	PCHP HIPAA Privacy and Confidentiality Piedmont Community Health Plan	
CENTRA	Name:	PCHP.PV.132 Sanctions
	ID Number:	PCHP.PV.132
	Start Date:	02/02/2016
	Approval Date:	09/05/2016
	Review Date:	09/05/2017
	Approved By:	Garland Morton/CentraNotes

Body

Policy Name: Sanctions – Privacy

Scope: Entire Piedmont workforce

Purpose: To ensure there are appropriate sanctions that will be applied to employees who violate the requirements of the HIPAA Privacy Rule and/or the Piedmont's HIPAA privacy policies and procedures.

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
DRS: Designated Record Set

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 will impose appropriate sanctions against employees who violate HIPAA or Piedmont's Privacy Policies and Procedures.

2. Piedmont will consider all relevant factors in determining the nature and severity of the sanction, including but not limited to:

   A. The intent of the employee,
   B. The severity of the violation, and
   C. Whether the violation indicated a pattern or practice of improper use or disclosure of Protected Health Information (PHI).

3. Piedmont's Compliance Officer will document all reported incidents and the sanctions that are applied.

Procedures:

1. Piedmont employees must report any violation of the HIPAA rules, regulations, or Piedmont's Privacy Policies and Procedures that they become aware of to his/her Manager or Director, who will report the breach to the Compliance Officer.

   A. Failure to report a breach will result in appropriate disciplinary action.

   B. Reporting a breach in bad faith or for malicious reasons will result in appropriate disciplinary action.

2. The Compliance Officer shall investigate the matter and determine the intent of the individual and severity of the violation. The offenses listed below, while not all-inclusive, are organized according to severity of the violation:

   A. Level I Breach of Privacy: Improper and/or unintentional disclosure of PHI.

   1). This level of breach occurs when an employee unintentionally or carelessly accesses, reviews, or reveals Piedmont member PHI to others without a legitimate need-to-know.

   2). Examples include but are not limited to:

   i. Employees who discuss member PHI in a public area;

   ii. An employee leaves a copy of member PHI in a public area;

   iii. An employee leaves a computer unattended in a public area with member PHI displayed

   B. Level II Breach of Privacy: Unauthorized use and/or misuse of PHI.

   1). This level of breach occurs when an employee intentionally accesses or discloses member PHI in a manner that is inconsistent with Piedmont policies and procedures, but for reasons unrelated to personal gain.

   2). Examples include, but are not limited to:

   i. An employee looks up birth dates, address of friends or relatives;

   ii. An employee accesses and reviews the PHI of a member out of curiosity or concern;

   iii. An employee reviews a public personality's PHI.

   C. Level III Breach of Privacy: Willful and/or intentional disclosure of PHI.

   1). This level of breach occurs when an employee accesses, reviews or discloses PHI for personal gain or with malicious intent.

   2). Examples include, but are not limited to:

   i. An employee reviews member PHI to use information in a personal relationship;

   ii. An employee uses member PHI to compile a mailing list for personal use or to be sold.

3. The Compliance Officer, in conjunction with the employee's manager, Human Resources department, or other appropriate Piedmont management will develop and implement an appropriate plan of corrective action including:

   A. A warning,

   B. Retraining,

   C. Suspension, or

   D. Other disciplinary actions, up to and including termination.

4. Reporting and Filing:

   A. For all levels of breach, the initial report will be logged in the Breach Notification Log and all supporting documentation scanned into the Supporting Documents File by the Compliance Officer and retained for six years.

   B. For all levels of breach beyond Level I, a copy of the report and supporting documentation will also be placed in the Personnel File of the employee.

Equipment: None

Forms and Letters: None

Reference(s): 45 CFR §164.530(e)

Interdisciplinary Review: None

Policy History:

	Revision		

Date	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 and included changes/updates from the HIPAA Omnibus Rule effective 9/23/13.	All
02/02/2016	1.1	• Converted to Centra format	
07/20/2016	2.0	• Reviewed for Compliance with Phase 2 Audit Protocol • Reviewed for Compliance with NCQA Standards 2016	

Document Link Manager

No Documents Linked No Documents Linked

Attachment Manager

No Attachments