Northern Light Health

Title: Sanctions for Violations of Confidentiality, Privacy and Information Systems Security	
Policy/Procedure #: 23-000	**Date Posted: 12/16/2025**
Initial Effective Date: 12/2007	Date Last Revised: 12/16/2025
Author: Jason Tankel, VP & Chief Compliance and Internal Audit Officer	
Executive Sponsor: VP & Chief Compliance and Internal Audit Officer	Final Approver: VP & Chief Compliance and Internal Audit Officer
Supersedes: 23-000	Dated: 04/01/2024

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 employees, contractors, medical staff members (including those who are neither employees nor contractors of Northern Light Health), vendors, students, and volunteers who Access Confidential Information.

RELATED POLICIES/PROCEDURES

System Policy 17-000, Information Systems Monitoring
System Policy 23-118, Information Classification
System Policy 23-004, Breach Notification - Instructions for Investigating, Documenting, and Providing Notice of an Unauthorized Disclosure or Access of Patient Information
System Policy 23-007, Reporting and Investigating Compliance Concerns

DEFINITIONS

12-Month Period: A time period that is less than 12 consecutive months after a Sanction has been imposed on the same User in response to a Violation.

Access/Accessing: The ability or the means necessary to hear, observe/see, read, write, modify, or communicate Confidential Information.

Breach: The unauthorized acquisition, Access, Use, or disclosure of unsecured patient protected health information (PHI) in a manner that compromises the security or privacy of the PHI, as further defined in System Policy 23-004 Breach Notification - Instructions for Investigating, Documenting, and Providing Notice of an Unauthorized Disclosure or Access of Patient Information.

Confidential Information: Any Northern Light Health or Northern Light Health Member Organization information subject to System Policy 23-118 Information Classification.

Covered Entity: A health plan, a healthcare clearinghouse, or a Healthcare Provider that transmits any Health Information to which HIPAA applies.

Privacy Officer: Any Northern Light Health or Member Organization Privacy Officer involved in investigating a Violation under this Policy.

Sanction: A corrective action taken in response to a Violation. Sanctions may include, along with other actions, additional training or education, verbal warnings, written warnings, suspension without pay, and/or termination.

Use/Using: With respect to Confidential Information, the sharing, disclosure, employment, application, utilization, examination, or analysis of such information.

User: Any individual who is authorized to Access or Use Confidential Information, including employees, contractors (including contracted medical staff members), vendors, volunteers, students, and trainees.

Violation: A Violation of any law, regulation, rule or Northern Light Health or Member Organization policy that addresses Confidential Information. A Violation does not include an Access or Use outside a User's reasonable control (e.g., the User is provided inaccurate information by an external party, etc.).

PURPOSE

To ensure Northern Light Health and its Member Organizations apply consistent Sanctions for privacy and information security Violations.

POLICY

1. User activity resulting in a Violation is subject to the Sanctions outlined within this policy. Reporting of known or suspected Violations is required per System Policies 23-004, Breach Notification – Instructions for Investigating, Documenting and Providing Notice of Unauthorized Disclosure or Access of Patient Information and 23-007, Reporting and Investigating Compliance Concerns. Failure of a User to report a known or suspected Violation may result in a Sanction.

    A. If a report is made, an initial investigation of the facts shall be completed without delay.
        i. Investigations involving medical staff members will be conducted by the Senior Physician Executive (SPE), with assistance from the Privacy Officer and/or a Human Resources representative.

ii. Investigations involving all other Users will be conducted by the appropriate individuals, e.g.:
    a. The employee's manager or supervisor will conduct investigations involving Northern Light Health employees;
    b. Privacy Officer;
    c. Human Resources representative;
    d. A contractor's (including contracted medical staff member's) direct employer will conduct investigations involving the contractor's employee if consistent with terms of the contractor's agreement with Northern Light Health or the Member Organization. Any involved Privacy Officer(s), Human Resources representative(s) and/or SPE(s) are responsible for documenting the results of these investigations and assuring that the classification of the Violation and applied Sanction comply with this Policy.

B. If the party conducting the initial investigation determines that no Violation occurred, the Privacy Officer will document the investigation using any relevant information provided by the party who conducted the investigation.

C. If the party conducting the initial investigation determines that the Violation is an At Risk Violation (see Table A below), they will ensure documentation of the event and of the associated User re-education is maintained in the personnel file and will notify the Privacy Officer.

D. If the party conducting the initial investigation determines that the Violation is a Minor Violation (see Table A below) and the Sanction applied is a documented oral reprimand, their obligations under this Policy are satisfied once the Privacy Officer and Human Resources representative have been notified.

E. If the party conducting the initial investigation determines that the Violation is other than an At Risk or Minor Violation (see Table A below) or expects to apply a Sanction other than a documented oral reprimand for a Minor Violation, the Violation must be discussed with the Privacy Officer and Human Resources representative before taking any additional action.

