

**TITLE: SANCTIONS FOR UNAUTHORIZED ACCESS, USE OR DISCLOSURE OF PROTECTED HEALTH INFORMATION**

**POLICY:**

Columbia University Medical Center will take appropriate corrective action against a member of its workforce that violates Privacy or Information Security. Organizational policies related to applicable city, state, or federal laws or regulations, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

**PURPOSE:**

The purpose of this policy is to describe the sanctions that can be imposed against workforce members that violate policies, procedures and / or a city, state, or federal laws or regulations.

**PROCEDURE:**

**1. Violation of Columbia University Medical Center policies or procedures.**

Failure to comply with the Columbia University Medical Center policies or procedures may result in corrective action.

- a. Sanctions as a result of a violation of an Information Security and / or Privacy policies or procedures shall be imposed consistently across the organization.
- b. Inadvertent violations of HIPAA HITECH requirements may also result in corrective action.
- c. Examples of violations include:
  1. Accessing a patient's medical record for any purpose outside of treatment, payment, or health care operations.
  2. Discussing a patient's PHI in a public area or outside of Columbia University Medical Center or without a legitimate business reason.
  3. Failing to follow established Information Security policies and procedures when accessing, using or disclosing protected health information including failing to logoff from an application or failing to properly secure electronic media that contains PHI or sharing your password
  4. Using a patient's PHI for personal reasons (such as developing a personal relationship with the patient) rather than for legitimate and authorized business reasons.
  5. Copying or compiling PHI with the intent to sell or use the PHI for personal or financial gain.
  6. Mailing a medical record to the wrong address / patient.

**2. Corrective Action**

Determined on a case by case basis, considering the specific circumstances, severity of the violation; and personnel work history:

- a. May be up to and including termination of employment, or of the business relationship as appropriate.
- b. Sanctions that may be imposed include, but are not limited to:
  1. A letter to the employee's personal file;

2. Administrative leave without pay;
  3. Attendance and successful completion of additional training;
  4. Reimbursement of expenses incurred by Columbia University Medical Center to resolve the matter; or
  5. Immediate termination of employment.
3. **Violations of city / state or federal confidentiality laws and regulations**  
Corrective action may also be taken against individuals or entities that violate related city / state or federal laws and regulations.
4. **Duty to report**
5. A workforce member who fails to report either a suspected or actual violation will have violated this policy, and may be subject to corrective action. Any workforce member who observes or become aware of, or suspects a wrongful use or disclosure of PHI maintained by Columbia University Medical Center is required to report his / her suspicion of the wrongful use or disclosure as soon as possible to his / her supervisor or the HIPAA Privacy Officer.
6. **No retaliation for good faith reporting**  
Columbia University Medical Center will not retaliate against a member of its workforce who acts in good faith believing the practice he / she reports is unlawful.

**Definitions.**

***Protected Health Information (PHI)*** means information, including demographic information that may identify the patient, that relates to the past, present or future physical or mental health or condition of an individual, the provision of health care to an individual or the past, present or future payment for the provision of health care to an individual and identifies or could reasonably be used to identify the individual.

***Workforce*** means employees of, volunteers and trainees at, and other persons affiliated with Columbia University Medical Center whose work is under the direct control of Columbia University Medical Center, regardless of whether they are paid by Columbia University Medical Center.

**RESPONSIBILITY:** HIPAA Privacy Officer, Departments, Human Resources

<b>ISSUED:</b>	<b>December 2003</b>
<b>REVIEWED:</b>	<b>October 2007</b>
<b>REVISED:</b>	<b>February 2010</b>
<b>REVISED:</b>	<b>November 2011</b>