North Shore–LIJ Health System, Inc.

POLICY TITLE: **Information Technology Risk Management Policy**	**ADMINISTRATIVE POLICY AND PROCEDURE MANUAL**
POLICY #: 900.16	**CATEGORY: Information Services**
System Approval Date: 1/15/2015 **Site Implementation Date:**	**Effective Date: 2/24/11** **Last Revised/Reviewed: 12/12**
Prepared by: Office of the CIO–IS Policy & Procedure Committee	**Superseded Policy(s)/#:** 900.16 System and Network Risk Management and Evaluation Policy

GENERAL STATEMENT of PURPOSE

This policy provides criteria for conducting an information risk assessment, risk analysis, and implementation of a risk management program. It provides guidance for determining the risks to critical information assets and ensuring the availability, integrity, and confidentiality of information to the extent required by the North Shore-LIJ Health System (Health System) and applicable law and regulation, including, but not limited to, the *Health Insurance Portability and Accountability Act* (HIPAA), *Health Information Technology for Economic and Clinical Health (HITECH) Act, The American Reinvestment & Recovery Act (Meaningful Use),* and the *Payment Card Industry Data Security Standard* (PCI DSS).

POLICY

The Health System will perform periodic risk analyses and assessments on Health System devices and applications which create, receive, maintain, store, process, or transmit Sensitive or Highly Sensitive Information to determine the potential risks and vulnerabilities to the confidentiality, integrity, and availability of critical information assets maintained, received, stored, processed and transmitted by the Health System.

The Health System shall have a Risk Management Program for the purposes of, on an ongoing and periodic basis, identifying risks and the controls that mitigate such risks, and evaluating and prioritizing those controls to verify they are sufficient to reduce the Health System's risk posture to a reasonable and appropriate level as determined by the Information Technology (IT) Risk Governance Committee. The Program includes processes for reviewing and recommending security controls.

The Risk Management Program includes periodic risk analyses and assessments on systems and processes that create, receive, maintain, store, process, or transmit the Health System's Sensitive and Highly Sensitive Information, including but not limited to:

- Protected Health Information
- Customer payment data (such as a major credit or debit card)
- Unpublished research data
- Other information assets identified as Sensitive and Highly Sensitive by the Health System

These ongoing risk assessments and analyses will be conducted on a periodic basis, including when new applications are implemented or significant changes occur. The purpose of the risk assessments and analyses is to evaluate the security controls in place and to determine the degree of residual risk in the environment. In the event that these risk assessments and analyses identify a discrepancy between the expected and actual risk level, the Office of the Chief Information Officer (OCIO) IT Risk Management Department will address such risk in accordance with the Risk Management process described below.

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

Control Activities: These include all policies and standard operating procedures that are created as a direct result of a risk assessment that drives the Health System's mitigation strategy. *Control activities* should include general controls over information systems as well as specific application controls that ensure the accurate and timely processing of transactions. *Control activities* may be grouped into two general categories, preventative and detective. Preventative control activities are designed to avoid the exercise of vulnerability. Detective control activities are designed to identify when vulnerability has been exercised so that corrective actions may be taken.

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.

Risk: A *risk* is defined as the net mission impact considering: (1) the probability that a particular threat will exercise (accidentally trigger or intentionally exploit) a particular vulnerability; and (2) the resulting impact if this should occur. Such risks may arise from legal liability or mission loss due to unauthorized (malicious or accidental) disclosure, modification, or destruction of information; unintentional errors and omissions; information technology disruptions due to natural or man-made disasters or failure to exercise due care and diligence in the implementation and operation of an information technology system.

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.

Threats: An adapted definition of *threat*, from NIST SP 800-30, is "[t]he potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability." There are several types of threats that may occur within an information system or operating environment. Threats may be grouped into general categories such as natural, human, and environmental.

Vulnerabilities: Vulnerability is defined in NIST SP 800-30 as "[a] flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy." Vulnerabilities may be grouped into two general categories, technical and non-technical. Non-technical vulnerabilities may include ineffective or non-existent policies, procedures, standards or guidelines. Technical vulnerabilities may include holes, flaws or weaknesses in the development of information systems or incorrectly implemented and/or configured information systems.

PROCEDURES/GUIDELINES

1. The IT Risk Management Department is responsible for implementing the requirements of this policy, and documenting exceptions that require a higher risk threshold than would otherwise be accepted under this policy.
2. OCIO will establish a periodic reporting requirement to monitor the compliance and effectiveness of this policy.

REQUIREMENTS

1. **Risk Analysis Methodology:** Each risk analysis or assessment conducted by, or at the direction of, the IT Risk Governance Committee should adhere to the following base methodology:

    a. **Identify the Scope of the Analysis:** The scope of any risk analysis or assessment encompasses the potential risks and vulnerabilities to the confidentiality, availability, and integrity of Sensitive and Highly Sensitive Information that the Health System creates,

receives, maintains or transmits electronically. For each individual risk analysis or assessment, IT Risk Management will define the information assets that will comprise the scope of the risk analysis or assessment, which will include, at a minimum, systems, applications, and devices that create, receive, maintain, or transmit Sensitive or Highly Sensitive Information.

b. Gather Data: Gather relevant data by reviewing past and/or existing projects, performing interviews, reviewing documentation, or using other data gathering techniques. Document data gathering activities and data gathered to be included as part of the risk analysis results.

c. Identify and Document Potential Threats and Vulnerabilities: Identify and document potential threats and vulnerabilities to the confidentiality, availability, and integrity of information assets. Identified threats should include possible threat vectors including people, process and technology.

d. Assess Current Security Measures: Analyze current control activities implemented to minimize or eliminate risks to Sensitive and Highly Sensitive Information. Document analysis, including whether requisite security measures are in place, and if current security measures are configured and used properly. This process may include recent audit testing results, updated technical scans, and control effectiveness observation.

e. Determine Likelihood of Threat Occurrence: Establish the probability (likelihood) that an identified threat will trigger or exploit a specific vulnerability. Ratings such as high, medium, and low or numeric representations of probability may be used to express the likelihood of occurrence.

f. Determine the Potential Impact of Threat Occurrence: Determine the potential impact of identified threats triggering or exploiting a specific vulnerability. Such impact may be expressed using quantitative, semi-quantitative or qualitative metrics, but should convey the potential impact to the Health System.

g. Determine the Level of Risk: Determine the level of risk by analyzing the values assigned to the likelihood of threat occurrence and the resulting impact of threat occurrence. Document each assigned risk level, including a list of corrective actions to be performed to mitigate each risk level.

h. Identify Security Measures and Finalize Documentation: Identify security measures that can be used to reduce risk to a reasonable and appropriate level and conduct cost/benefit analysis to determine appropriate, effective, and efficient controls. Generate a risk analysis report that documents the risk analysis process, output of each step and initial identification of security measures.

2. **Risk Management Procedures:** In connection with the Health System's Risk Analysis process, IT Risk Management is responsible for performing the following activities:

- **Develop and Implement a Risk Management Plan:** Evaluate security measures identified as part of the risk analysis or assessment and recommend appropriate security measures for implementation based on the results of the risk assessment or analysis and the cost/benefit analysis. Document assigned resources and responsibility to implement the approved solution.
- **Evaluate and Maintain Security Measures:** Establish a structure and methodology for the periodic evaluation, recommendation, prioritization and implementation of risk-

reducing control activities. Conduct periodic risk assessments (including, but not limited to vulnerability assessments, procedural reviews, facilities assessments, control configuration evaluations, and penetration tests) to determine the effectiveness of implemented security controls and identify appropriate corrective actions. Participate in the change management process by conducting environmental and operational impact reviews. Controls assessed include, but are not limited to:

- System access
- Audit log monitoring
- Vulnerability assessments
- Data integrity
- Security awareness and training

- **Report Risk Posture:** Participate in the IT Risk Governance Committee whose mission is to (1) identify risks and controls that are in place to mitigate those risks, (2) review residual risk not addressed by existing controls, and (3) verify whether additional security measures are reasonable and appropriate based on the circumstances.
- **Recommend Security Measures:** Recommend control activities (technical and non-technical) to IT Management and the IT Risk Governance Committee (as appropriate) to reduce the risks to critical information assets to an acceptable level of risk. Once control activities have been approved by IT Management and the IT Risk Governance Committee (as appropriate) and implemented by the technical support teams, the risk level of information assets will be periodically re-evaluated and adjusted, as appropriate. Risk Analysis and Risk Management program information will be provided to members of the IT Risk Governance Committee.

3. Evaluation

OCIO undertakes periodic evaluations of its security safeguards. To determine the extent of compliance with the standards implemented under the HIPAA Security Rule, subsequent periodic reevaluations are conducted in response to environmental or operational changes occurring since the last evaluation that might impact the confidentiality, integrity or availability of ePHI.

OCIO shall perform evaluations directly or engage the services of a third party to conduct on behalf of the Health System. Evaluations may include a review of policies and procedures to evaluate their appropriateness and effectiveness in protecting against reasonably anticipated threats, a gap analysis, an assessment of security controls, and testing and evaluation to determine whether controls have been implemented properly. Following each evaluation, the Health System shall update its security policies, procedures, controls and processes, as appropriate, based on the results of the evaluation.

4. Exception Handling

OCIO will evaluate and document policy and standard exceptions that pose a higher degree of risk than typically approved under this policy. The evaluation and determination is based on various factors including business/clinical requirements as well as controls which are

already in place or can be implemented to mitigate the risk. The IT Risk Governance Committee will periodically review exceptions to determine if the risk level is appropriate.

5. Training

OCIO will provide periodic training to relevant individuals on the applicable provisions of this policy. The purpose of this training is to ensure that Risk Management personnel maintain a current understanding of the universe of threats creating risks in need of control, techniques for measuring inherent and residual risk, and which risks are addressed by a given control.

The Risk Management Program will participate in the development of the OCIO Security Awareness and Training Program to ensure that the Program is aligned with identified risks to the Health System.

6. Document Retention

Any documentation generated in compliance with this policy will be retained in accordance with the *Records Retention and Destruction 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 Help Line	800-894-3226
Office of Corporate Compliance Website	www.northshore-lij.ethicspoint.com

REFERENCES to REGULATIONS and/or OTHER RELATED POLICIES

- *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*.
- NS-LIJ Health System Human Resources Policy and Procedure Manual, Part V-2
- NS-LIJ Health System Human Resources Policy and Procedure Manual, Part V-3
- 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
- 100.97 Records Retention and Destruction Policy
- 800.42 Confidentiality of Protected Health Information Policy
- 900.12 Data Classification and Handling Policy
- 900.20 OCIO Security Awareness Training Program

CLINICAL REFERENCES

None

FORMS
None

APPROVAL	
System P&P Committee	1/11/11; Provisional Approval 10/25/12; Final Approval 11/29/12; 12/18/14
System PICG/Clinical Ops Committee	2/24/11; 12/13/12; 1/15/15

Versioning History:
10/12