

Statement of Confidentiality Policy and Procedure

Policy #:	HCDPRIV224	Effective Date:	01/16/2013
Business Unit:	Home Office-Corporate	Last Review Date:	02/10/2020
Approval Group:	Compliance	Document Owner(s):	Compliance
Board Approval Date:	01/16/2013		

PURPOSE

The purpose of this policy is to protect the confidentiality of all patients, members, residents and the District itself by limiting disclosure of confidential information to those having a need to know in order to perform the duties of their job.

SCOPE

This policy applies to all workforce and committee members of the Health Care District of Palm Beach County and its Affiliated Entities (the "District"), including, Lakeside Medical Center, E.J. Healey Center, Primary Care and Dental Clinics, School Health, Pharmacy, Aeromedical, Trauma and Managed Care that handle protected health information.

DEFINITIONS

Confidential information: includes protected health information maintained or transmitted in any form including verbally, in writing, or in electronic form.

Protected Health Information ("PHI"): 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.

POLICY

The District prohibits the unlawful or unauthorized access, use or disclosure of confidential information obtained during the course of employment or appointment with the District. Every employee, committee member, physician, student, volunteer and contractors affiliated with the District will keep all information concerning patients, members, and residents confidential both during and after service at the District.

EXCEPTIONS

N/A

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

Statement of Confidentiality Policy and Procedure

Procedure #:	HCDPRIV224	Effective Date:	01/16/2013
Business Unit:	Home Office-Corporate	Last Review Date:	02/2020
Approval Group:	Compliance	Document Owner(s):	Compliance

PROCEDURE

1. All District workforce members must sign the Confidentiality and Data Security Agreement contained in this policy indicating acceptance and support of this policy and any department specific policy at their annual review. A copy of the agreement will be maintained on file according to the District's records retention policies.
2. All committee members must sign the Statement of Confidentiality at the beginning of their term and annually thereafter. A copy of the agreement will be maintained on file according to the District's records retention policies.
3. Physicians must sign the Confidentiality and Data Security Agreement during their credentialing process and annually thereafter. A copy will be maintained in the physician's file.
4. Students, residents, volunteers and any applicable vendor must sign the agreement prior to providing services at any District Entity.
5. All workforce members who access confidential information are responsible for taking prudent measures to protect its security by following physical safeguards and employing technical safeguards such as file encryption, selecting and maintaining strong passwords, etc.
6. Any request for disclosure of health information to organizations outside of the District should be referred to and will be handled by the Records Department and the Health Information Management Department of Lakeside Medical Center. Other such disclosures by individuals should never occur.
7. Workforce members should only access or use PHI for legitimate business purposes and must limit access/use of PHI to the least amount of information necessary ("minimum necessary") required to fulfill their assigned duties.
8. Paper copies of PHI must be discarded in accordance with the *Disposal of PHI Policy*.
9. Employees found to have misused or abused their access to PHI are subject to disciplinary action up to and including termination in accordance with the *Performance Management Policy*.
10. To ensure confidentiality in the situations that follow, workforce members are required to adhere to the following:
 - a) Never use privileges or access to PHI or other confidential information (such as claims and referrals) granted to them for personal reasons.
 - b) District workforce members must, at all times, demonstrate trustworthy, honest behaviors and actions in the collection and use of health and other information.
 - c) Workforce members are prohibited from using their own or family members' protected health information or other confidential information to which they have been granted access.

- d) Workforce members who contact patients via telephone or email must ensure that they are familiar with the guidelines for contacting patients and leaving voicemails and/or emails appropriately.

RESPONSIBILITY

It is the responsibility of all workforce members to report any violations of this policy to their supervisor, Human Resources or Compliance Departments. Violations may also be reported to the Chief Compliance and Privacy Officer via the:

1. Compliance Hotline: 1-866-633-7233
2. Compliance Department at (561) 804-5524 ext. 295524
3. Privacy Email at privacy@hcdpbc.org

ENFORCEMENT

Violation of this policy may result in disciplinary action up to and including immediate termination of employment, privileges or contractual rights in accordance with applicable District policies and procedures. Unauthorized use or release of confidential information may also subject the individual to personal, civil, and/or criminal liability and legal penalties.

RELATED DOCUMENTS	
Related Policy Document(s)	
Related Forms	
Reference(s)	Stat. §456.082
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.