North Shore–LIJ Health System, Inc.

POLICY TITLE: **OCIO Security Awareness and Training Program**	**ADMINISTRATIVE POLICY AND PROCEDURE MANUAL**
POLICY #: 900.20	**CATEGORY: Information Services**
System Approval Date: 4/17/14 **Site Implementation Date:**	**Effective Date: 4/17/14** **Last Revised/Reviewed: NEW**
Prepared by: Office of the CIO– **IS Policy & Procedure Committee**	**Superseded Policy(s)/#:** **n/a**

GENERAL STATEMENT of PURPOSE

This document establishes the uniform policy for the OCIO Security Awareness and Training Program. This policy also establishes minimum standards for mandatory periodic training in OCIO security user awareness including accepted computer security practices of all users. Our goal is to help individuals understand the risks in using today's technology and how to effectively defend against today's cyber threats, and how to protect confidential information.

POLICY

The Health System shall develop and implement an OCIO Security Awareness and Training Program as required by relevant laws and regulations, to help maintain the security of confidential data.

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

Protected Health Information (PHI) is defined as 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.

- Names
- 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

- 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
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social Security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers
- Medical Device Identifiers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable images
- Any other unique identifying number, characteristic, or code

PROCEDURE/GUIDELINES

The OCIO Security Awareness and Training Program ("Program") provides the necessary and relevant skills to maintain the security of confidential data, and is applicable to all members of the workforce (including management). Training and awareness aim to change behavior and culture. The content of this program will include topics delivered to general audiences, and where appropriate, to users with specific roles. The Program may be presented using different media, such as videos, intranet, Web sites, articles in internal publications, screensavers, posters, the *Computer Security Tips* website on HealthPort, and our *Security Sense* online newsletter.

Mandatory training is managed as a part of the Corporate Compliance training program. Other training may be done by OCIO Security, Corporate Compliance, or in partnership with each other.

1. Training Program

New Hire (On boarding) Training

All newly hired personnel must receive information security training during their new-hire orientation where they will be issued a copy of the *900.00 Computer Use Policy*.

Role-based Training

Specialized, role-based training tailored to each user's role or department specific shall be provided. An example of such a group of users is IT Staff (OCIO, system owners, security analysts, system administrator, Help Desk personnel, and network

administrator). Business Unit leadership working with Corporate Compliance and OCIO Security are responsible to determine if specialized training is warranted. All personnel will be required to take this program annually.

Training completion will be maintained in the personnel files, as part of the permanent record.

2. Awareness Program

Awareness is less formal than training and is intended to reinforce common security concepts, issues, and risks. The Awareness Program will provide periodic security updates and reminders. All members of the workforce, including management, must be included in this program.

Content

The Health System provides security awareness training for members of the workforce, which may include, but is not limited to, the following content.

- Maintaining PHI confidentiality including encryption of data when appropriate;
- Acceptable computer, Internet, and email usage including secure mobile and remote computing;
- Procedures for creating, changing, and safeguarding passwords including user account confidentiality; and
- Sanction process for non-compliance with policies.

3. Roles and Responsibilities

All employees must:

- Implement and act in accordance with the organization's information security policies.
- Protect assets from unauthorized access, disclosure, modification, destruction or interference.
- Must ensure responsibility is assigned to the individual for actions taken.

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

- Human Resources Part XII-1 Termination of Employment: Voluntary, Involuntary
- Health Insurance Portability and Accountability Act, 45 CFR Parts 160 and 164
- NIST SP 800-50, Building an Information Technology Security Awareness and Training Program.
- HITRUST Alliance Common Security Framework (2012)
- 900.00 Computer Use Policy

CLINICAL REFERENCES

None

Forms
None

APPROVAL

System P&P Committee	2/27/14
System PICG/Clinical Operations Committee	4/17/14

Versioning History: