North Shore–LIJ Health System, Inc.

POLICY TITLE: **Information System Review and Audit Controls Policy**	**ADMINISTRATIVE POLICY AND PROCEDURE MANUAL**
POLICY #: 900.27	**CATEGORY: Information Services**
System Approval Date: 1/15/2015 **Site Implementation Date:**	**Effective Date: 10/25/12** **Last Revised/Reviewed:11/14**
Prepared by: Office of the CIO-IS Policy and Procedure Committee	**Superseded Policy(s)/#:** **N/A**

GENERAL STATEMENT of PURPOSE

North Shore-LIJ Health System (Health System) will maintain a comprehensive internal security control and audit program, and established procedures and record keeping activities to ensure proper legal, ethical and business practices.

POLICY

This program will complement the user authentication process and acts as a deterrent to internal abuse by making users aware that audit trails, access reports, and security incident tracking reports are produced, reviewed and, where applicable, investigated. These internal security controls may take various forms including regular information system activity review. These reviews incorporate logon monitoring, audit trails and logs, access reports, and manually produced security incident tracking reports for network and ePHI systems.

SCOPE

This policy applies to faculty and students of the North Shore-LIJ School of Medicine conducting research on behalf of the School of Medicine or at any North Shore-LIJ Health System facility and 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

Electronic Protected Health Information (ePHI): Any electronic Protected Health Information that is created, received, maintained, stored or transmitted by the health system via electronic digital or computerized systems.

Information Systems: Commercial applications that support the clinical, financial, or other documentation and care for patients. These systems typically store and process ePHI and may interface with other systems such as EHRs. Examples of information systems include laboratory information systems, radiology information systems, pharmacy systems, patient registration and scheduling systems, and billing systems. EHRs are also information systems.

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

Personally Identifiable Information (PII): Any information which can be used to track back to an individual. PII is therefore any information which can be used to identify an individual, whether directly or indirectly. The key test of PII is whether the data reveals a clearly identifiable person. Typical examples of PII include Social Security numbers, full names, credit card information, bank account numbers, phone numbers, and addresses.

Suspicious Activity: System activity which includes, but is not limited to, the following:

- More than 10 unsuccessful logon attempts within 10 minutes
- Multiple simultaneous logon sessions from different locations (IP addresses)
- Printing more than 10 records in 10 minutes

- Accessing records that are flagged as VIP

PROCEDURE/GUIDELINES

A. General

The HIPAA Security Rule (45 CFR Part 160) on Audit Controls (§ 164.312(b)) states that covered entities must, where reasonable and appropriate, "implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information." Although this is an addressable safeguard, if logging functionality is not available, or not technically or operationally feasible, other equivalent alternative measures must be implemented and documented. Proper controls must be implemented to safeguard ePHI wherever it resides including test and development environments.

B. Logging for Information Systems

Information Systems that create, store, process, or transmit confidential information such as PHI or PII may have various levels of logging capability. Minimally, Information Systems capable of generating audit logs must record the following system details:

- Date/time stamp of activity
- User ID
- Device location (for example, IP address or workstation ID)
- Type of activity (for example, successful and failed log on attempts, viewing or updating a patient's record, and printing)

Audit logs should be configured to record as many events and as much detail as reasonable above and beyond the preceding minimum requirements, taking into account system performance and storage requirements. If further guidance is needed, contact OCIO Security.

If an EHR, Information System or application cannot meet the minimum logging requirements, an exception must be approved by the Chief Information Officer and Business Unit Leadership (such as an Executive Director or his or her designee) and documented.

The audit log should capture enough data for the purpose of supporting a security incident investigation. Preserve the audit logs in accordance with the Records Retention and Destruction policy (100.97).

C. Monitoring of System Activity

The Health System will regularly review records of information system activity, including generating and reviewing, without limitation, audit logs, access reports, failed logon attempts and security incident reports in accordance with the standard S900.27.01 "Auditing Applications with Confidential Information." Monitoring of system activity may be

performed by Information Services, Corporate Compliance, or a local administrator or software vendor, where appropriate (e.g. a software vendor or Practice Manager may be responsible for monitoring the activity on an EHR at a Medical Group Practice). This review promotes individual workforce member accountability and gives the Health System the ability to reconstruct significant events or examine suspicious activities as necessary.

The Office of the Chief Information Officer (OCIO) has designated individuals responsible for conducting the review of network activity logs and correlating activity entries on a regular basis. Persons designated to review information system activity, including generating and reviewing audit logs and other security incident reports referenced above, shall document their review and findings. Suspicious activity will be escalated, as applicable, and researched by the Health System OCIO Security Group for possible incident and direct remediation to the appropriate area.

D. Audit Procedures

The Office of Corporate Compliance HIPAA Privacy and Security Officer will approve audit control procedures, which may include logging of certain systems and applications, information to be logged for each system, and review of audit logs and activity reports. The level and type of auditing mechanisms implemented by the Health System will be driven by the Health System's Risk Analysis process.

E. Workforce Accountability

The Health System will educate its applicable workforce members on the specific audit procedures and requirements as necessary. This includes incorporating the concept of audit trail and individual user accountability.

F. Record Storage Requirements

Audit trails, access reports, and automated security incident reports will be retained in a secure manner, taking into consideration system capability, space issues, modality and applicable record retention requirements (Policy 100.97).

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	516-465-8097
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

100.97 Records Retention and Destruction Policy
900.12 Data Classification Policy
S900.27.01 Auditing Applications with Confidential Information Standard
HIPAA Security Rule (45 CFR Part 160) on Audit Controls (§ 164.312(b))

CLINICAL REFERENCES

N/A

FORMS

N/A

APPROVAL	
System P&P Committee	Provisional Approval 10/25/12; Final Approval 11/29/12; 12/18/14
System PICG Committee/Clinical Operations Committee	12/13/12; 1/15/15

Versioning History: