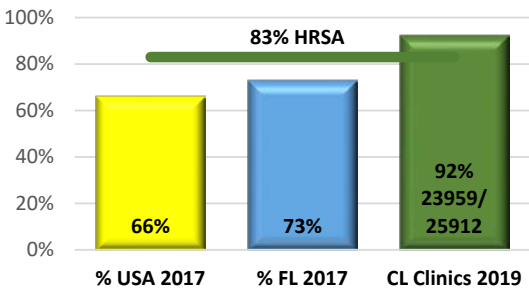
Interventions: 1. Encourage POD 2. More robust patient follow up through phone call reminders. 3. Custom report developed and dashboard created 4. Work on importing colonoscopy quality data into Athena.



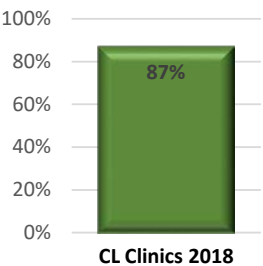
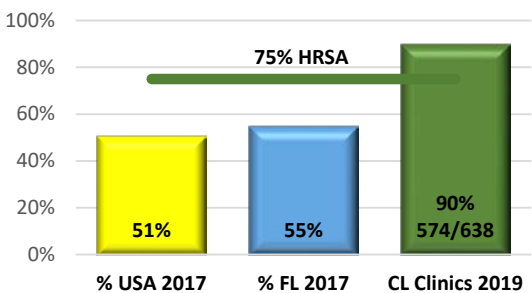
HIV LINKAGE TO CARE



PATIENTS SCREENED FOR DEPRESSION AND FOLLOW-UP

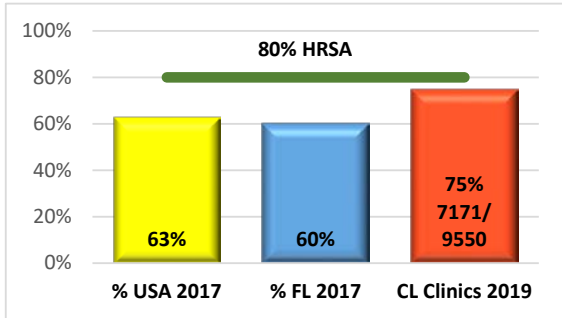


DENTAL SEALANTS



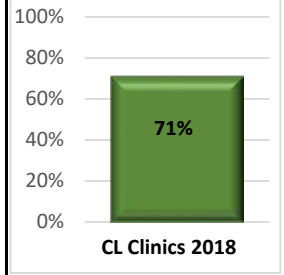
C. L. BRUMBACK PRIMARY CARE CLINICS
YTD November 2019

HYPERTENSION

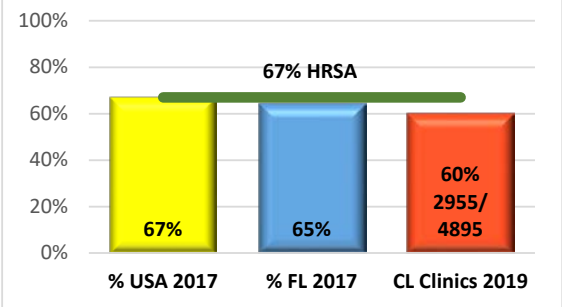


Findings: 1. Providers failing to give short term follow up for uncontrolled BP 2. non-adherence to medication regimen.

Interventions: 1. Reeducate on short interval follow up for uncontrolled hypertension and advancement of therapy 2. Encourage use of combination pills. 3. Pharmacy will begin sending patient messages to providers to recommend changing to combination therapy when appropriate.



DIABETES



Findings: 1. Patients are non-compliant with therapy for various reasons (pill burden, fear of insulin, lack of understanding the disease). 2. Clinical inertia

Interventions: 1. Implement POC A1c machines in clinic. 2. Collaborate with pharmacy on educating patients on medications and medication reconciliation. 3. Build care teams to include health educator to address high risk patients. 4. Provide lunch and learns on Diabetes management. 5. Outreach to patients without A1c on chart.

