Health Care District
PALM BEACH COUNTY

Provider Bulletin

Attention:	**Participating Providers**		
Subject:	Benefit Changes		
Program:	District Cares (Option 1)	**Bulletin Date:**	April 18, 2019
Bulletin Number:	19-004	**Effective Date:**	May 1, 2019

Purpose:

This bulletin serves to notify participating providers of benefit changes for District Cares members.

Change:

Effective May 1, 2019 – Benefits for the following services are as follows:

SERVICE	AUTHORIZATION	BENEFIT
Inpatient – Acute Care	Yes / Required	Ten (10) days per calendar year (combined with Rehab)
Inpatient – Rehabilitation (hospital setting)	Yes / Required	Ten (10) days per calendar year (combined with Acute Care)
Outpatient - Cardiac Rehabilitation	Yes / Required	One (1) 12-week (24 visits) occurrence per year
Observation Stay	No / Not required	(2) 23-hour stays per calendar year
Optometry	N/A	Not covered
Home Care / Home Infusion	Yes / Required	Combined 45 days per calendar year (skilled nursing care and home infusion)
Hospice	N/A	Not covered

The **CCP Prior Authorization Request Form** is available for submitting authorization requests **through April 30, 2019**.

Beginning May 1, 2019 – all authorization requests must be submitted through **CCP's PlanLink portal**.

PlanLink Registration information is available at:

https://www.hcdpbc.org/for-providers/provider-portal-planlink-registration

Questions:

If you have any questions pertaining to this bulletin, please contact the Provider Services Department at (866) 930-1002.

Please insert the bulletin into your Provider Handbook. The policies and procedures in this bulletin supersede any related policies and procedures in the handbook.

Health Care District Palm Beach County (HCDPBC)

PRIOR AUTHORIZATION REQUEST FORM

Fax #: 954-699-0741

CONFIDENTIAL HEALTH INFORMATION

Prior to visit, check Plan Link or call HCDPBC Customer Service at 866-930-0035 to verify eligibility
To register for Plan Link visit :
https://www.hcdpbc.org/for-providers/provider-portal-planlink-registration

Include supporting clinical documentation with every request | INCOMPLETE REQUESTS WILL NOT BE PROCESSSED

Mbr Name: _____

Mbr ID#: _____ Phone #: _____ DOB: _____

Mbr Address: _____

Requesting Provider Name:_____ NPI#_____

Requesting Provider Address: _____

Phone #: _____ Fax #: _____

Office contact person name: _____ Date: _____

Service Request: _____ ☐ Inpatient ☐ Outpatient

Provider Name: _____ **NPI# (Required)**_____ Phone #_____

Provider Address:_____ Fax #: _____

Diagnosis/ ICD-10 Code(s):_____

Procedure/ CPT/ HCPCS Code(s): _____

_____

Submit claims for DOS 4/1/19 forward through Availity, Payer ID PBHD1/Community Care Plan (Palm Beach Health District)

Authorization DOES NOT GUARANTEE PAYMENT. Payment is subject to member's eligibility on the date of the service is rendered, contractual provision of the plan, and standard industry billing guidelines. Prior Authorization Request Forms received after 5:00PM, will be considered received the next business day.

Initial here once you read all policies (Page 4 -22 of package)

Person requesting access must sign and date the form.

To send applications via fax, send to:
Fax number 954-251-4044.

To send applications via email, send to:
ccp.provider@ccpcares.org.

Memorial Healthcare System

ENTERPRISE SYSTEM ACCESS REQUEST FORM

You have the right to not provide the personal information on this form. If you choose not to complete this form in its entirety, you will be required to present yourself in person to the Department leader/MHS sponsor approving the access so that we can confirm your identity.

Please fill out this form entirely. Incomplete forms can delay your account setup process.
NON-MHS EMPLOYEES: ALL REQUIRED NOTICES MUST BE SENT TO MHS IT SYSTEM ACCESS TEAM VIA FAX (954-276-5397) OR EMAIL (MHSAccessRequestformONLY@mhs.net)
MHS EMPLOYEES: PLEASE SUBMIT AN ONLINE REQUEST AND ATTACH COMPLETED FORM

**All Users are required to read the following Policies. Initial by each Policy to confirm that you have received it.

- System Access Establishment. Modification and Termination Policy and Procedure ___
- Risk Analysis and Risk Management Policy ___
- Information System Activity Review Policy and Procedure ___

USER INFORMATION (TO BE FILLED OUT BY THE PERSON REQUIRING ACCESS)			
*Today's Date:	* Legal Last Name:	*Legal First Name:	MI:

Note: As part of the user ID creation process, all users will automatically be setup with MHS network login IDs as well as an MHS email account (if requested). User IDs are normally established with the first initial of the first name and complete last name, depending on availability. Please write legibly. You will be notified by MHS when the user ID is established. If an MHS email account is set up, we will use the email address to send periodic updates and other important system-related notifications, so please be sure to check this email account often.

*Birth Date (MM/DD/YY):	* Office Phone:	* Last 4 digits Social Security #:
*Office street address:		*Mobile Phone:
*City:	*State: *Zip Code:	* Your Email Address:

The above information is true to the best of my knowledge. I understand my obligations under MHS policies and applicable law, including HIPAA and related rules and regulations, and agree to utilize information only as needed to perform my job as part of the workforce of a Covered Entity or as a Business Associate of a Covered Entity (each as defined in HIPAA). **I agree to comply with all MHS policies and procedures, and the terms of the Confidentiality and Data Security Agreement attached to this 3 page form and incorporated by reference. I agree that I am responsible for maintaining the custody and security of any MHS data I access, view, print, download or otherwise obtain from MHS. It is my sole responsibility to report any suspected breach of security or loss of custody of any MHS confidential information to the Privacy Reporting Number (954) 265-1165 or I can also send an email to mhsprivacy@mhs.net.**

*Requestor's Signature:	*Date:

MHS SPONSOR VERIFICATION SECTION (TO BE FILLED OUT BY MHS SPONSOR ONLY FOR CONTRACTOR/STUDENT/VENDOR REQUESTS)		
User Title:	Company/School:	
Start Date:	End Date:	Sponsor's Employee ID #:
Name of MHS Sponsor approving this request:		
Sponsor's Department:		Sponsor's Email Address:
Sponsor's Title (Supervisor or above):		Sponsor's Office Phone:
***Applications/Access Requested:		

The above information is true to the best of my knowledge. I understand my obligations under MHS policies and applicable law, including **HIPAA** and related rules and regulations, and certify that the above named user has a legitimate need to access MHS systems to perform duties for my department. I authorize this user to be setup with access to the systems as indicated on this form. I agree to notify MHS IT System Access Team via fax (954) 276-5397 or email MHSAccessRequestformONLY@mhs.net of any changes to this user's status under my Department. All user IDs that are not used within a 3 month period will be disabled as a security precaution. I agree to comply with all MHS policies and procedures and will ensure that this user complies by those policies. Remote access to any MHS system may require the use of a type of security device such as a token. Upon termination of the user's assignment or duties in my department, I agree to immediately return all devices that have been provided to this user. I will immediately notify MHS IT System Access Team via fax (954) 276-5397 or email MHSAccessRequestformONLY@mhs.net to delete the user IDs that have been setup for this user.

*Sponsor's Signature:	*Date:

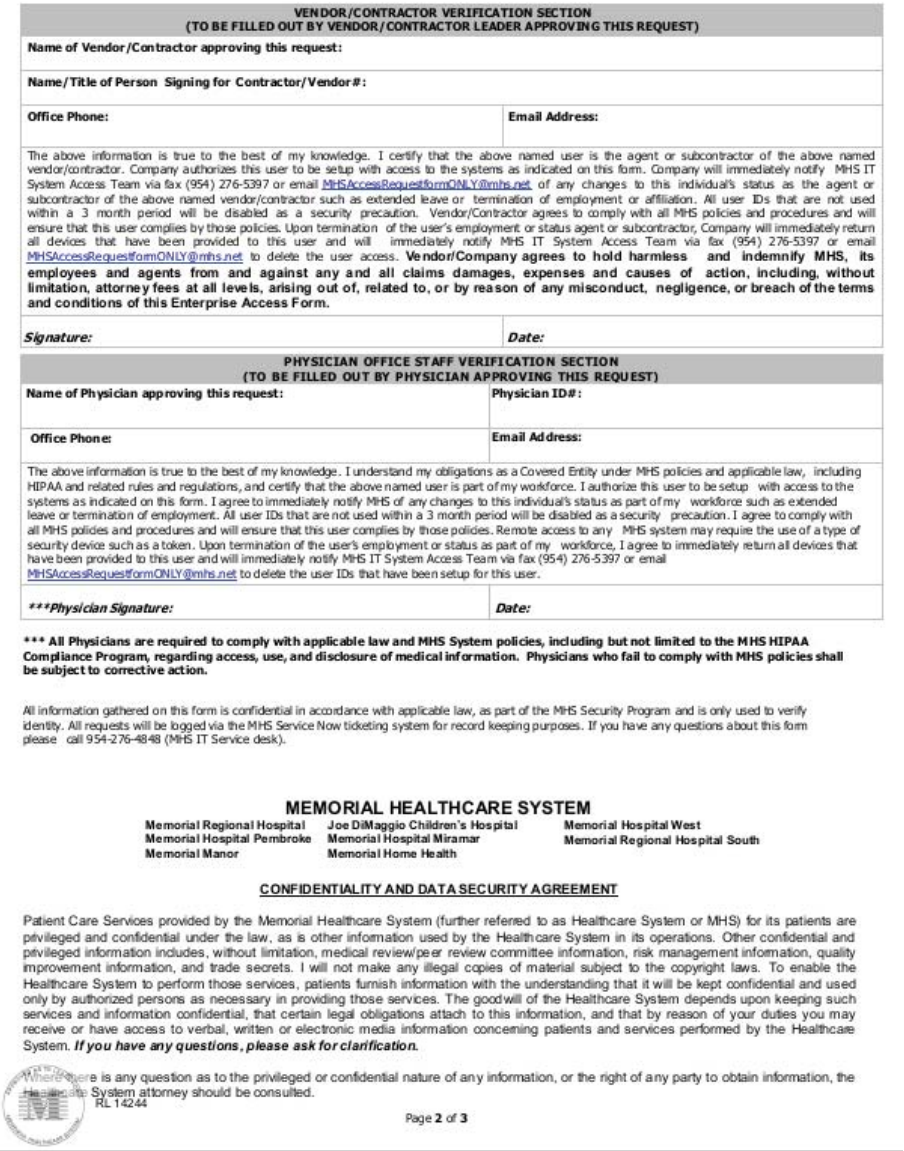
RL 14244

Each person requesting access to Plan Link/Epic Link must complete this form including the office Site Managers.

All PlanLink users complete this Form. Complete this top section with information pertaining to the person requesting the access to PlanLink.

Enter the last 4 of SS# or a 4-digit PIN. NOTE: you must remember the 4 digit PIN. You will not be able to reinstate your access without this PIN and you will need to submit new forms for access.

DO NOT COMPLETE THIS SECTION



VENDOR/CONTRACTOR VERIFICATION SECTION
(TO BE FILLED OUT BY VENDOR/CONTRACTOR LEADER APPROVING THIS REQUEST)

Name of Vendor/Contractor approving this request:

Name/Title of Person Signing for Contractor/Vendor#:

Office Phone: | **Email Address:**

The above information is true to the best of my knowledge. I certify that the above named user is the agent or subcontractor of the above named vendor/contractor. Company authorizes this user to be setup with access to the systems as indicated on this form. Company will immediately notify MHS IT System Access Team via fax (954) 276-5397 or email MHSAccessRequestformONLY@mhs.net of any changes to this individual's status as the agent or subcontractor of the above named vendor/contractor such as extended leave or termination of employment or affiliation. All user IDs that are not used within a 3 month period will be disabled as a security precaution. Vendor/Contractor agrees to comply with all MHS policies and procedures and will ensure that this user complies by those policies. Upon termination of the user's employment or status agent or subcontractor, Company will immediately return all devices that have been provided to this user and will immediately notify MHS IT System Access Team via fax (954) 276-5397 or email MHSAccessRequestformONLY@mhs.net to delete the user access. **Vendor/Company agrees to hold harmless and indemnify MHS, its employees and agents from and against any and all claims damages, expenses and causes of action, including, without limitation, attorney fees at all levels, arising out of, related to, or by reason of any misconduct, negligence, or breach of the terms and conditions of this Enterprise Access Form.**

Signature: | ***Date:***

PHYSICIAN OFFICE STAFF VERIFICATION SECTION
(TO BE FILLED OUT BY PHYSICIAN APPROVING THIS REQUEST)

Name of Physician approving this request: | **Physician ID#:**

Office Phone: | **Email Address:**

The above information is true to the best of my knowledge. I understand my obligations as a Covered Entity under MHS policies and applicable law, including HIPAA and related rules and regulations, and certify that the above named user is part of my workforce. I authorize this user to be setup with access to the systems as indicated on this form. I agree to immediately notify MHS of any changes to this individual's status as part of my workforce such as extended leave or termination of employment. All user IDs that are not used within a 3 month period will be disabled as a security precaution. I agree to comply with all MHS policies and procedures and will ensure that this user complies by those policies. Remote access to any MHS system may require the use of a type of security device such as a token. Upon termination of the user's employment or status as part of my workforce, I agree to immediately return all devices that have been provided to this user and will immediately notify MHS IT System Access Team via fax (954) 276-5397 or email MHSAccessRequestformONLY@mhs.net to delete the user IDs that have been setup for this user.

******Physician Signature:*** | ***Date:***

***** All Physicians are required to comply with applicable law and MHS System policies, including but not limited to the MHS HIPAA Compliance Program, regarding access, use, and disclosure of medical information. Physicians who fail to comply with MHS policies shall be subject to corrective action.**

All information gathered on this form is confidential in accordance with applicable law, as part of the MHS Security Program and is only used to verify identity. All requests will be logged via the MHS Service Now ticketing system for record keeping purposes. If you have any questions about this form please call 954-276-4848 (MHS IT Service desk).

MEMORIAL HEALTHCARE SYSTEM

Memorial Regional Hospital | **Joe DiMaggio Children's Hospital** | **Memorial Hospital West**
Memorial Hospital Pembroke | **Memorial Hospital Miramar** | **Memorial Regional Hospital South**
Memorial Manor | **Memorial Home Health**

CONFIDENTIALITY AND DATA SECURITY AGREEMENT

Patient Care Services provided by the Memorial Healthcare System (further referred to as Healthcare System or MHS) for its patients are privileged and confidential under the law, as is other information used by the Healthcare System in its operations. Other confidential and privileged information includes, without limitation, medical review/peer review committee information, risk management information, quality improvement information, and trade secrets. I will not make any illegal copies of material subject to the copyright laws. To enable the Healthcare System to perform those services, patients furnish information with the understanding that it will be kept confidential and used only by authorized persons as necessary in providing those services. The goodwill of the Healthcare System depends upon keeping such services and information confidential, that certain legal obligations attach to this information, and that by reason of your duties you may receive or have access to verbal, written or electronic media information concerning patients and services performed by the Healthcare System. ***If you have any questions, please ask for clarification.***

Whenever there is any question as to the privileged or confidential nature of any information, or the right of any party to obtain information, the Healthcare System attorney should be consulted.
RL 14244

Page **2** of **3**

This section is to be completed by the PlanLink Site Manager.

The PlanLink Site Manager is the person in charge of maintaining and updating the access to PlanLink for all users within the office/site/group.

If the person requesting access is a physician on staff at Memorial Healthcare, complete this section. Otherwise, leave blank.

To send applications via fax, send to:
Fax number 954-251-4044.

To send applications via email, send to:
ccp.provider@ccpcares.org.

YOUR SIGNATURE ON PAGE THREE INDICATES ACCEPTANCE OF THE FOLLOWING:

User agrees to hold harmless and indemnify MHS, its employees and agents from and against any and all claims damages, expenses and causes of action, including, without limitation, attorney fees at all levels, arising out of, related to, or by reason of any misconduct, negligence, or breach of the terms and conditions of this Enterprise Access Form.

1) **I HEREBY AGREE, I WILL NOT ACCESS ANY COMPUTER OR ELECTRONIC DATA, EXCEPT AS REQUIRED TO PERFORM MY DUTIES AND SUBJECT TO THE ABOVE LIMITATIONS**. I further agree that, except as directed by the Healthcare System or as required by law, I will not at any time disclose or misuse any confidential or privileged information to any unauthorized person, or permit any such person to examine or make copies of any reports or other documents prepared by me, coming into my possession or control, or to which I have access, that concerns in any way the privileged or confidential information of the Healthcare System.

2) **Work Station Security:** Under no circumstances will I give my password to any other individual. I will choose quality passwords, which I will remember. I will not write my password where another individual may find it. I will log out or secure my workstation whenever I leave the workstation, including closing blinds and placing patient identifiable information in a secure area out of plain view. I will not use a workstation that has been logged onto by another user unless I log them out. All information gained by my password will be treated as confidential and never be released to any person or misused unless they have a need to know and I have been authorized to release that information by my supervisor. I understand that I will be held responsible for all computer transactions that occur under my sign-on. I understand that all data from, or on MHS computers and computer systems is legally owned by the Healthcare System. I will not electronically copy or transmit MHS information (patient, financial, etc.) not directly related to my authorized duties without written consent from the authorized source. I understand the need to protect the Healthcare System's assets (its data), and that every individual is responsible for data security. I will report any and all suspected security breaches to the Chief Information Security Officer / Corporate Directory of Privacy. I can also all the Privacy Reporting Number (954) 265-1165 or email mhsprivacy@mhs.net. I understand that if I have been given remote access to the Healthcare System's computer system, I will abide by all of the above conditions.

I RECOGNIZE THAT THE UNAUTHORIZED ACCESS AND/OR DISCLOSURE OF INFORMATION BY ME MAY VIOLATE STATE OR FEDERAL LAWS, AND THAT THE UNAUTHORIZED ACCESS AND/OR RELEASE OF INFORMATION MAY RESULT IN CRIMINAL AND/OR CIVIL LIABILITY, DISMISSAL OR OTHER DISCIPLINARY ACTION BEING TAKEN AGAINST ME.

3) **Security of Healthcare System Information/Equipment:** I agree that I will comply with all security regulations in effect at the Healthcare System. I understand that all software used on a computer owned by the Healthcare System must be properly licensed and approved by the Healthcare System Administration for use on that computer. The use of unlicensed or unapproved software constitutes a serious risk to Healthcare System operations. If I use or allow to be used any unlicensed or unapproved software on a Healthcare System computer, I may be subject to criminal and/or civil liability, dismissal or other disciplinary action. **I acknowledge that an IT Security presentation is available on the MHS intranet site under IT Security, under the section marked, IT Security Presentations. I agree to access and completely review this presentation prior to any other use of MHS computer systems.**

Print Requestor's Full Name: _____

Requestor's Signature:_____ **Date:** _____

RL 14244

The Enterprise System Access form must be submitted to CCP by the designated PlanLink Site Manager and not by individual users.

ID/Login is emailed to the applicant from "MHS IT Service Desk".

The person requesting the access to PlanLink must complete this section.

To send applications via fax, send to:
Fax number 954-251-4044.

To send applications via email, send to:
ccp.provider@ccpcares.org.