North Shore–LIJ Health System, Inc.

POLICY TITLE: **OCIO IS Investigation Support Services Policy**	**ADMINISTRATIVE POLICY AND PROCEDURE MANUAL**
POLICY #: 900.07	**CATEGORY: Information Services**
System Approval Date: 1/23/14 **Site Implementation Date:**	**Effective Date: 1/09** **Last Revised/Reviewed: 3/11**
Prepared by: **Office of the CIO-IS Policy and Procedure Committee**	**Superseded Policy(s)/#:** **900.22 Data Loss Response**

GENERAL STATEMENT of PURPOSE

It is the policy of the health system to conduct OCIO security investigations and forensics, as needed, to support the confidentiality, integrity and availability of all services and resources provided. The health system also promotes consistent organizational behavior by evaluating activities concerning dignity at work, ethical or other work-related misconduct as needed, as well as handling potential data loss.

POLICY

It is the policy of the Health System to provide Computer Security Investigation Services. The policy identifies circumstances in which an investigation will be necessary, the steps which should be taken, and the rights of custodians during the process, and potential outcomes.

DEFINITIONS

ESI: Electronically stored information is any data that is stored in an electronic form and may be subject to production under common electronic discovery rules. This type of data has historically included email and user created documents.

eDiscovery: Electronic discovery of ESI is identified as potentially relevant by attorneys and placed on legal hold. This data is subject to rules and agreed-upon processes, and is often reviewed for privilege and relevance before being turned over to opposing counsel.

Computer Forensic: Computer forensic procedure is a collection, preservation, and analysis that pertains to ESI found in computers and digital storage media related to a custodian's misuse, misconduct, misbehavior and/or criminal activities.

Custodian: Employee who is under investigation.

AARC: Authorized Approvers and Requestors Committee

Data Loss: a breach in the confidentiality, availability or integrity of any data or system. Examples include:

- Erasure or deletion of records or files in media.

- Data or file corruption.
- Media failure.

Data Breach: the real or potential exposure of Sensitive or Highly Sensitive data, such as PHI or PII to the public. This policy addresses the technical unavailability of system data and does not address data breach procedures**.** For information regarding steps to be taken in the event of a data breach, refer to *Policy 900.19 Computer Security Response & Management Policy.*

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

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.

PROCEDURES/GUIDELINES

1. Investigation

a. Submission

i. All investigations requests must submitted by an authorized approver.

ii. A non-authorized approver must submit their request through the Authorized Approvers and Requestors Committee (AARC).

iii. Investigations of non-Health System employees (such as voluntary medical staff, vendors and consultants) are initiated by the Health System sponsoring owner of the entity. The Investigation requestor must submit their request to a representative of the AARC for approval. After the approval is authorized, the authorized requestor (AARC member) will send the request to OCIO Investigations.

iv. Investigation requests should ***never*** be submitted to the IS Help Desk to maintain privacy and confidentiality. If a request is submitted, the IS Help Desk must immediately notify OCIO Security Director or designee.

b. Approval

All investigation must be approved by the authorized approvers; all authorized approvers and requestors can submit an investigation request.

The committee consists of *select* team members from the following departments.

- Corporate Compliance
- Corporate Security
- Human Resources
- Information Services
- Internal Audit
- Office of Legal Affairs
- Risk Management

c. Acknowledgement and Processing

In today's legal and technological landscape, the comprehensive and scalable solution for effectively managing electronically stored documents in litigation, arbitration, and internal or regulatory investigations significantly reduces the risk and cost. A portfolio that spans an investigation life-cycle to identification, preservation/collection, processing and production is essential for any Health System investigation.

OCIO Security conducts two types of investigations: **Computer Forensic** and **eDiscovery**. Computer forensics process involves identifying, preserving, collecting, analyzing, and reporting on digital information (both the *visible* and the *invisible* information on a computer that comprise deleted files, unallocated space, slack space,

hidden files, and encrypted files). eDiscovery is the process of identifying, preserving, collecting, processing, reviewing, and analyzing ESI in litigation.

All information gathered is considered confidential and may only be discussed with the team member(s) directly involved, if necessary. The requestor is responsible for the safe-keeping (for future reference) and proper disposal of the investigation results after completion of the investigation.

Sources that may be investigated but not limited to include the following:

- Email
- Workstation (desktop/laptop)
- File Shares (Home Share & Department Share)
- Mobile phone and desk phone logs
- Custodian auditing (Internet usage, Instant Messaging, Web browsing, logon/logoff activities)
- Printing
- EMR
- PeopleSoft
- Security Events

d. Delivery of Results

To retain confidentiality, the investigators will only communicate, share details, and deliver results to the requestor or authorized personnel.

2. **Data Loss Handling Methodology**

In addition to maintaining the confidentiality and integrity of Health System data, OCIO Security is responsible for its continued availability.

1. Immediately upon identifying that expected critical data is not available, notification must be made to OCIO Security via the IS Help Desk.
2. OCIO Security will document all information related to the incident.
3. When the lost data involves Sensitive or Highly Sensitive data, such as PHI, financial information or other data covered by federal or state regulations, OCIO Security will work with the Corporate Compliance, Office of Legal Affairs, and Risk Management Departments, and the appropriate business leaders, to determine if the incident meets the Health System's security breach notification requirements in accordance with *Policy 800.17 HIPAA and State Privacy Breach Notifications*, or any other regulatory requirements.
4. Root cause analysis will be performed identifying the cause of the data loss, as well as proposed preventive measures to minimize the likelihood of future incidents.
5. OCIO Security will submit a final report to the Chief Technology Officer (CTO), Chief Information Officer (CIO), Director of OCIO Security, and appropriate department managers.

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
OCIO Investigations	OCIOinvestigations@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

- 8.14 IS Investigation Support Service Procedure
- 800.17 HIPAA and State Privacy Breach Notifications Policy
- 900.12 Data Classification Policy
- 900.19 Computer Security Response & Management Policy
- Human Resources Part XII-1 Termination of Employment: Voluntary, Involuntary
- Human Resources Policy Part V-3 Conduct in the Workplace/Progressive Discipline
- 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	1/13/09; 7/14/09; 3/8/11; 12/19/13
System PICG/Clinical Operations Committee	1/29/09; 7/23/09; 3/24/11; 1/23/14

Versioning History:
1/09
7/09
3/11