

TITLE: BREACH NOTIFICATION: UNAUTHORIZED ACCESS, USE OR DISCLOSURE OF INDIVIDUALLY IDENTIFIABLE PATIENT OR OTHER PERSONAL INFORMATION

POLICY:

Columbia University Medical Center provides appropriate notification(s) in the event of an unauthorized acquisition, access, use or disclosure of individually identifiable patient or other personal identifiable information consistent with state and federal regulations.

To establish and consistently use criteria to identify, track and make appropriate notifications in the event of breach of the privacy or security of individually identifiable patient or other personal information. To establish measures to be taken to prepare and respond to a data breach incident including determining

PROCEDURE:

1. Known or suspected incidents involving breach of PHI should be reported to the Office of HIPAA Compliance. The Information Security and Privacy Officer will review all potential breach reports with the Information Security and Privacy Workgroup. In addition, a risk assessment will be documented when indicated. The documentation of a risk assessment includes an evaluation of the potential for financial, reputational, or other harm to the individual, recommended mitigation steps to reduce the potential for harm, and application of the applicable breach notification and reporting requirements.
2. Computerized Data Security Breach of Personal Information:
 - A. Known or suspected incidents involving events where computerized data may have been hacked, stolen, lost or otherwise compromised should be reported to the Information Security Officer for investigation and determination of whether a Computerized Data Security Breach has occurred.
 - B. When Personal Information is believed to have been present in the system/data compromised, the CUMC Office of HIPAA Compliance should be notified. The CUMC IT Security Officer will consult with the Workgroup in the investigation and management of the incident and application of the applicable breach notification and reporting requirements.
3. If consensus is not clear regarding the breach notification and mitigation response required as a result of an incident or if the business leader believes an exception to the recommended response are appropriate, then a final determination will be made by General Counsel.
4. The business unit from which the breach occurred is responsible for any costs of notification and mitigation as determined to be necessary.

Notification

The following will be notified of a breach including 500 or more records containing PHI/IIHI.

- General Counsel
- Public Relations
- Dean of the School
- Other individuals as required

For additional information refer to the Columbia University Administrative Library Policy titled Electronic Data Security Breach Reporting Response.

DEFINITIONS:

- A. Protected Health Information (PHI): is Individually Identifiable Health Information (IIHI) that is transmitted or maintained in any form or medium by a covered entity. IIHI is information collected from an individual that is created or received by a health care provider, employer, plan, or clearinghouse and 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 the individual, or can reasonably be used to identify the individual.
- B. Covered Entity: is a defined term within the Health Insurance Portability and Accountability Act (HIPAA) and includes health care providers, health plans, and health care clearinghouses.
- C. Business Associate: is a defined term within the HIPAA and includes a person or entity that performs or assists in the performance of a function or activity, for or on behalf of a covered entity, which involves the use of disclosure of IIHI.
- D. Personal Information: is an individual's first name or first initial and last name, in combination with any one or more of the following:
1. Social security number;
 2. Drivers license number;
 3. Account number, credit or debit card number, in combination with any required security code, access code or password.

Personal Information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

- E. Computerized Data Security Breach: unauthorized acquisition or control of data that compromises the security, confidentiality, or integrity or unencrypted computerized Personal Information. This includes unauthorized use or disclosure or another individual's Personal Information by a CUMC staff or faculty member who is otherwise authorized to use CUMC information systems within the scope of their job.

RESPONSIBILITY:

Information Security Officer, Privacy Officer & General Counsel and
Departments

ISSUED:

January 2011