

TITLE: EPHI10. INFORMATION SECURITY INCIDENT PROCEDURE

POLICY:

CUMC implements an Information Security Incident Procedure to identify and respond to suspected or known information security incidents; to mitigate, to the extent practicable, harmful effects of incidents that are known to the institution; and to document incidents and their outcomes. This policy is an addition to the ***Columbia University Electronic Data Security Breach Reporting and Response policy***.

PURPOSE:

CUMC improves security controls based on recognition of realized security threats in form of information security incidents, and through prompt capture, analysis, and subsequent actions, to reduce short and long term exposure.

APPLICABILITY:

CUMC faculty, staff, students, owners, custodians, and users of EPHI systems

PROCEDURE:

The process for information security incident includes:

- Identify and report an incident
- Validate an incident
- Evaluate the incident for its extent of its threat
- Take actions based on prioritization of assets and processes
- Re-evaluate and repeat actions until threat is controlled
- Inform workforce members and management, as necessary
- Document details, as appropriate
- Initiate long-term actions to reduce likelihood of recurrence, as appropriate.

These steps are expressed in detail below.

1. Workforce members should report a potential information security incident to the appropriate management personnel. The following is a non-exhaustive list of types of incidents, and the proper authority to be informed:

Suspected virus, spyware, trojan, and other intrusions	... report to CUMC Service Desk
Unauthorized access, and violations of workstation use or password policy	... report to CUMC Service Desk

Violations of access to confidential information and/or PHI	... report to manager, or Privacy Office, or Information Security Office
Suspected identity theft	... report to manager, Information Security Office, or Public Safety
Copyright violations (illegal transfer of movies, music, software, etc.)	... report to manager, or CUMC Service Desk
Loss or theft of institutional property containing confidential information and/or PHI	... report to manager, Privacy Office, Information Security Office, or Public Safety
Suspected violations of privacy or information security policies	... report to Privacy Office or Information Security Office

A workforce member may not prohibit or otherwise attempt to hinder or prevent another workforce member from reporting an information security incident.

2. Incidents may also be identified through automated processes such as periodic virus scan, intrusion detection analysis, firewall and other log analysis, and other audit mechanisms.
3. Information security incidents are evaluated for their damage potential, size and reach, and importance. All significant incidents should be reported to the Information Security Office. Individual incidents (such as virus infections) are addressed routinely with follow up actions to disinfect, or re-imaging of devices, as appropriate, as well as discussion with user regarding safe computing practices in **Workstation Use and Security policy** (#EPI5) and **Columbia University Desktop and Laptop Security Policy**.
4. CUMC Service Desk and CUMC Public Safety should investigate if any complaint is related to Protected Health Information, and if affirmative, will inform the Privacy Officer and Information Security Officer for follow up.
5. Significant incidents are addressed by a group of necessary professionals (such as network/operating system/database administrators, security administrators, biomedical engineer, other custodians as needed, etc.) with appropriate communication and discussion. Once collectively confirmed as an information security incident, the Information Security Office guides the follow-up steps. If

an incident has privacy implications for the PHI, the incident handling will include the Privacy Officer for reporting and incident response.

6. The guiding principle of a significant event handling is to isolate a threat and to make the critical assets available while minimizing impact and preventing additional damage. Towards this, the custodians are authorized to take all steps necessary to address the incident. Possible actions include:
 - A. Disconnection from the Internet, and/or further logical break up of networks
 - B. Disconnection of workstations, hosts and devices from the network
 - C. Turning off devices.
 - D. Removal of privileges of certain users or classes of users based on criteria such as location, title, affiliation, etc.
 - E. Any other step as identified towards isolation and remedy of the incident

Custodians are required to restore the integrity of the network and devices, and access privileges once the incident is appropriately addressed.

7. The group is responsible for informing senior management and the affected user community about the impact of the incident, and for providing updates as necessary. Based on this information, the owners of application assets may evaluate the need to invoke emergency mode access procedures in **Information security: Disaster contingency and recovery plan policy** (#EPHI9).
8. A security incident involving PHI is also reported to The University Response Team (URT) as defined in **Columbia University Electronic Data Security Breach Reporting and Response policy** by the Information Security Officer and the Privacy Officer.
9. The incident documentation includes details of the incident, including possible timing of detection and actions, monitoring of the incident handling, affected assets, etc. If necessary, the documentation is used towards sanctions as detailed in the **Sanctions policy**. The Information Security Officer maintains the documentation for a period of no longer than 6 years.
10. The Information Security Office will initiate steps to address the vulnerability which caused the incident with relevant owners and custodians to attempt to prevent recurrence of the problem. Custodians should maintain an incident summary with consequent changes in application procedures, if applicable. Consult Information Security Office for documentation in *Application security documents list: Security metrics*.

POLICY MAINTENANCE:

Information Security Office

REFERENCES:

All information security policies

CU Administrative policies in Computing & Technology

Health Insurance Portability and Accounting Act of 1996, 45 CFR

164.308(a)(6)(i), 164.308(a)(6)(ii)

REVIEW/REVISION DATE:

November 2007