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

POLICY:

Columbia University Medical Center will take appropriate corrective action against any 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) and the Health Information Technology for Economic and Clinical Health (HITECH) Act

PURPOSE:

The purpose of this policy is to describe the sanctions that can be imposed against workforce members that violate policies, procedures and / or 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 and/or 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, including education.
      2. Discussing a patient's protected health information (PHI) in a public area inside 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 PHI including but not limited to:
         a. Failing to logoff from an application that contains PHI
         b. Failing to properly secure electronic media that contains PHI
         c. Failing to encrypt PHI on an endpoint device.
         d. Sharing a 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, emailing or faxing a medical record to the wrong address / patient.
      7. Research conducted on human subjects or the collection of research data without HIPAA Privacy approval.
      8. Failure to register an Information System for certification, as defined in the CUMC System Registration and Certification Policy.

2. **Corrective Action**
   Determined on a case by case basis, considering the specific circumstances, severity of the violation; and personnel work history. Sanctions that may be imposed include, but are not limited to:
      1. A letter to the employee's personnel file;
      2. Administrative leave without pay;
      3. Attendance at and successful completion of additional training;

4. Reimbursement of expenses incurred by Columbia University Medical Center to resolve the matter;
5. Fines paid by the department;
6. (Immediate) Termination of employment; or
7. Non-renewal of faculty appointment

3. **Duty to report**
A workforce member who fails to report either a suspected or actual violation may 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 their suspicion of the wrongful use or disclosure as soon as possible to their supervisor or the HIPAA Privacy Officer. Guidance on how to report can be found in the Information Security Incident Procedure.

4. **No retaliation for good faith reporting**
Columbia University Medical Center will not tolerate retaliation against a member of its workforce who acts in good faith to report a practice they believe 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.

Endpoint means any user device, such as a workstation, laptop, PC, Macintosh, tablet (iPad, Galaxy Tablet, etc), smartphone (iPhone, Blackberry, Android, etc.), removable media such as flash drives or external hard drives, and other portable electronic devices that store, access or process data**.**

RESPONSIBILITY:

HIPAA Privacy Officer, Departments, Human Resources, Office of Faculty Affairs, CUMC Information Security Officer

REFERENCES:

CUMC System Registration and Certification Policy
Information Security Incident Procedure
Acceptable Use of IT Resources Policy

REVIEW / REVISION DATE:

ISSUED:	December 2003
REVIEWED:	October 2007
REVISED:	February 2010
REVISED:	November 2011
REVISED:	November 2012

COLUMBIA UNIVERSITY MEDICAL CENTER

Guideline for Sanctioning Violations of Policy on Unauthorized Access, Use or Disclosure of PHI

Incident Finding	No confidential records	PHI	PII (SSN, Credit Card Numbers, Banking Information	Notes - All fines will be based around the severity of the incident. Re-occurring incidents within departments will raise fines. In case of gross negligence as determined by an investigation, any incident could lead to expulsion as a student, non-renewal of faculty position and termination of employment.
Sharing a password	Education	Education	Education - $10,000	
Failure to register an Information System	Education	$10,000	$10,000	Any department with a system found to have PHI/PII during regular Information Security operations that has not been previously registered will be fined.
Discussing identifiable patient information in a public area or outside of CUMC	N/A	Education - $50,000	N/A	
Mailing confidential data to a wrong address or patient	N/A	Education - $50,000	Education - $50,000	
Loss or theft of device with unencrypted confidential data	Education - $25,000	$25,000 - $75,000	$25,000 - $75,000	Unencrypted workstations, laptops or usb/removable drives that are stolen or lost.
Releasing PHI/PII to Internet via website	N/A	$50,000 - $75,000	$50,000 - $75,000	Examples include removing access control on an Internet facing website that contains PHI or PII
Research on human subjects/PHI without HIPAA privacy approval and use of electronic data.	Education - $25,000	$25,000 - $75,000	$25,000 - $75,000	Even if data are de-identified they still need IRB approval
Research with human subjects/PHI without establishing a security certified computing environment	N/A	$25,000 - $75,000	$25,000 - $75,000	To be implemented after the IRB policy update for 2012.
Staff member receives a copyright violation (DMCA notice)	Education - $10,000	$50,000 - Termination/Non-Renewal	$75,000 - Termination/Non-Renewal	Releasing PHI/PII through peer to peer programs is a breach and considered egregious.
Using PHI/PII with malicious intent	NA	Termination/Non-Renewal	Termination/Non-Renewal	Includes copying or compiling PHI with intent to sell or profit in other ways