I. Introduction

Columbia University is committed to compliance with all applicable federal and state laws and regulations relating to the compromise of Sensitive Data (as such term is defined in the Columbia University Information Security Charter (the “Charter”) http://policylibrary.columbia.edu/information-security-charter). This Policy establishes measures that must be taken to report and respond to a possible breach or compromise of Sensitive Data, including the determination of the Systems affected, whether any Sensitive Data have in fact been compromised, what specific Sensitive Data were compromised and what actions are required for forensic investigation and legal compliance.

The University’s HIPAA Breach Investigation and Reporting Policy supplements this Policy and should be complied with if the possible breach or compromise of Sensitive Data relates to PHI.

Capitalized terms used herein without definition are defined in the Charter.

II. Policy History


III. Policy Text

A. Reporting

Any suspected or confirmed breach or compromise of Sensitive Data must be reported to the appropriate University office as set forth in Section D below in a timely manner in order to mitigate the risk to Information Resources and protect the University’s operations.

B. University Response Team

Upon receipt of such report, the Chief Information Security Officer, the CUIMC Chief Information Security Officer, the HIPAA Privacy Officer and the General Counsel or his or her delegate will convene the University Response Team (“URT”).

The URT consists of representatives of the following units:
The following lists the general responsibilities of the members of the URT:

- The applicable Information Security Office will be responsible for serving as Incident Lead for any actual or suspected compromise of Sensitive Data (other than PHI).
- The Office of HIPAA Compliance will be responsible for serving as Incident Lead for any actual or suspected compromise of PHI.
- The General Counsel is responsible for all legal issues associated with an actual or suspected compromise of Sensitive Data.
- The Office of Public Safety is responsible for all contacts with law enforcement and for non-technical aspects of any investigation.
- The Office of Public Affairs is responsible for all internal and external communications and media relations.
- Human Resources will advise on personnel issues and communications to University staff.
- The affected University department(s) will provide the support required to investigate and respond to the actual or suspected compromise of Sensitive Data.

C. Procedures

Each Information Security Office will establish detailed internal procedures for compliance, external and internal communications, oversight of the investigation and technical support associated with a suspected or actual breach of Sensitive Data.

The specific incident response procedures are set forth in the applicable Information Security and Privacy Incident Procedure and Checklist.

The general steps in a response include the following:

1. Incident Categorization

Incidents will be categorized based on the applicable Information Security Office’s internal procedures. Based on the severity of the incident, an appropriate response action will be taken.
2. Response and Recovery

The URT may call upon any necessary additional offices and resources required to carry out the investigation and remediation of any breach. This expanded URT will be responsible for the investigation of the incident and any technical support required. Incident team members will include representatives of affected Data Owners and any other units responsible for the Information Resources involved.

Any individual responsible for an Information Resource containing Sensitive Data that may have been compromised must take immediate steps to secure that system and preserve it without change.

3. Lessons Learned

After an incident has been resolved, an incident report will be created and distributed to the URT. The URT will then convene to discuss the security controls that failed and establish the steps necessary to prevent or limit the risk of the incident recurring.

D. Contact Information

To report a possible breach of PHI:
Office of HIPAA Compliance
Web: http://www.cumc.columbia.edu/hipaa/
Email: hipaa@columbia.edu
Telephone: 212-305-7315

To report a possible breach of Sensitive Data at CUIMC:
CUIMC IT Information Security Office
Email: security@cumc.columbia.edu
Telephone: 212-305-4357

To report a possible breach of Sensitive Data at any University campus other than CUIMC:
Columbia University Information Technology
Web: http://www.columbia.edu/cuit/support/
Email: security@columbia.edu
Telephone: 212-854-1919

IV. Cross References to Related Policies and Other Documentation

The Information Security Policies and certain additional documentation referred to in this Policy are listed in Appendix A hereto.
Appendix A

Related Policies and Other Documentation

HIPAA Breach Response and Reporting Policy

Information Security and Privacy Incident Procedure + Checklist
[for a copy of this document, contact the applicable Information Security Office]

Information Security Charter
http://policylibrary.columbia.edu/information-security-charter