North Shore–LIJ Health System, Inc.

POLICY TITLE: **Computer Security Response & Management Policy** **Previously Titled:** **Security Incident Management Policy**	**ADMINISTRATIVE POLICY AND PROCEDURE MANUAL**
POLICY #: 900.19	**CATEGORY: Information Services**
System Approval Date: 1/23/14 **Site Implementation Date:**	**Effective Date: 11/18/10** **Last Revised/Reviewed:**
Prepared by: **Office of the CIO–IS Policy and Procedure Committee**	**Superseded Policy(s)/#** **n/a**

GENERAL STATEMENT of PURPOSE

It is the policy of the Health System to manage and respond to any computer security incidents as needed to support the confidentiality, integrity and availability of all services and resources provided.

The Computer Security Incident Response Team (CSIRT) reviews and monitors security related events on an on-going basis and takes immediate action if needed to prevent or stop misuse or failures.

POLICY

It is the policy of the Health System to identify and respond to security-related incidents such as computer viruses, unauthorized user activity, and serious software vulnerabilities in a timely manner. Where required, investigations to resolve security-incidents will be performed by authorized personnel.

SCOPE

This policy applies to all members of the North Shore–LIJ Health System workforce including, but not limited to, employees, medical staff, volunteers, students, physician office staff, and other persons performing work for or at North Shore–LIJ Health System.

DEFINITIONS

Computer Security Incident: any adverse event whereby some aspect of computer security is threatened, such as actual or attempted breach of data confidentiality, disruption of data or system integrity, and disruption or loss of availability. Examples include:

- Compromise of integrity, such as when a virus affects a system or when serious system vulnerability is discovered.

- Denial of Service, such as when an attacker has disabled a system or a network worm has saturated network bandwidth.
- Misuse, such as unauthorized access of information systems or computerized data.
- Damage, such as when a virus destroys data.
- Theft or loss of *Sensitive or Highly Sensitive* data, whether on paper or electronic media
- Intrusions, such as when an intruder penetrates system security.

Computer Security Incident Response Team (CSIRT): a team consisting of qualified staff to investigate and report on a computer security incident. The CSIRT may include different members depending on the nature and severity of the reported incident.

Protected Health Information (PHI): Any oral, written, or electronic individually identifiable health information collected or stored by a facility. Individually identifiable health information includes demographic information and any information that relates to the past, present, or future physical or mental condition of an individual. The *Health Insurance Portability and Accountability Act* (HIPAA) details eighteen items that render PHI identifiable.

1. Names
2. Geographic subdivisions smaller than a state, including street address, city, county, precinct, Zip code, and their equivalent geocodes, except for the initial three digits of a Zip code in certain situations
3. All elements of date (except year) for dates directly related to an individual, including birth date, discharge date, date of death; and all ages over 89 and all elements of dates indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
4. Telephone numbers
5. Fax numbers
6. Electronic mail addresses
7. Social Security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers
13. Medical device identifiers
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code

PROCEDURE/GUIDELINES

The Health System uses the following communication methods for receiving possible security alerts or incidents on a timely basis.

- Network security alerts
- OCIO Security Hotline
- IS Help Desk receiving calls from constituents
- Vendor notification of critical patches and vulnerabilities
- Internal communications
- Security incident and event monitoring
- Calls/Emails to HRIT and/or the HRIT Security email box

OCIO Security provides security tips to the workforce via HealthPort to inform them of these communication methods used for reporting potential security incidents.

A. Security-Related Incident Handling and Event Handling Methodology

OCIO Security is responsible for the management of computer security incidents, and will assemble the CSIRT, work with Information Services, and, as needed, Office of Legal Affairs, Corporate Compliance, Internal Audit, Corporate Security, business leaders, HRIT and HR to resolve security incidents and, where necessary, initiate investigations. *Refer to Policy #900.07 OCIO IS Investigation Support Services Policy.*

- Security incidents affecting non-critical systems are handled at the OCIO Security Manager's discretion based on the criticality of the incident.
- OCIO Security monitors key IT Security information on a 24x7 basis. Items of interest are sent to the Security Operations Center and reviewed. Items of concern are escalated to an on call OCIO Security analyst for immediate review.
- When the security-related incident involves patient or employee information (such as member specific health information), OCIO Security will work with Corporate Compliance, the Office of Legal Affairs and appropriate business leaders to determine the Health System's security breach notification requirements and communication methods, in accordance with *Policy #800.17 HIPAA and State Privacy Breach Notifications.*

B. Monitoring and Reporting

The Health System logs network activity for monitoring and reporting on security related activity. The level of monitoring is based on the level of risk with the access control deviation. Logs must be designed to allow monitoring and reporting on transaction activity and the state of systems for an appropriate period of time.

Reporting is based on the security incident being assessed and information being provided to OCIO Security and appropriate Health System leaders. The list below provides some guidelines as to what information should be collected for incident reporting, if available.

- Name and business area of individual reporting the incident where applicable.
- Date and time that the incident was discovered.
- Type of incident (for example, Denial of Services (DOS) virus, unauthorized access by internal or external individual, or malicious code).
- Date and time incident occurred.
- Current status of incident.

- Source and/or cause of incident, including hostnames and IP addresses.
- Description of the incident (such as how it was detected, what occurred).
- Description of affected resources (for example, network, host, applications, data), including systems' hostnames and IP addresses.
- Estimated technical impact of the incident (for example, data deleted, system crashed, or application unavailable).
- Level of PHI disclosed where applicable, and information regarding parties involved in this disclosure.
- Response actions performed (for example, shut off host or disconnected host from network).

ENFORCEMENT

Users should report any violations of this policy immediately to his or her manager. If appropriate, the violation should be escalated and reported to the IS Help Desk or the Office of Corporate Compliance Help Line. Anyone found in violation of this policy may be subject to disciplinary action, up to and including termination of employment or engagement, as applicable, in consultation with Human Resources.

CONTACT INFORMATION

What	**Where**
NS-LIJHS Help Desk	(516) (718) (631) 470-7272
NS-LIJHS Help Desk Email	servicedesk@nshs.edu
OCIO Security Email	security2@nshs.edu
Office of Corporate Compliance Help Line	(800) 894-3226
Office of Corporate Compliance Website	www.northshore-lij.ethicspoint.com

REFERENCES to REGULATIONS and/or OTHER RELATED POLICIES

- 800.17 HIPAA and State Privacy Breach Notifications Policy
- 8.14 Investigation Service Procedure
- 900.07 OCIO IS Investigation Support Services Policy
- Human Resources Part XII-1 Termination of Employment: Voluntary, Involuntary
- Health Insurance Portability and Accountability Act, 45 CFR Parts 160 and 164
- Health Information Technology for Economic and Clinical Health (HITECH) Act
- Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA) Pub. L. No. 111-5 (February 17, 2009)

CLINICAL REFERENCES

None

FORMS

None

APPROVAL	
System P&P Committee	11/09/10; 12/19/13
System PICG/Clinical Operations Committee	11/18/10; 1/23/14

Versioning History:
11/18/10