
TITLE: **INFORMATION SECURITY INCIDENT PROCEDURE**

POLICY:

An Information Security Incident Procedure is implemented to identify and respond to suspected or known information security incidents; to mitigate, to the extent practicable, harmful effects of incidents; and to document incidents and their outcomes.

PURPOSE:

Improve security controls by recognizing and addressing security threats.

APPLICABILITY:

Hospital staff, employees, affiliates, owners, custodians, and users of information systems

PROCEDURE:

1. The process for information security incident includes:

   A. Identify and immediately report an incident
   B. Validate an incident
   C. Evaluate the incident for extent of its threat
   D. Take actions based on prioritization of assets and processes
   E. Re-evaluate and repeat actions until threat is controlled
   F. Inform workforce members and management, as necessary
   G. Document details, as appropriate
   H. Initiate long-term actions as appropriate to reduce likelihood of recurrence.
   I. Report to regulatory agencies, as needed.

   These steps are explained in detail below.

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

Suspected virus, phishing, spyware, bot, and other intrusions	… report to IT Service Desk
Unauthorized access, and violations of workstation use or password policy	… report to IT Service Desk
Violations of access to sensitive data (including PHI and PII)	… report to manager, or Privacy Office, or Information Security Office
Suspected identity theft	… report to manager, or IT Service Desk, or Compliance Office
Copyright violations (illegal transfer of movies, music, software, etc.)	… report to manager, or IT Service Desk, or Compliance Office
Loss or theft of institutional property containing sensitive data (including PHI and PII)	… report to manager, or Physical Security Office, or Compliance Office
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, prevent or retaliate against another workforce member from reporting an information security incident.

3. Incidents may be identified through automated processes such as periodic virus scan, data leakage detection, intrusion detection analysis, firewall and other log analysis, and other audit mechanisms.

4. Information security incidents are evaluated for their harm 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 a discussion with user regarding safe computing practices in ***Workstation Use and Security policy*** (# I230).

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, 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 clinical assets available while minimizing impact and preventing additional harm. 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 wired and wireless network
   C. Turning off devices
   D. Removing privileges of certain users or classes of users based on criteria such as location, title, affiliation, etc.
   E. Taking any other step necessary to isolate and remedy the incident

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

7. The group constituted in Step 5 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*** (# I250).

8. The group constituted in Step 5 collects documentation, and evidence, related to the incidents. The documentation includes details of the incident, including possible timing of detection, monitoring of the incident handling, affected assets, etc. Documentation will be considered in applying the ***Corrective Action to Deter and Sanction Breaches of Protected Health Information (PHI) policy*** (#C140). If an incident is declared to be a breach, regulatory reporting must adhere to the NYP HITECH reporting procedures.

9. The Information Security Office will initiate steps to address the vulnerability that caused the incident with relevant owners and custodians to attempt to prevent recurrence of the problem.

RESPONSIBILITY:

Information Security Office
Privacy Office
Compliance Office

REFERENCES:

All information security policies
Health Insurance Portability and Accountability Act of 1996, 45 CFR 164.308(a)(6)(i), 164.308(a)(6)(ii)
Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, 45 CFR 160, 164

REVIEW/REVISION DATE:

March 2005
June 2009
June 2011
Revised: June 2013; **March 2015**