F. For Violations other than those categorized as At Risk or Minor Violations, the Violation level (see Table A below) will be decided by consensus of all individuals involved in conducting the investigation. The local Human Resources representative will assure that the required minimum Sanction is applied consistent with Table A below.

G. Conditional Reporting (medical staff and contracted Users)
    i. For Violations involving medical staff members, the group involved in the investigation will determine if the facts and circumstances of the investigation require additional reporting to the Medical Executive Committee or to the medical staff member's employer or medical group as applicable.

ii. For Violations involving vendors or contracted Users, the group involved in the investigation will determine how to engage with the User's employer based on the facts and circumstances of the investigation and the terms of any applicable contract the employer has with Northern Light Health or the Member Organization.

H. If more than one Northern Light Health Member Organization is involved in or affected by a Violation that is more serious than an At Risk or Minor Violation, the involved Privacy Officers will work together to conduct and document the initial investigation in consultation with the Northern Light Health Chief Compliance Officer and the Northern Light Health Chief Information Security Officer as appropriate.
   i. The involved Privacy Officers will document the facts, findings, and outcomes of the initial investigation.
   ii. If the Privacy Officers conducting and/or documenting the initial investigation determine that a Violation occurred, they will discuss the facts and findings with and provide related documentation to the appropriate Human Resources representatives and managers or Senior Physician Executives.
   iii. The Violation level (see Table A below) will be decided by consensus of the Northern Light Health group involved in conducting the investigation.
      a. In the event consensus on the Violation level cannot be reached, the involved Privacy Officers will bring the matter to the Northern Light Health Chief People & Administrative Officer, Chief Compliance Officer and SVP/SPE. This group will by consensus assign the Violation level.
   iv. For Violations involving medical staff members, vendors or contracted Users, refer to section F of this Policy, Conditional Reporting.

2. When an initial investigation is conducted by a third party, the involved Privacy Officer(s) and any other Northern Light Health employees involved in the investigation may rely on the findings of the third party to the extent reasonable.

3. The facts, findings, and outcome of all investigations (including the applied Sanction) must be documented and shared with any involved Privacy Officer(s).

4. Information security incidents that involve a Violation as defined in this Policy (e.g., a lost laptop, compromised logon resulting from phishing, etc.) are subject to the Sanctions outlined in this Policy. The Violation Level and resulting Sanction, if any, will be determined by consensus between the Northern Light Health Chief Compliance Officer, the Northern Light Health Chief Information Security Officer, Chief People & Administrative Officer, and any additional stakeholders as determined by this group.

5. This Policy is to be used, as applicable, in conjunction with System and Member Organization Human Resources policies covering progressive disciplinary action and in accordance with the Northern Light Health Medical Staff Bylaws as applicable.

6. This Policy provides for progressive Sanctions for repeated and/or more serious Violations. Table A below provides guidance for determining the Violation level. Violations should be classified consistent with the examples provided in Table A below.

7. Whether an event rises to the level of a Violation, or to a particular Violation level, will depend on all associated facts and circumstances.

8. After a Violation level is assigned, the minimum Sanction corresponding to that Violation is required. For example, a Violation classified as a Serious Violation requires at least a written warning, with discussion of policies, procedures, and requirements of position.

9. Any deviation from the minimum Sanction prescribed in Table A for a Minor or Serious Violation requires documented agreement between all involved Human Resources representatives, Privacy Officers and, as applicable, SPEs.

10. Any deviation from the minimum Sanction prescribed in Table A for a Major or Flagrant Violation requires documented agreement among the Northern Light Health Chief People & Administrative Officer, Chief Compliance Officer, Chief Legal Officer and SVP/SPE.

Table A: Violation Severity Guidance and Required Minimum Sanction

Violation Level	**Examples (Illustrative Only – Not Inclusive of All Possible Violations/Breaches)**	**Minimum Sanction**
At Risk Violation: Typically, a single inadvertent act which does not result in compromise of patient or organizational information. Often involves a repetitive, high-volume task.	• Causing a misdirected fax/mail/email/print internally or to another Covered Entity (escalates to Serious if misdirected to an external location/entity/individual that is not a Covered Entity)	Documented re-education on policies and procedures.
Minor Violation: A second At Risk Violation in a 12-Month Period; or an inadvertent act caused by inattention or carelessness which results in the potential compromise of patient or organizational information.	• Leaving information where it is accessible to unauthorized persons (escalates to Serious if left in a non-Northern Light Health location) • Discussing Confidential Information (otherwise appropriately disclosed) in public areas of the organization under circumstances where information may be overheard by those not authorized to know (escalates to Serious if	Documented oral reprimand with discussion of policies, procedures and requirements of position.

