North Shore – LIJ Health System, Inc.

POLICY TITLE: **IS Asset Theft Reporting Procedure**	**ADMINISTRATIVE POLICY AND PROCEDURE MANUAL**
POLICY #: 900.14	**CATEGORY: Information Services**
System Approval Date: 12/12/13 **Site Implementation Date:**	**Effective Date: 7/13/2010** **Last Revised:**
Prepared by: Office of the CIO **IS Policy and Procedure Committee**	**Superseded Policy(s)/#:** **n/a**

GENERAL STATEMENT of PURPOSE

The discovery of theft or loss of a Health System owned electronic device, or other devices which may contain Health System data requires reporting and investigation to ensure the confidentially continued and to assist in the recovery of the asset. The high value and portability of laptop computers and "smartphones", as well as the inherent value of any data that may be stored on them, makes them particularly susceptible to theft and require the highest degree of care. Of equal importance to protecting them from theft is the prompt and diligent reporting of the loss of any such devices.

POLICY

Employees, contractors and others in possession of North Shore-Long Island Jewish Health System, Inc. ("Health System") owned electronic devices or any device storing or containing Health System data, are responsible for the protection of such equipment and data from theft or damage and the prompt reporting of the loss or theft of any such device.

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): 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 data, 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

Private Information: means any information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted, or encrypted with an encryption key that has also been acquired;

1) Social Security number; or
2) Driver's license number or non-driver identification number; or
3) Account number, credit or debit card number, in combination with any required Security code, access code, or password that would permit access to an Individual's financial account.

Private Information does not include publicly available information which is lawfully made available to the general public from federal, state or local government records.

1. RESPONSIBILITIES

- It is the entity's obligation upon discovery of the theft or loss of an IS asset, such as a laptop, workstation, server, blackberry or other IS device, to immediately notify the IS Help Desk.
- If an entity contacts Corporate Security, Site Security or OCIO Security, they must be instructed to notify the IS Help Desk and Corporate Compliance in order that proper notification and follow-up can be tracked.

- Corporate Security is responsible for interviewing the reporting entity responsible, collecting evidence and interacting with appropriate law enforcement agencies.
- OCIO Security is responsible for evaluating the technical risk of data compromise and coordinating with the Chief Technology Officer (CTO), Chief Information Officer (CIO), Office of Legal and Chief Corporate Compliance Officer or their designee will determine any appropriate breach notification steps, which should be taken to meet regulatory requirements.
- Any media or external communications regarding Health System thefts or loss should be handled by Public Relations.

2. PROCEDURE/GUIDELINES

2.1 Help Desk Team

- Collect relevant base information from reporting entity.
- Create Service Desk Ticket from information, notification to Corporate Security, OCIO Security and Corporate Compliance.

2.2 Corporate Security

- Collect additional relevant information from reporting entity.
- In emergency situations, Corporate Security must contact OCIO Security and Corporate Compliance to alert them to the situation.
- As appropriate, Corporate Security may contact Law Enforcement and Corporate Risk Management.

2.3 OCIO Security

- Confirm that device was encrypted.
- If necessary, speak with entity to determine nature of any data placed at risk as a result of the theft of the device.
- OCIO Security must contact Corporate Security and Corporate Compliance to confirm they are aware of the situation.
- If necessary, contact CTO to discuss actions to be taken. As appropriate, OCIO Security will contact other technology areas such as Service Management and the Telecommunications areas.

2.4 Corporate Compliance

- When the security-related incident involves Protected Health Information or Private Information, Corporate Compliance will work with applicable departments to determine whether the health system needs to comply with any applicable patient and regulatory notification requirements in accordance with *Policy 800.17 HIPAA and State Privacy Breach Notifications.*

3. 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.

4. 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
Corporate Security	Business hours: (516) 465-3078 After hours or on weekends: (516) 719-5000
Office of Corporate Compliance Help Line	(800) 894-3226
Office of Corporate Compliance Website	www.northshore-lij.ethicspoint.com
Office of Corporate Compliance	(516) 465-8097

REFERENCES to REGULATIONS and/or OTHER RELATED POLICIES
800.17 – HIPAA and State Privacy Breach Notifications Policy

CLINICAL REFERENCES
None

FORMS
None

APPROVAL	
System P&P Committee	7/13/2010; 11/21/13
System PICG /Clinical Operations Committee	7/29/2010; 12/12/13

Versioning History:
7/2010