POLICY/PROCEDURE: PP-01
Effective date: 04/14/2003
Date(s) of revision: 05/21/2003
12/17/2009; 7/1/2013; 2/1/2016

POLICY REGARDING INVESTIGATIONS OF POSSIBLE BREACHES OF PATIENT CONFIDENTIALITY, DISCIPLINARY SANCTIONS FOR SUCH BREACHES, AND EXTERNAL REPORTING AS REQUIRED BY LAW

Purpose: To set forth the policy and procedures of WVU Physicians of Charleston (WVUPC) regarding the investigation of possible breaches of patient privacy and confidentiality, the disciplinary sanctions for violation of patient privacy and confidentiality, and circumstances in which WVUPC is obligated to provide notifications to individuals and/or the U.S. Department of Health & Human Services of such breaches.

Standard: The faculty and staff of WVUPC will at all times exercise reasonable care and due diligence to protect and preserve patient privacy and confidentiality, and will at all times comply with the policies and procedures of WVUPC as required by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and related amendments. As set forth in WVUPC Privacy Policies, the medical record is a confidential document and must be treated as such by all faculty and staff who have access to the content of such records. All employees of WVUPC must understand that good faith protection and preservation of patient privacy is, at all times, a condition of continuing employment. Any breaches of patient confidentiality by an employee of WVUPC are subject to formal disciplinary action as set forth in this policy.

Policy: A breach of patient confidentiality occurs when any WVUPC employee:

(a) Accesses or reviews patient clinical information for any reason not related to the provision of care and treatment of the patient or for another authorized purpose; or
(b) Discusses with or reveals to any individual(s) clinical information for purposes not related to the care and treatment of the patient or another authorized purpose; or
(c) Otherwise violates the provisions of WVUPC's policies concerning the permissible uses and disclosures of protected health information.

WVUPC will, in cases of confirmed violations of patient confidentiality, apply appropriate disciplinary sanctions against members of its workforce who fail to respect, maintain and/or protect the integrity, confidentiality and security of patient health information, and/or who fail to comply with the organization's privacy and security policies and

procedures as required by law. The type of sanction applied shall vary depending upon the severity of the violation, whether the violation was intentional or unintentional, whether the violation indicates a pattern or practice of improper access, use or disclosure of protected health information, and other similar factors.
Breaches in patient confidentiality have been divided into three levels with the corresponding disciplinary action for each level of breach listed below. All instances of disciplinary action shall be documented in writing and maintained in the employee's personnel record and housed in the Human Resources Department.

1. ***Carelessness****:*

This level of breach occurs when a WVUPC employee unintentionally or carelessly accesses, reviews or reveals patient information to himself/herself or others without a legitimate need to know. Examples include discussion of patient information in public areas, or leaving copies of medical information in public areas

Procedure:

Procedures for investigating this level of breach:

a. The WVUPC Privacy and Security Officers will conduct an appropriate investigation into reported incidents of such breaches of patient confidentiality in an extent and manner commensurate with the level of the breach and the specific facts. The investigation may include, but is not necessarily limited to, interview(s) of the employee accused of the breach, interview(s) of other individuals, and reviews/analysis of relevant documentation.
b. Upon concluding their investigation, the Privacy and Security Officers shall prepare a written report, including their findings and conclusions with regard to the alleged breach, and shall report their findings to Human Resources.
c. Progressive discipline shall be applied by Human Resources as follows:

First Offense: Written Warning
Second Offense: Final Written Warning
Third Offense: Termination

Whenever applicable, discipline levied pursuant to this policy shall be reported as required to applicable professional licensing boards.

2. ***Curiosity or Concern (no personal gain):***

This level of breach occurs when an employee intentionally accesses or discusses patient information for purposes other than the care of the patient or other authorized purposes, but for reasons unrelated to personal gain. Examples include but are not limited to: an employee looks up birth dates, addresses of friends or relatives; an employee accesses and reviews a patient records out of concern or curiosity; or an employee reviews a public personality's record.

Procedures for investigating this level of breach:

a. The WVUPC Privacy and Security Officers will conduct an appropriate investigation into reported incidents of such breaches in an extent and manner commensurate with the level of the breach and the specific facts. The investigation may include, but is not necessarily limited to, interview(s) of the employee(s) accused of the breach, interview(s) of other individuals, and reviews/analysis of relevant documentation.
b. Upon concluding their investigation, the Privacy and Security Officers shall prepare a written report, including their findings and conclusions with regard to the alleged breach, and shall report their findings to Human Resources.

Discipline for this level of breach:

Such offenses will be evaluated on a case-by-case basis with consideration given to the nature of the breach, the amount of material accessed, the motive of the person(s) involved, whether there were disclosures to third parties, etc.

First Offense: Depending on such factors as described above and the severity of the infraction, the first offense shall call either for a Final Written Warning or Termination.

Second Offense, if applicable: Termination

Whenever applicable, discipline levied pursuant to this policy shall be reported as required to applicable professional licensing boards.

3. *Personal Gain or Malice*

This level of breach occurs when an employee accesses, reviews or discusses patient information for personal gain, or with malicious intent. Examples include, but are not limited to, situations in which an employee reviews a patient record to gain and use information in a personal relationship, an employee compiles a mailing list for personal use or to be sold, or an employee obtains information for use in securing credit or to make purchases fraudulently or in violation of the law.

Procedures for investigating this level of breach:

a. The WVUPC Privacy and Security Officers will conduct an appropriate investigation into reported incidents of such breaches in an extent and manner commensurate with the level of the breach and the specific facts. The investigation may include, but is not necessarily limited to, interview(s) of the employee accused of the breach, interview(s) of other individuals, and reviews/analysis of relevant documentation.
b. Upon concluding their investigation, the Privacy and Security Officers shall prepare a written report, including their findings and conclusions with regard to the alleged breach, and shall report their findings to Human Resources.

Discipline for this level of breach:

First Offense: Termination

Whenever applicable, discipline levied pursuant to this policy shall be reported as required to applicable professional licensing boards.

Reporting & Filing Requirements:

For all levels of breach, after final resolution, the initial report of the Privacy and Security Officers, and all related disciplinary documentation, shall be placed in the employee's personnel file.

BREACH NOTIFICATION OBLIGATIONS:

The Privacy and Security Officers shall also ensure that external reports of breaches in patient confidentiality are made as required by law.

1. **There is a presumption that an impermissible use or disclosure of PHI is a breach unless the Covered Entity or business associate demonstrates that there is a "low probability that the protected health information has been compromised." Breach notification is not necessary if a Covered Entity or business associate demonstrates through a documented risk assessment that there is a low probability that the PHI has been compromised.**

2. **Exceptions to notification/reporting**

a. Unintentional good faith acquisition, access or use of PHI by a workforce member;
b. Inadvertent disclosure between two individuals who are otherwise authorized to access the PHI;
c. Disclosure to an unauthorized person who would not reasonably have been able to retain such information.

3. **Risk Assessment**

The required risk assessment to determine the probability of PHI compromise must be thorough, completed in good faith, and must reach conclusions that are reasonable. To meet these requirements, the Covered Entity's risk assessment must consider at least the following:

- The nature and extent of the PHI involved (i.e. the types of identifiers, likelihood of re-identification, and the amount of data and its sensitivity);
- The type of unauthorized person who used the PHI or to whom the data was disclosed;
- Whether the PHI was actually acquired or viewed; and
- The extent to which the risk to the PHI has been mitigated.

4. **Notice must be given, when applicable, to**:

a. The individual whose information was breached
b. HHS, in an annual log (after 9/23/09)
c. If greater than 500 individuals are affected a report must also be provided to prominent media outlets and HHS concurrently.

5. **The Notice must include:**

a. A brief description of what happened, including the date of breach and the date of discovery, if known;
b. A description of the type of information involved or unsecured PHI breached
c. A brief description of what WVUPC is doing to investigate the breach, mitigate the harm to the individuals whose information was breached, and to safeguard against further breach;
d. Any steps individuals should take to protect themselves from the potential harm of the breach; and
e. Contact information, which must include a toll-free telephone number, e-mail address, website or postal address, so that affected individuals can ask questions and obtain additional information.
f. Notice must be given without unreasonable delay, and no later than 60 days following discovery (i.e. when the breach is known or should have been known with reasonable diligence).
g. Notice shall be delayed at the written request of law enforcement officials for the period requested

h. Notice must be given by first class mail, except: e-mail is permitted if the individual has agreed to electronic notice; substitute notice shall be made if specific contact information is not known; if less than 10 individuals, by written notice, telephone or other means; if 10 or more individuals, by conspicuous posting on the corporate website home page for 90 days, or in major print or broadcast media.

Exceptions:

The policy and procedures relating to disciplinary sanctions contained herein do not specifically apply when members of WVUPC's workforce exercise their right to:

a. File a complaint with HHS over alleged privacy violations;
b. Testify, assist or participate in an investigation, compliance review, proceeding, or hearing;
c. Oppose any act made unlawful by the HIPAA privacy rule, provided the individual has a good faith belief that the act opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of protected health information in violation of the HIPAA privacy rule;
d. Disclose protected health information as a whistleblower and the disclosure is to a health oversight agency; public health authority; or an attorney retained by the individual for purposes of determining the individual's legal options with regard to the whistleblower activity; or
e. An employee who is a victim of a crime and discloses protected health information to a law enforcement official, provided that the protected health information is about a suspected perpetrator of the criminal act; and is limited to the information listed in the WVUPC policies regarding disclosures for law enforcement purposes.

References:

HIPAA Privacy Regulations, 65 Fed. Reg. 82562, 82747 (12/28/00)
45 C.F.R. § 164.530; 45 C.F.R. 164.400; 2013 HITECH Omnibus Rule, 78 Fed. Reg. 5,566 (1/25/2013)