

TITLE: **MITIGATING EFFECTS OF LOSS OR UNAUTHORIZED
RELEASE OF PROTECTED HEALTH INFORMATION**

POLICY:

Columbia University Medical Center will mitigate, to the extent possible, any harmful effect that is known to Columbia University Medical Center, resulting from a loss of Protected Health Information (PHI) or an improper use or an unauthorized disclosure of PHI made by Columbia University Medical Center.

PURPOSE:

Columbia University Medical Center is committed to safeguard the PHI in its possession and to mitigating any harmful effect resulting from a loss of PHI or an unauthorized use or disclosure of PHI made by Columbia University Medical Center. This Policy describes the procedures for notifying the HIPAA Privacy Officer of a loss of PHI or an unauthorized use or disclosure of PHI.

PROCEDURES:

- 1. Discarding or disposal of documents/items that contain PHI.** Each Department is responsible for defining policies and procedures for the discarding and/or disposal of documents or items that contain PHI to minimize the risk of inadvertent disclosures of PHI to unauthorized individuals or individuals not affiliated with Columbia University Medical Center

- 2. When PHI is lost.**
 - a. If PHI is stolen (i.e., a laptop containing PHI that is stolen from an office or at the airport, PHI in files that are stolen during a burglary, etc.), the Columbia University Medical Center employee who initially discovers the loss or is made aware of the theft by someone outside Columbia University Medical Center is responsible for reporting the incident to Public Safety as soon as possible after learning of the loss.
 - (1) Notification of the Public Safety should be made in addition to any other procedures required by the Department.
 - (2) Public Safety is responsible for notifying the Information Security and/or HIPAA Privacy Officer.
 - (3) If police or other law enforcement authorities are notified of the theft, and they take a report, a copy of the report or the report's Identification Number, if available, should be included with the written report submitted to the HIPAA Privacy Officer.
 - b. If PHI is accidentally lost (i.e., records being carried from one place to another are dropped and some pages blow away, documents are forgotten and get left in a temporary work area, etc.), the Columbia University Medical Center employee who lost or misplaced the documents is responsible for reporting the incident to the HIPAA Privacy Officer as soon as possible after discovering the loss.
 - (1) Notification of the HIPAA Privacy Officer should be made in addition to any other procedures required by the Department.

- 3. Mitigating the effect of a loss or an unauthorized use or disclosure of PHI.**

Upon receipt of a report of loss or an unauthorized use or disclosure of PHI by the HIPAA Privacy Officer and/or his/her designee

 - a. Will review the circumstances surrounding the loss of unauthorized use or disclosure;

- b. Involve others at Columbia University Medical Center as necessary;
- c. Determine the extent to which Columbia University Medical Center can mitigate the effects of any potential harm that might result from the loss or unauthorized use or disclosure; and
- d. Make recommendations to management, review and revise policies and procedures if necessary, and/or take action as appropriate.
- e. Coordinate with the Information Security Officer (ISO) and General Counsel to determine if additional regulatory reports are indicated.

4. Definitions

Protected Health Information is information about a patient, including demographic information that may identify, that relates to the patient's past, present or future physical or mental health or condition, related health care services or payment for health care services.

RESPONSIBILITY: Departments, HIPAA Privacy Officer

REVIEW/REVISION DATE: December 2003

September 2008

September 2012