Violation Level	Examples (<u>Illustrative Only – Not Inclusive of All Possible Violations/Breaches</u>)	Minimum Sanction
	conversation occurs in a non-Northern Light Health location) • Failing to sign off or lock a personal computer terminal when not in use (escalates to Serious if a shared computer terminal)	
Serious Violation: A third At Risk or second Minor Violation in a 12-Month Period; or what generally is a <u>reckless</u> act which could potentially compromise the security, integrity or confidentiality of patient or organizational information.	• Not properly verifying an individual's identity before disclosing Confidential Information • Failing to sign off a shared computer terminal when not in use • Not accounting for disclosures outside of treatment, payment or healthcare operations • Accessing, Using or disclosing patient information when there is no business purpose (i.e., no Northern Light Health treatment, payment or healthcare operations need) to do so but there is proof that (i) the patient is okay with the Access, Use or disclosure (e.g., User is patient's identified parent, guardian, agent or other personal representative, applicable ROI is on file, etc.) and (ii) the patient information Accessed, Used or disclosed is **not** subject to heightened privacy protections (e.g., the information relates to care to which a minor patient has consented, etc.) • Emailing Confidential Information outside of Northern Light Health without encrypting the data • Disregard of authorization requirements resulting in an	Written warning with discussion of policy, procedures and requirements of position. Possible suspension without pay, suspension or termination of Access, termination of contract and/or suspension of privileges as appropriate based on role and employment status.

Violation Level	Examples (<u>Illustrative Only – Not Inclusive of All Possible Violations/Breaches</u>)	Minimum Sanction
	unintentional unauthorized disclosure • Causing an unintentional unauthorized disclosure through a misdirected fax/mail/email to a non-Covered Entity • Mistakenly giving patient discharge instructions, a patient visit summary, or other medical record to the wrong patient	
Major Violation: A fourth At Risk or third Minor Violation in a 12-Month Period or a second Serious Violation; or what generally is an <u>intentional</u> act which compromises the security, integrity, or confidentiality of patient or organizational information.	• Accessing, Using or disclosing patient information when there is no business purpose (i.e., no Northern Light Health treatment, payment or healthcare operations need) to do so and, while there may be proof that the patient may be okay with the Access, Use or disclosure (e.g., User is patient's identified parent, guardian, agent or other personal representative, applicable ROI is on file, etc.), the patient information Accessed, Used or disclosed is subject to heightened privacy protections (e.g., the information relates to care to which a minor patient has consented, behavioral health records, HIV information, substance abuse treatment information, etc.) • Failing to report a suspected or known privacy or information security Violation • Sharing sign-on information (User ID and password) with another User • Disclosing User sign-on information (e.g., entering User ID and password into unauthorized links or websites,	Suspension without pay, suspension of Access, termination of contract and/or suspension of privileges as appropriate based on role and employment status.

Violation Level	Examples (Illustrative Only – Not Inclusive of All Possible Violations/Breaches)	Minimum Sanction
	or providing User ID and password to someone over the phone) • Using another User's sign-on information (User ID and password) to Access or Use a Northern Light Health information system (includes Use of a Northern Light Health information system after the previous User failed to sign off) • Displaying sign-on information (User ID and password) where it can be seen by others (e.g., on a sticky note attached to a computer monitor, etc.) • Downloading or installing unauthorized software or other material on an electronic device that connects to Northern Light Health information systems	
Flagrant Violation: Any serious or major Violation following suspension of employment pursuant to this policy; or what generally is an intentional act which could significantly compromises the security, integrity or confidentiality of patient or organizational information.	• Unauthorized Use of PHI for marketing purposes • Accessing, Using or disclosing patient information when there is no business purpose (i.e., no Northern Light Health treatment, payment or healthcare operations need) to do so, and the Access, Use or disclosure is not legally permissible • Sharing sign-on information (User ID and password) with a non-User • Any Access, Use or disclosure of patient information for personal gain or to harm someone else • "Snooping" (e.g., Accessing the patient information of a co-worker, neighbor, or someone	Immediate termination of employment, contract, Access, and/or privileges as appropriate based on role and employment status.

Violation Level	Examples (Illustrative Only – Not Inclusive of All Possible Violations/Breaches)	Minimum Sanction
	who is part of a news event to satisfy the User's curiosity, etc.) • Use of financial information, strategic plans, credentialing or peer review information, or other types of Confidential Information for personal gain or to harm someone else • Circumventing security policies to access the internet or changing computer IDs to avoid detection • Undermining the integrity of PHI (e.g., inappropriately altering PHI, etc.) • Posting sensitive or identifiable patient information online or in any other public forum	

This Policy is written to assist Northern Light Health and its Member Organizations to comply with their obligations under HIPAA. Users not employed by Northern Light Health may have additional compliance and reporting obligations under HIPAA and should consult their own compliance officer, Privacy Officer or legal counsel for guidance.

PROCEDURE
None.

REFERENCES
None.

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, 12/2007, 3/28/2024
Compliance Committee, 8/9/2023, approved via email on 2/12/2024, 11/12/2025
Compliance Task Force, 5/24/2016, 1/11/2017, 2/26/2019, 1/26/2021