North Shore–LIJ Health System, Inc.

POLICY TITLE: **Information Services Disaster Recovery Policy**	**ADMINISTRATIVE POLICY AND PROCEDURE MANUAL**
POLICY #: 900.24	**CATEGORY: Information Services**
System Approval Date: 1/15/2015 **Site Implementation Date:**	**Effective Date:** 10/25/12 **Last Revised/Reviewed:**
Prepared by: Office of the CIO–IS Policy and Procedure Committee	**Superseded Policy(s)/#:** **900.24 Disaster Planning and Operations Policy**

GENERAL STATEMENT of PURPOSE

The purpose of this policy is to outline the North Shore-LIJ Health System (Health System) strategies and processes for recovering key systems and data, including Sensitive and Highly Sensitive Information, in the event of an emergency situation or other significant occurrence which disrupts critical systems.

POLICY

The Information Services Disaster Recovery Policy requires the development and maintenance of data backup plans, disaster recovery plans, emergency mode operations plans, testing and revision procedures, and application data criticality analyses.

It is the responsibility of Information Services to develop, maintain, and periodically exercise the Disaster Recovery Plan for enterprise systems (the "Enterprise Disaster Recovery Plan").

If individual business units utilize systems, applications or devices that are not addressed in the Enterprise Disaster Recovery Plan, then each business unit, with oversight from Information Services to ensure compliance with regulatory requirements, is responsible for developing its own Disaster Recovery Plans in accordance with this policy. Each individual business unit is responsible for exercising its plans periodically and maintaining such plans on an ongoing basis. In connection with the Disaster Recovery activities covered by this policy, Information Services, or each business unit, as applicable, is responsible for safeguarding ePHI in a consistent manner during an emergency.

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

Disaster Recovery: The ability to restore an organization's critical systems and return the entity to an acceptable operational condition following a catastrophic event, by activating a disaster recovery plan.

Disaster Recovery Plan: A technology recovery plan to reestablish an organization's critical business applications following a disaster or significant impacting event.

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

Highly Sensitive Information: As defined by the *Data Classification Policy*, is PHI or any information that, if lost, corrupted, disclosed to or accessed by an unauthorized person, or disclosed or accessed by unauthorized means, may (i) violate federal, state, and/or local law, (ii) cause significant harm, injury or damage to another person or entity, or (iii) cause financial loss to another person or entity. Examples include, but are not limited to, Social Security number, credit card data, and driver's license information.

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 or 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; and
18. Any other unique identifying number, characteristic, or code.

Sensitive Information: As defined by the *Data Classification and Handling Policy*, is any information that, if lost, corrupted, disclosed to or accessed by an unauthorized person, or disclosed or accessed by unauthorized means, may cause harm, injury or damage to another person or entity. Examples include, but are not limited to, a number of PII data elements.

PROCEDURES/GUIDELINES

Information Services or each individual business unit, if such business unit utilizes systems or applications that are not covered by the Enterprise Disaster Recovery Plan (this plan does not include Huntington Hospital, Staten Island University Hospital, Feinstein Institute for Medical Research, and Medical Group Practices not on the enterprise Electronic Health Record), is responsible for developing and maintaining the following procedures:

- Data Backup
- Disaster and Systems Recovery
- Emergency Mode Operation
- Testing and Revision

Information Services and each individual business unit, as applicable, are responsible for conducting and documenting the Applications and Data Criticality Analysis.

Information Services will oversee the establishment, implementation, periodic testing and review of the Enterprise Disaster Recovery Plan. The Enterprise Disaster Recovery Plan includes the procedures, referenced in the following sections, that address recovery and restoration priorities, roles and responsibilities, and procedures for response and recovery. In addition, Information Services will oversee and assist each business unit with the development, implementation and periodic testing and review of Disaster Recovery Plans applicable to applications and systems that are not covered by the Enterprise Disaster Recovery Plan. Collectively, this policy and those policies and procedures reference below, including the Enterprise Disaster Recovery Plan and individual business unit level Disaster Recovery Plans, compose the enterprise contingency plan as contemplated by HIPAA CFR Part 45 164.308(a)(7).

Each Disaster Recovery Plan shall include a procedure to safeguard the integrity and accessibility of ePHI during recovery.

A. Data Backup Plan

The Data Backup Plan includes backup procedures for all important data sources such as patient accounting systems, electronic medical records, health maintenance and case management information, digital recordings of diagnostic images, electronic test results, or any other electronic documents created or used. The Data Backup Plan specifies data encryption requirements, backup and retention procedures, and offsite storage requirements for Disaster Recovery purposes.

B. Disaster Recovery Plan

The Disaster Recovery Plan reestablishes an organization's computing environment for critical business applications following a significant system or service disruption. The Disaster Recovery Plan must include the following components and set forth the person, group or division responsible for each activity:

1. Priorities for recovery and restoration, including a plan to recover and safeguard ePHI;
2. A list of applications that use Sensitive or Highly Sensitive Information, such as ePHI, categorized into tiered levels of priority;
3. Roles and responsibilities of recovery teams;
4. Business and personnel contact information for key individuals responsible for response and recovery;
5. Procedures for replacement of critical equipment; and
6. Procedures for authorized workforce members to access data centers and offsite locations where backup storage media are stored.

C. Emergency Mode Operations Plan

The Emergency Mode Operations Plan contains procedures to safeguard Sensitive or Highly Sensitive Information while operating in an emergency mode. The procedures include contact information for all persons that must be notified in the event of a disaster, roles and responsibilities of those people involved in the restoration process and procedures for responding to and maintaining operations during emergency situations and disasters.

The Emergency Mode Operations Plan also contains Emergency Access Procedures that support the continuity of operations should the normal access procedures be disabled or unavailable by establishing procedures to safeguard Sensitive or Highly Sensitive Information during an emergency and to identify personnel who are authorized to access the facility to perform data restoration.

Information Services will maintain procedures for the safeguarding and protection of Sensitive or Highly Sensitive Information, including ePHI, while operating in an emergency mode.

D. Testing and Revision Procedures

Testing and Revision Procedures require periodic exercises and review of System and Disaster Recovery documentation. Results from these exercises are documented, evaluated and reported to Information Services management. Identified corrective actions from these exercises are tracked and periodic status updates are communicated to appropriate individuals.

E. Application and Data Criticality Analysis

Information Services will conduct Application and Data Criticality Analyses to determine the overall relative importance to clinical, financial, and business needs to establish priorities for data backup, disaster recovery, and/or emergency operations plans by conducting business impact analyses.

TRAINING

The IT Disaster Recovery Team provides the appropriate workforce members with periodic Disaster Recovery Awareness training. and awareness of various emergency access plans.

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

- 100.009 Payment Card Industry Data Security Standards (PCI DSS) IT Security Policy
- 100.010 Payment Card Industry Data Security Standards (PCI DSS) Governance Policy
- 100.011 Payment Card Industry Data Security Standards (PCI DSS) Standard Policy
- 900.12 Data Classification Policy
- NS-LIJ Health System Human Resources Policy and Procedure Manual, Part V-3

- Human Resources Part XII-1 Termination of Employment: Voluntary, Involuntary
- Health Information Technology for Economic and Clinical Health (HITECH) Act
- The Enterprise Disaster Recovery Plan is located on the IT Disaster Recovery SharePoint Team Site
- 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)
- Health Insurance Portability and Accountability Act, 45 CFR Parts 160 and 164
- National Institute of Standards and Technology (NIST) 800 Series of Special Publications (SP), SP 800-30-Risk Management Guide for Information Technology Systems

CLINICAL REFERENCES

None

FORMS
None

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

Versioning History: