Northern Light Health℠

Title: Information Security Risk Assessment	
Policy/Procedure #: 22-057	**Date Posted: 01/06/2026**
Initial Effective Date: 10/3/2013	Date Last Revised: 01/06/2026
Author: Christie Polley, VP & Chief Information Security Officer	
Executive Sponsor: SVP & Regional President – IT Executive Sponsor	Final Approver: SVP & Regional President – IT Executive Sponsor
Supersedes: 22-057	Dated: 04/03/2025

APPLICABILITY

☒ Northern Light Health adopts the following (and any Attachment(s)) for all its Member Organizations, specifically including, but not limited to, those listed below:

☐ Northern Light Health adopts the following (and any Attachment(s)) for its Member Organizations selected below:

- ☐ Northern Light Acadia Healthcare
- ☐ Northern Light Acadia Hospital
- ☐ Northern Light AR Gould Hospital
- ☐ Northern Light Blue Hill Hospital
- ☐ Northern Light CA Dean Hospital
- ☐ Northern Light Eastern Maine Medical Center
- ☐ Northern Light Health Foundation
- ☐ Northern Light Health Home Office
- ☐ Northern Light Home Care & Hospice
- ☐ Northern Light Maine Coast Hospital
- ☐ Northern Light Mayo Hospital
- ☐ Northern Light Medical Transport
- ☐ Northern Light Mercy Hospital
- ☐ Northern Light Pharmacy
- ☐ Northern Light Sebasticook Valley Hospital
- ☐ Work Health
- ☐ Other (list): _____

SCOPE

This Policy applies to all Users of Northern Light Health Systems.

RELATED POLICIES/PROCEDURES

System Policy 23-000, Sanctions for Violations of Confidentiality, Privacy and Information Systems Security

DEFINITIONS

For a more comprehensive list of definitions, please refer to the Northern Light Health HIPAA Policy Definition Set, linked above this Policy as a Related Document.

Adverse Events: Events (as defined in this Policy) with a negative consequence, such as an outage of functionality or application degradation, network packet floods, unauthorized use of system privileges, defacement of a web page, execution of a malicious code that destroys data, or receipt of sensitive data by unintended recipients.

Electronic Protected Health Information or ePHI: A specific type of PHI that is any PHI which is stored, accessed, transmitted or received electronically. ePHI includes Individually Identifiable Health Information contained in any medium used to store, access, process, transmit or receive PHI electronically. As technology progresses, any new device for accessing, transmitting, or receiving ePHI will be covered by the HIPAA Security Rule. Examples of ePHI media include, but are not limited to:

- Personal computers with their internal hard drives used at home, work, or while traveling;
- External portable hard drives;
- Magnetic tape or disks;
- Removable storage devices such as flash memory sticks/keys or optical media;
- Smartphones, tablets and other mobile computing devices;
- Electronic transmissions including data exchange (e.g., email or file transfer).

Event: Any observable occurrence in a System or network, such as a User connecting to a file share, a server receiving a request for a web page, a User sending electronic mail (e-mail), or a firewall blocking a connection attempt.

Protected Health Information or PHI: Individually Identifiable Health Information—which means it necessarily contains at least one Identifier—that is (1) transmitted by electronic media; (2) maintained in electronic media; or (3) transmitted or maintained in any other form or medium e.g., paper, images, recordings, etc. (45 CFR §160.103). PHI includes all Individually Identifiable Health Information, including information in research databases and tissue bank samples with Identifiers, relating to the:

- past, present or future physical or mental condition of an Individual;
- provision of Healthcare to an Individual; or to the
- past, present or future payment for the provision of Healthcare to an Individual.

Risk: The likelihood of a given Threat triggering or exploiting a particular Vulnerability and the resulting impact on the organization. Risks are mitigated by reducing the likelihood, Vulnerabilities or both. A security Risk is a function of the likelihood of an Adverse Event on a System and the impact of the Adverse Event.

Risk Assessment: A periodic, documented analysis of the potential Risks, potential adverse impacts, the likelihood they will occur and Vulnerabilities to the confidentiality, integrity and availability of ePHI, and an estimation of the security measures sufficient to reduce the Risks and Vulnerabilities to a reasonable and appropriate level. Risk analysis involves determining what requires protection, what it should be protected from and how to protect it.

System: An integrated set of components for collecting, storing, processing and communicating information. Examples of Systems are applications, databases, servers and other computing devices.

System Owner: The authority, individual or organizational head who has final responsibility for Systems which create, access, transmit or receive ePHI, including responsibility for the ePHI

data. In some complex Systems, the functional responsibility for the System and the responsibility for one or more applications or ePHI database(s) may lie with more than one individual. Decisions regarding who has access to the System and related ePHI data and responsibility for the Risk analysis rest solely with the System Owner. The System Owner may delegate responsibility for the technical management of a System to a qualified System administrator or staff member who is capable of implementing appropriate technical, physical and administrative safeguards.

Threat: The potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific Vulnerability. A Threat source can be human (hacker, uninformed employee) or non-human (natural disaster, chemical spill, etc.).

User: The person for whom a hardware or software solution has been designed and created to carry out job related functions.

Vulnerability: A flaw or weakness in System security procedures, design, implementation or internal controls that can be accidentally triggered or intentionally exploited, resulting in a security breach or a violation of the System's security policy. Vulnerabilities can be identified through manual or automated inspection.

PURPOSE

To provide a framework for assessing, prioritizing, and remediating Risks to Northern Light Health Information Systems and ePHI.

DIRECTIVE

All Northern Light Health and Member Organization Systems will have a Risk Assessment completed according to the Risk Management Framework below. System vendors and/or System Owners must provide all relevant and requested Systems information to the Northern Light Health Information Security Department for the purpose of completing a Risk Assessment. System Owners will also ensure that all requirements and recommendations are implemented once the System is put into production.

POLICY

A Risk Assessment for all Northern Light Health Systems is to be conducted prior to acquisition or implementation, and at least annually thereafter, and re-evaluated for each major upgrade or modification, when the Threat environment changes, and when Systems are renewed. Threat sources and Vulnerabilities are weighed against impact and likelihood of occurrence to define Risk. Northern Light Health and all Northern Light Health Member Organizations will conduct Risk Assessments based on the Information Security Risk Management Framework contained below in this Policy designed to assist Northern Light Health Leadership with decisions concerning:

- The protection of Northern Light Health Systems, recognized as primary organizational assets, from unauthorized modification, destruction, disruption or disclosure, whether accidental or intentional.
- The protection of the data contained in Northern Light Health Systems.

- The implementation of privacy and security requirements to support a compliance framework for policies and procedures.
- The creation of a secure enterprise that will meet the requirements of FISMA, HIPAA and other regulatory mandates.

This standard applies to all implemented and proposed Northern Light Health Information Systems, including those that support business and/or clinical operations. It consists of three parts, characterization, security control documentation and the Risk Assessment and remediation process. All parts must be completed to meet Risk Assessment requirements.

PROCEDURE

A. System Definition

1. System definition must identify the purpose, nature, and function of a System. At a minimum, the following information must be provided:

    a. System name: should uniquely and consistently identify the System and be familiar to System Owners and support personnel.
    b. System Owner: must include name, department, title and contact information.
    c. Primary System administrator: must include name, department, title, and contact information.
    d. Physical location(s) of the System components.
    e. System classification: must identify any components that create, access, transmit or receive (1) primary source ePHI or confidential organizational information; (2) ePHI critical for Treatment, Payment or Healthcare Operations; or (3) any form of ePHI where the host System is configured to allow access by multiple people.
    f. Workflow: must provide a description that details the nature of User interaction with the System.

2. All other relevant information that characterizes what the computing device or System is or does must be provided. The System definition must be such that someone other than the System Owner or administrator can explain the purpose of the computing device or System if asked when those individuals are not available.

B. Security Controls

1. Security controls are countermeasures designed to mitigate security Risks. A complete listing of security controls must be provided such that the security posture of the System in question can be determined. Security controls include, but are not limited to:

    - Physical controls such as locked doors and air conditioning.
    - Procedural controls such as incident response processes and security awareness training.
    - Technical controls such as User authentication and authorization, encryption, firewalls, and anti-virus protection.
    - Legal controls such as policies and contracts.

- Formal Risk management process, including a documented Risk Assessment of all Systems, an annual Risk review of organizational controls and remediation action plans.

2. All Systems must be securely configured to ensure compliance with regulations on the safeguarding of patient and confidential information. Such safeguards include, but are not limited to:

    - Access and authorization: how User and administrative access is provisioned, monitored and revoked.
    - Physical security: how the System's physical assets are protected from theft and unauthorized access.
    - Backup and restoration: the backup and restoration procedure for the electronic data that resides within the System in question.
    - System maintenance: what processes and procedures are in place to secure both the hardware and software used on the System. This includes, but is not limited to, hardware upgrades, application updates and operating System patches.
    - Protection against malicious software: what controls are in place to mitigate the Risk of exposure to malicious software, including, but not limited to, the use of anti-virus, application patching or System hardening.
    - Network security: what controls are in place to mitigate network-based attacks, such as the use of a firewall.
    - Encryption: how encryption is used to protect the confidentiality and integrity of patient and confidential information. This includes the encryption of data both in transit and at rest.
    - Auditing and Event logging: how and which Events are recorded and managed and the processes for analyzing them; at a minimum all "read" and "read/write" activity is to be logged and available for review.
    - Risk Assessment: past Risk Assessment results and the actions taken.
    - Business continuity: the plan to ensure business operations are not impacted by problems affecting the System and a definition of the System's criticality.
    - Security agreements: agreements with third parties responsible for providing components or services as part of the System.

3. All other documentation relevant to maintenance and security of the device or application must be provided. Examples of other documentation include software configuration or data center operations procedures.

C. Risk Management Framework

Risk management can be viewed as a holistic activity that is fully integrated into every aspect of the organization. Risk Assessments and organizational Risk reviews provide Northern Light Health leadership with the information necessary to both accept and understand factors that can negatively influence operations and to make informed judgments concerning the extent of actions needed to reduce Risk.

The Northern Light Health Information Security Department will conduct both internal and external Risk Assessments on a regular basis for all of Northern Light Health as follows:

1. Internal Risk reviews take place on an annual basis with quarterly updates.

2. Proposed acquisitions, renewals and any substantive changes to the Northern Light Health IS network and its applications require an internal System Risk Assessment prior to acquisition or implementation.

3. Northern Light Health Information Security will ask for a third-party external Risk review (audit) on an annual basis. A Risk audit provides a measure of independence and perspective not usually present in a Risk review conducted by line management. The Risk audit is to focus on compliance with standards, procedures and legislative requirements. It is to be Risk based and is to focus on assessing the effectiveness of Northern Light Health Risk treatment measures.

   <u>Internal Risk Assessment</u>:

   1. Northern Light Health will follow the security control baselines, as defined by the NIST 800-53 guidelines. Identified Risks will be rated and prioritized based on a Risk score derived from the level of Threat the Vulnerability poses and the likely impact on the Risk to the System(s).

      a. Internal Risk reviews of the controls are conducted annually with updates provided on a quarterly basis.
      b. Network Vulnerability scans are conducted and reviewed quarterly.
      c. The Northern Light Health Information Security Department maintains the System Security Plan (SSP) and the Plan of Action & Milestones (POAM) as the documentation for the control Risk reviews.
      d. The SSP and the POAM are to include recommendations for the controls and remediation action plans provided by the System Owners and/or the designated IS System Director.

   2. The Northern Light Health Information Security Department will conduct a System Risk Assessment for all proposed, renewing or upgrade software and application acquisitions and report findings to the Risk Assessment Review Team.

a. Requests for System Risk Assessments should be submitted through ServiceNow via the Idea/Demand Management process and are to be conducted before the acquisition is finalized.
b. All requests must be accompanied by a completed Northern Light Health IS Application Risk Security Questionnaire.
c. Identified Risks will be rated and prioritized based on a Risk score derived from the level of Threat the Vulnerability poses and the likely impact on the Risk to the System(s).
d. Identified Risks are to be addressed with a formal mitigation plan prior to the acquisition.
e. An acquisition or renewal that contains any identified High and Critical Risks that cannot be fully mitigated requires the System Owner to submit a business use case to the Northern Light Health Chief Information Security Officer (CISO). The CISO will engage Northern Light Health senior executive leadership for further review and approval where appropriate.
f. Northern Light Health Information Security will maintain the documentation for each System Risk Assessment.
g. The System Owner will be provided a copy of the completed Risk Assessment and will be required to sign an attestation acknowledging (1) receipt of the completed Risk Assessment; and (2) understanding of their responsibility for any remediation actions. Failure to complete an attestation timely will be escalated to Northern Light Health Compliance.
h. Introducing a System onto a Northern Light Health network or device without a Risk Assessment or placing PHI on an unapproved System are grounds for sanctions under System Policy Sanctions for Violations of Confidentiality, Privacy and Information Systems Security (23-000).

External Risk Review:

1. An external third-party Risk review (audit) will be conducted on an annual basis for Northern Light Health.

2. The purpose of a Risk audit is to test the Systems in place to manage Risk and report deficiencies to ensure remedial actions are taken. Identified deficiencies indicate systemic weakness and require remediation of the System, not just the symptoms.

3. The external Risk Assessment and remediation recommendations resulting from this audit will be provided to Information Security Council.

REFERENCES

1. NIST 800-66 rev 1, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA), October 2008
2. NIST 800-30 rev 1, Guide for Conducting Risk Assessment
3. NIST 800-53, Recommended Security Controls for Federal Information Systems

ATTACHMENTS
Northern Light Health HIPAA Policy Definition Set, linked above this Policy as a Related Document

This document was approved by the committee(s) noted below on the date(s) as noted:
Leadership Council, 9/17/2013, 6/28/2024
Information Security Council, 9/11/2017, 4/25/2018, 11/24/2020, 12/17/2021, 9/16/2022, 6/28/2023, 5/21/2024
Compliance Committee, 9/14/2022, 6/14/2023, 5/8/2024, 3/12/2025, 12/10/2025
Compliance Task Force, 5/24/2016, 3/27/2018, 12/11/2019, 2/23/2021, 12/14/2021
IS Vice Presidents, 8/29/2019