	PCHP.PV.105 Safeguarding and Storing Protected Health Information V3 PCHP.PV.105	
CENTRA	Name:	PCHP.PV.105 Safeguarding and Storing Protected Health Information
	ID Number:	PCHP.PV.105
	Approval Date:	10/18/2017 07:26:59 AM
	Approved By:	Garland Morton/CentraNotes

Body

Policy Name: Safeguarding and Storing Protected Health Information

Purpose: To provide guidelines for the safeguarding and storing of Protected Health Information (PHI) and to limit unauthorized disclosures of PHI that is contained in an enrollee's file, while ensuring that PHI is easily accessible to those involved in providing health care benefits to our enrollees.

Definitions & Acronyms:

CMS: Centers for Medicare & Medicaid
CFR: Code of Federal Regulations
PBM: Pharmacy Benefit Manager
HIPAA: Health Insurance Portability and Accountability Act of 1996
HITECH: Health Information Technology for Economic and Clinical Health Act
PHI: Protected Health Information
BA: Business Associate

Piedmont: "Piedmont" collectively refers to Piedmont Community Health Plan (PCHP), Piedmont Community HealthCare (PCHC) and any future entities that are owned, affiliated with and/or operated by Piedmont.

Policy:

1. Piedmont must use reasonable and appropriate administrative, technical, and physical safeguards to protect all PHI from any intentional or unintentional use or disclosure that is in violation of 45 CFR 164 Subpart C. In doing so Piedmont must:

   A. Ensure the confidentiality, integrity, and availability of all PHI the covered entity or BA creates, receives, maintains, or transmits;

   B. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

   C. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required under subpart E of the HIPAA Security and Privacy Rule;

   D. Ensure workforce members only access PHI when there is a legitimate clinical, billing or business reason to do so;

   E. Ensure appropriate controls are in place regarding access to facilities, equipment and software that contain PHI.

   F. Piedmont must establish and implement procedures to allow access in support of restoration of lost data during disaster or emergency.

2. Piedmont must periodically monitor its compliance regarding its reasonable efforts to safeguard PHI.

3. All staff members are responsible for the privacy and security of PHI in and around their workstations.

Procedures:

1. Administrative: administrative safeguards exist to protect electronic use and access of PHI. Piedmont is defined as a "related" entity to Centra, and Piedmont utilizes Centra's IT network and database security. Centra has policies which govern access to the network, systems, device management, password management, etc. Additionally, see policy PCHP.PV.101 which describes the program to implement applicable policies and procedures to protect PHI. The following safeguards are administrative guides for Piedmont employees.

   A. Written PHI. All documents containing PHI should be stored appropriately to reduce the potential for incidental use or disclosure. Documents should not be easily accessible to any unauthorized staff or visitors.

      1). Piedmont employees will protect PHI by:

         i. filing or covering PHI on their desks when they leave each day.

         ii. lock drawers and offices when possible.

   B. Meetings during which PHI is discussed.

      1). Meetings will be conducted in an area that is not easily accessible to unauthorized persons.

      2). Meetings will be conducted in a room with a door that closes, if possible.

      3). Voices will be kept to a moderate level to avoid unauthorized persons from overhearing.

      4). Only staff members who have a "need to know" the information will be present at the meeting.

      5). The PHI that is shared or discussed at the meeting will be limited to the minimum amount necessary to accomplish the purpose of sharing the PHI.

   C. Conversations.

      1). PHI shared in phone or in-person conversations will be limited to the minimum amount necessary to accomplish the purpose of the use or disclosure.

      2). Telephones used for discussing PHI are located in as private an area as possible.

      3). Staff members will take reasonable measures to assure that unauthorized persons do not overhear conversations involving PHI. Reasonable measures may include:

         i. Lowering the voice

         ii. Requesting unauthorized persons move away from the area

         iii. Moving to a more private area before continuing the conversation.

   D. Centra IT Security Administration:

      1). Piedmont relies on Centra's IT Security program for facilitation of disaster recovery and emergency mode operations in the event such a circumstance occurs.

2. Technical: Technical safeguards exist to protect electronic use and access of PHI. Piedmont is defined as a "related" entity to Centra, and Piedmont utilizes Centra's IT network and database security. Centra has policies which govern access to the network, systems, device management, password management, etc.

   In addition to the technical protections Centra has in place, the following statements help expand on the aspects of technical safeguards Piedmont has for access to PHI:

   A. Electronic PHI.

      1). Employees should store all PHI, PII and other data on the network drive unless absolutely necessary to perform your job. If data must be stored on a portable device, that device must be encrypted.

      2). All laptops and portable devices, used to store PHI data, must be encrypted.

      3). Do not store any PHI or employee information on an unencrypted USB or external drive.

   B. Computer Access.

      1). All users of computer equipment must have unique login and passwords.

2). Passwords should be changed every 90 days.

3). Posting, sharing and any other disclosure of passwords and/or access codes is **strongly discouraged**.

4). Access to computer-based PHI shall be limited to staff members who need the information for treatment, payment or health care operations.

5). Staff members shall lock their workstation when leaving the work area.

6). Computer monitors shall be positioned so that unauthorized persons cannot easily view information on the screen.

7). Employees will immediately report any violation of this policy to their Supervisor, Compliance Officer, or Compliance Department.

C. Adding and Removing Access to Computers and ePHI:

1). Employees are required to have their manager/supervisor approval before being granted authority to access systems and files containing PHI.

2). Voluntary termination: Employees voluntarily leaving the company will be allowed access until they leave the building on their last day of work.

3). Involuntary termination: Employees who are involuntarily terminated will have access privileges removed immediately upon their termination notice from their supervisor/manager/HR representative.

D. Printers, copiers and fax machines.

1). Printers, copiers and fax machines will be located in areas not easily accessible to unauthorized persons.

2). Documents containing PHI that must be disposed of due to error in printing will be destroyed by placing the documents in the secure shredding bins until destroyed.

E. Destruction of PHI.

1). When discarding printed materials with PHI, place documents in the locked shredding bins located in each department until the time that it is destroyed.

2). Prior to the disposal of any electronic media or equipment, such as floppies, CDs, hard drives, computers, etc., determine if PHI has been stored in the equipment and delete all PHI prior to disposal (including donation, sale or destruction). When in doubt, contact the Compliance Officer or the IT Department.

3). See "Policy PCHP.PV.109 – Retention and Destruction of PHI" for additional guidance.

3. Physical: Physical safeguards to PHI include the following:

A. Badge Entry: Piedmont has installed a badge entry system to enter the operational areas.

1). All employees are granted a badge on orientation day. Upon termination (voluntary or involuntary), badges will be collected by the employee's supervisor/manager/HR representative.

2). Piedmont has a front desk reception that tracks every visitor. Receptionist will contact necessary Piedmont employee(s) in operational areas to confirm authorized entry of guests. All visitors and guests are required to be escorted while in operational areas.

B. Server Room: Locked doors are installed so that only the IT professionals have access to the server room(s) at Piedmont locations.

C. Centra IT Security Physical:

1). Piedmont relies on Centra's IT Security program to maintain proper security of the physical servers and hardware used to operate the network.

2). If repairs or modifications to the physical components and security are made, Centra maintains records of such repairs.

Equipment: None

Forms and Letters: None

Reference(s): 45 CFR § 164.105(a)(2)(ii), 164 Subpart C; 45 CFR § 164.310 (a)(1) & (a)(2); NCQA Manual – RR4 – Privacy & Confidentiality – Element A & B;

Interdisciplinary Review: None

Policy History:

Date	Revision No.	Reason for Change	Sections Affected
04/14/2003	NEW		All
09/23/2013	1.0	• Updated policy to new format. • Provided more detailed clarification.	All
02/01/2016	1.1	• Converted to Centra format	
07/05/2016	2.0	• Reviewed for compliance with Phase 2 Audit Protocol • Reviewed for compliance with NCQA manual RR4 • Added policy language to clarify requirement • Added procedure language for Administrative, Technical and Physical safeguards	
09/22/2017	3.0	• Reviewed for compliance with HIPAA Audit protocol. • Added sections that correspond to Security rule requirements, 45 CFR 145.310 (a)(1) (a)(2)	Policy & Procedure

Document Link Manager

No Documents Linked No Documents Linked

Attachment Manager

No Attachments