TITLE: PHI10. PRIVACY AND INFORMATION SECURITY INCIDENT PROCEDURE AND BREACH NOTIFICATION POLICY

POLICY:

This policy governs Columbia University Medical Center's (CUMC) response to malicious, suspected, and/or accidental unauthorized acquisition, access, use or disclosure of confidential data, such as Protected Health Information (PHI), Personally Identifiable Information (PII), or the information systems that support these data. This Incident Response Policy and Procedure intends to mitigate, to the extent practicable, harmful effects of incidents that are known to the institution; and to document incidents and their outcomes consistent with state and federal regulations.

This policy is an addition to the ***Columbia University Electronic Data Security Breach Reporting and Response policy***.

PURPOSE:

To establish and consistently use criteria to identify, track and make appropriate notifications, the CUMC ***Information Security Incident Procedure and Breach Notification Policy*** is established to protect the confidentiality, integrity and availability of confidential data and assets. CUMC improves security controls based on recognition of realized privacy and security threats in form of information security incidents, and through prompt capture, analysis, and subsequent actions, to reduce short and long term exposure in the event of a potential breach of privacy and/or security of confidential data.

APPLICABILITY:

Members of the CUMC covered entity (hereby referred to as "workforce members"), such as faculty, staff, students, owners, custodians, and users of confidential data systems, as well as institutionally-owned and personally-owned assets used for CUMC business purposes.

ROLES AND RESPONSIBILITIES:

Workforce members should report a potential privacy or information security incident to the appropriate management personnel (see below). Failure to report a suspected or potential issue may result in sanctions. The following is a non-exhaustive list of types of incidents, and the proper authority to be informed:

POTENTIAL INCIDENT	REPORT TO
Suspected virus, spyware, trojan, and other intrusions	… CUMC Service Desk
Unauthorized access, and violations of workstation use or password policy	… CUMC Service Desk
Violations of access to confidential information and/or PHI	… manager, or Office of HIPAA Compliance, or Information Security Office
Suspected identity theft	… manager, Information Security Office, or Public Safety
Copyright violations (illegal transfer of movies, music, software, etc.)	… manager, or CUMC Service Desk
Loss or theft of institutional property containing confidential information and/or PHI	… manager, Office of HIPAA Compliance, Information Security Office, or Public Safety
Suspected violations of privacy or information security policies	… Office of HIPAA Compliance or Information Security Office
Institutional Review Board (IRB) Compliance Oversight Team (COT) notification of violation of privacy or information security policies	… the Office of HIPAA Compliance or Information Security Office
An event or incident that the workforce member is unsure of where to report to	… the Office of HIPAA Compliance or Information Security Office

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

The CUMC Response Team (CUMCRT) will be made up of the following key designations: The Office for HIPAA Compliance, the CUMC Information Security Office, and the Office of General Counsel. At times the CUMC URT will need to involve other key departments and personnel, such as CUMC Public Safety and Departmental IT custodians (such as network administrators, system administrators and desktop administrators).

PROCEDURES:

Privacy and information security events occur on a frequent basis and thus it is important to prioritize the events received based on the severity of the exposure to the institution and our patients. Events are escalated into full incidents after the

CUMCRT has evaluated their specific criteria. As such, the following process is followed for triaging privacy and information security events and incidents:

GENERAL PROCEDURES

1) Identification and classification of the privacy or information security event or incident as Critical, Non-Critical, or Non-Actionable
    a. The event or incident will be evaluated based on the extent of its threat and the vulnerabilities exploited. Any Critical event or incident will be escalated with the "Incident" designation.
    b. Any incident classified as Critical will involve alerting and escalating to the CUMCRT.
    c. Additional key personnel will be deputized under the authority of the CUMCRT on an as needed basis.

2) Containment of identified events or incidents to reduce exposure.
    a. Non-Critical events and incidents will be handled as part of normal Information Security operational processes.

3) Eradication of the identified event or incident in order to remove the original vulnerability or flaw.

4) Recovery of the identified event or incident to bring the business process or IT asset back online and in a functional state.

5) Incident documentation and management follow up which can include any of the following:
    a. Formal documentation of the Incident
    b. Informing senior management of Incident details
    c. Education of workforce members
    d. Sanctions to workforce members and/or departments
    e. Initiation of long-term corrective actions to reduce the likelihood of recurrence, as appropriate.

SPECIFIC PROCEDURES

These steps are expressed in detail below.

1. The detailed procedure for classifying an incident as Critical, Non-Critical or Not-Actionable will be maintained by either the Office for HIPAA Compliance and/or the CUMC Information Security Office

2. Critical incidents will be escalated to the CUMCRT whereby a formal Incident Response procedure will be followed, which is inclusive of the following elements:

a. Interviews of affected data/system owners or custodians
b. Forensics conducted to determine full impact of data exposed / assets affected.
c. In the case of an Incident involving PHI, a Risk Assessment useing HITECH criteria for the determination of the Incident's impact.
    i. 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.
d. Risk assessment of the Incident under investigation
e. Full report submitted to senior management with applicable risk assessment to determine Incident severity
f. Breach reporting and notification, where necessary
    i. 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.
g. Sanctions will be applied, as necessary
h. CUMCRT may coordinate with the CU URT, given the circumstances of the incident, as defined in ***Columbia University Electronic Data Security Breach Reporting and Response policy***.
i. 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).

3. Incidents classified as Non-Critical or Not-Actionable will be processed by internal processes and procedures by the Information Security Office and/or the Office for HIPAA Compliance. Typically these events or incidents are identified through automated processes such as:
    a. periodic virus scan,
    b. intrusion detection analysis,
    c. firewall and other log analysis,
    d. other audit mechanisms, and
    e. reports received from workforce members or patients

4. Information security incidents are evaluated for their damage potential, size and reach, and importance. Non-Critical or Not-Actionable 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 (#EPHI5) and ***Columbia University Desktop and Laptop Security Policy***.

5. CUMC Service Desk and Public Safety will notify the HIPAA Privacy Officer and CUMC Information Security Officer for follow-up if they receive a report of an incident which is related to confidential data

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 CUMC Information Security Office and Office of HIPAA Compliance will review all potential breach reports with the *Information Security and Privacy Workgroup*.

8. 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.

SPECIAL PRIVISIONS:

Any personally-owned endpoints used for business purposes, such as laptops, desktops, smartphones, tablets, wireless devices or other electronic mediums which are used to store or access confidential data, may be subject to risk mitigating procedures, such as a remote secure wipe of electronic storage mechanisms, device seizure or retention. .

DEFINITIONS:

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 access, use or disclosure of PHI.

Computerized Data Security Breach: unauthorized acquisition or control of data that compromises the security, confidentiality, or integrity or unencrypted computerized confidential data. 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.

Confidential Data: Any data as described by the ***Columbia University Data Classification Policy*** that has a rating of Highest Sensitivity. This is inclusive of PHI and PII.

Covered Entity: A defined term within the Health Insurance Portability and Accountability Act (HIPAA) and includes health care providers, health plans, and health care clearinghouses.

CU URT: Standing committee at Morningside. Definition for this group of individuals can be found in the ***Columbia University Electronic Data Security Breach Reporting and Response Policy*.**

CUMCRT: Standing committee at the Medical Center that is charged with the protection of PHI within the covered entity and is made up of Information Security Office, Office of HIPAA Compliance, and General Counsel. This committee can deputize additional members on an as needed basis, depending on the severity of the Incident.

Event: A suspicious, or otherwise notable occurrence that warrants further investigation in order to determine the severity of the potential threat and/or vulnerability. Events are common occurrences, such as a suspicious log entry in a firewall, and can ultimately be classified as an Incident by the CUMCRT, the Office for HIPAA Compliance or the CUMC Information Security Office.

Incident: An event that has been deemed by the CUMCRT, or other organizational policies and procedures, to be a breach of the CUMC's Privacy and Security policies.

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.

Personally Identifiable Information (PII): As defined in the ***Columbia University Data Classification Policy Appendix B*** any information about an individual that could cause harm to such individual, such as medical, financial, employment or criminal records or other information, together with information that can be used to identify or trace an individual's identity, including any other personal information that is linked or linkable to that individual. Below is a non-exhaustive list of such information:

1. Credit card numbers
2. SSN
3. Driver license
4. Passwords
5. Student records
6. Prospective student info
7. Personnel record
8. Donor or prospect info
9. Financial info
10. Research materials
11. Contract
12. Confidential agreements
13. Other data not listed here but identified within HIPAA, GLBA, FERPA, PCI DSS or other privacy acts, regulations, laws.

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

POLICY MAINTENANCE:

Office of HIPAA Compliance
CUMC 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
January 2013
April 2013