POLICY TITLE: HIPAA and State Privacy Breach Notifications	SYSTEM POLICY AND PROCEDURE MANUAL
POLICY #: 800.17	**CATEGORY:** Compliance and Ethics
System Approval Date: 07/22/2025❖ **Site Implementation Date:** 07/22/2025❖	**Effective Date:** 6/2011 **Last Reviewed/Approved:** 04/2025
Prepared by: Office of Corporate Compliance	**Notations:** N/A

GENERAL STATEMENT of PURPOSE

The purpose of this document is to provide guidance on notifying patients and other applicable individuals, the United States Department of Health and Human Services ("HHS"), media outlets and state agencies if either a Breach of a patient's Unsecured Protected Health Information ("PHI") or a Security Breach of an individual's Private Information as required.

POLICY

It is the policy of Northwell Health to notify affected individuals, HHS (if applicable), media outlets (if applicable), and state agencies (if applicable) if a Breach of Unsecured Protected Health Information or a Security Breach of Private Information occurred as soon as possible and in no case later than 60 days of discovering the Breach, unless otherwise required by law.

SCOPE

This policy applies to all Northwell Health employees, as well as medical staff, volunteers, students, trainees, physician office staff, contractors, trustees and other persons performing work for or at Northwell Health; faculty and students of the Donald and Barbara Zucker School of Medicine at Hofstra/Northwell or the Hofstra Northwell School of Nursing and Physician Assistant Studies conducting research on behalf of the Zucker School of Medicine on or at any Northwell Health facility.

DEFINITIONS

Breach: where there has been an acquisition, access, use, or disclosure of PHI in a manner not permitted by the Health Insurance Portability and Accountability Act ("HIPAA") Privacy Rule, the matter shall be considered a Breach unless Northwell Health demonstrates there is a low

probability that the PHI has been compromised based on a risk assessment of at least the following factors:

1. The nature and extent of the PHI involved, including types of identifiers and the likelihood of re-identification;

2. The unauthorized person who accessed or used the PHI or to whom the disclosure was made;

3. Whether the PHI was actually acquired or viewed; and

4. The extent to which the risk to the PHI has been mitigated.

In all cases, the Office of Corporate Compliance must be contacted as soon as possible to make this determination.

The term Breach does not include:

1. Any unintentional acquisition, access, or use of PHI by a Northwell Health workforce member or individual acting under the authority of a Northwell Health facility or Business Associate if:
   - Such acquisition, access, or use was made in good faith and within the course and scope of authority; and
   - Such information is not further used or disclosed in a manner not permitted; or

2. Any inadvertent disclosure of PHI by a person who is authorized to access PHI at a Northwell Health facility or Business Associate, or through an organized health care arrangement in which Northwell Health participates with another person authorized to access PHI at the same Northwell Health facility or Business Associate, or through an organized health care arrangement in which Northwell Health participates; and any such information received as a result of such disclosure is not further used or disclosed in a manner not permitted; or

3. A disclosure of PHI where a Northwell Health facility or Business Associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

Individuals are required to consult the Privacy Officer of their facility or Office of Corporate Compliance, 516.465.8097, to determine if a Breach has occurred.

Business Associate (BA): A person or entity that performs certain functions or activities, or provides services that creates, receives, maintains, processes or transmits PHI on behalf of, or to Northwell Health and is an external person or entity.

Examples of BA functions or activities can include, but are not limited to claims processing or administration, data analysis, utilization review, quality assurance, billing, benefit management, practice management, and software hosting of PHI. Examples of BA services include legal,

actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, and financial.

If you have any questions regarding whether a person or entity's function qualifies as a BA, contact the Procurement office.

Health Insurance Information: an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual or any information in an individual's application and claims history, including, but not limited to, appeals history.

Medical Information: any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

Personal Information: any information concerning a person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person.

Protected Health Information ("PHI"): Any oral, written, or electronic individually identifiable health information. PHI is information created or received by Northwell that (i) may relate to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the payment for the provision of health care to an individual; and (ii) identifies the individual who is the subject or based on which there is a reasonable basis to believe that the individual who is the subject can be identified. The Health Insurance Portability and Accountability Act (HIPAA) further clarifies that PHI includes information that identifies the individual by one or more (depending on context) of the following 18 identifiers:

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/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.

Unsecured PHI: PHI that is not encrypted or PHI that is made usable, readable, or decipherable to unauthorized individuals through the use of another technology or methodology specified by the HHS.

Private Information:

1. Personal Information consisting of any information in combination with any one or more of the following data elements, when either the data elements or the combination of Personal Information plus the data element is not encrypted, or is encrypted with an encryption key that has also been accessed or acquired;

    a. Social Security number;
    b. Driver's license number or non-driver identification number;
    c. Account number, credit or debit card number, in combination with any required security code, access code, password or other information that would permit access to an individual's financial account;
    d. Account number, credit or debit card number, if circumstances exist wherein such number could be used to access an individual's financial account without additional identifying information, security code, access code, or password;
    e. Biometric information, meaning data generated by electronic measurements of an individual's unique physical characteristics, such as a fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation of biometric data which are used to authenticate or ascertain the individual's identity;
    f. Medical information; or
    g. Health insurance information; or

2. A username or e-mail address in combination with a password or security question and answer that would permit access to an online 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.

Security Breach: an unauthorized access to or acquisition of computerized data which compromises the security, confidentiality or integrity of Private Information maintained by Northwell Health except:

Good faith access to, or acquisition of Private Information by an employee or agent of Northwell Health for the purposes of Northwell Health is not a Security Breach, provided that the Private Information is not used or subject to unauthorized disclosure.

In determining whether information has been accessed, or is reasonably believed to have been accessed, by an unauthorized person, such business may consider, among other factors, indications that the information was viewed, communicated, used, or altered by an unauthorized person.

In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person, such business may consider the following factors, among others:

1. Indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; or

2. Indications that the information has been downloaded or copied; or

3. Indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

Individuals are required to consult the Privacy Officer of their facility or the Office of Corporate Compliance, 516.465.8097, to determine if a Security Breach has occurred.

PROCEDURE

Internal and External Health System Notification

If an individual becomes aware of a Breach of Unsecured PHI or a Security Breach of Private Information, they must notify the Office of Corporate Compliance immediately. If a Business Associate becomes aware of a Breach of Unsecured PHI or a Security Breach of Private Information, they must notify Northwell Health as soon as reasonably possible after discovery of the Breach, but in no case later than as specified in the applicable business associate agreement.

The Office of Corporate Compliance will coordinate with the Office of Legal Affairs, Enterprise Digital Services, and any other appropriate department to determine if a Breach or Security Breach has occurred and will document its breach analysis in applicable cases of non-Breaches and shall notify Risk Management if Compliance determines a Breach or a Security Breach occurred.

Patient Notification

If an investigation confirms that a patient's PHI has been Breached, the following procedure will be followed:

1. The Office of Corporate Compliance, or its designee, will notify affected patients, in writing, of such Breach and any services offered to reduce the risk of harm, such as credit monitoring, without unreasonable delay and in no case later than 60 calendar days after the discovery of a Breach. The time period of discovery begins when the incident is first known, or should have been known, even if it is initially unclear whether the incident constitutes a Breach.

2. If the patient is deceased, the next of kin or personal representative shall be notified. If the patient is incapacitated/incompetent, the personal representative shall be notified. If the patient is a minor, the parent or guardian shall be notified unless otherwise required by law.

Method and Format of Notification

The notification shall be written in plain language and sent by first-class mail to the last known address of the patient or the next of kin, or if specified by the patient, by encrypted electronic email. The notification may be provided in one or more mailings as information becomes available.

If a facility determines the patient should be notified urgently of a Breach because of possible imminent misuse of Unsecured PHI, the facility may, in addition to providing the notice outlined above, contact the patient by telephone or other means, as appropriate.

Insufficient Notification Data

If Northwell Health has insufficient or out of date information for **fewer than ten** patients, Northwell Health shall attempt to provide an alternative form of notice such as a telephone call.

If **ten or more** individuals require alternative/substitute notice, then notice of the Breach shall be posted prominently for 90 days on the applicable Northwell Health website homepage and include a toll-free number or include the same information in prominent media outlets. The individual representing the department or facility in which the Breach occurred shall work directly with the Public Relations Department or its designee in arranging this notification.

Media Notification

If the Breach involves the Unsecured PHI of more than **500** individuals of any one state or jurisdiction, in conjunction with the Office of Corporate Compliance, the Public Relations Department will provide notice, within 60 days of discovery, to prominent media outlets.

HHS Notification and Breach Log

The Office of Corporate Compliance shall provide notice of the Breach to HHS without unreasonable delay and in no case later than 60 days from the Breach discovery if a single Breach event affected **500 or more** individuals.

If a Breach affects **fewer than 500** individuals, the Office of Corporate Compliance shall use the electronic form available on the HHS website and submit to HHS no later than 60 days after the end of the calendar year in which the Breach was discovered.

All Breaches reported to HHS shall also be reported to the New York State Attorney General, the department of state and division of state police regardless of whether they constitute Security Breaches. Notification shall be made to the New York State Attorney General within five business days of notifying HHS. In the event that more than five thousand New York residents are to be notified at one time, Northwell Health shall also notify consumer reporting agencies as to the timing, content and distribution of the notices and approximate number of affected persons.

The Office of Corporate Compliance shall maintain a log of all reported Breaches of Unsecured PHI and Security Breaches. The Office of Corporate Compliance shall submit required reports of such to the Secretary of HHS and applicable New York State agencies annually.

Identifying, Receiving, and Investigating Complaints Involving Improper Disclosures of PHI

HIPAA Case Tracking Log

A HIPAA Case Tracking Log, containing the status of all active HIPAA-related matters, is maintained to track all potential HIPAA violations. The HIPAA Case Tracking Log is updated and reviewed on a weekly basis by appropriate Office of Corporate Compliance Team Members as well as the Senior Vice President and Chief Corporate Compliance Officer and the Corporate Privacy Officer, to ensure issues involving the improper disclosure of PHI are carefully monitored and resolved.

Any case that remains open after 30 days or more requires the Compliance team member and Privacy Officer to have a meeting with the Corporate Privacy Officer. Any case that is open 40 days or more requires the Compliance team member and Privacy Officer to follow up with the Chief Corporate Compliance Officer and the Corporate Privacy Officer to provide an update on the matter.

After the investigation is complete, and accompanying documentation finalized, the matter is closed out and moved to either the Breach or Non-Breach Log, as applicable.

The HIPAA Case Tracking Log is shared with our Risk Management Department, Corporate Security, Human Resources and Quality Management on a weekly basis and other departments, as applicable. Also, Corporate Security shares a report of all incoming cases to their department with Compliance on a periodic basis.

All alleged and confirmed identity theft cases that are reported are tracked in the Identity Theft Log maintained by Corporate Compliance and distributed, as needed, to Corporate Security, Risk Management, Legal Affairs and the Executive Audit and Compliance Committee.

Cases received through our Compliance HelpLine are reviewed weekly by the applicable Compliance professional to ensure all cases that involve improper disclosures of PHI are also being tracked on the HIPAA Log and Identity Theft Log, where applicable.

Both the HIPAA Case Tracking Log and Identity Theft Log are shared with the Protected Health Information Committee, the Executive Privacy and Security Committee and the Executive Audit and Corporate Compliance Committee at each meeting.

Audit

In order to ensure applicable patients and government agencies are notified of an improper acquisition, access, use or disclosure of PHI, the Office of Corporate Compliance will conduct an audit at the end of the reporting year to ensure patients and applicable government agencies were properly notified of a reportable breach.

Delay of Notification Exception

If a law enforcement official states that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, such notification, notice or posting shall be delayed by up to 30 days, if the statement is made orally. Such oral statement should be documented and include the identity of the official making the statement. If the statement is in writing and specifies the time for which a delay is required, such notification, notice or posting shall be delayed for the time period specified by the official.

A decision to delay a notification shall be made by the Office of Legal Affairs.

Content of Notification

Regardless of the method by which notice is provided to an individual(s) as set forth above, a notice of a Breach shall include, to the extent possible, the following:

1. Brief description of what happened, the date of the Breach and the date of the discovery of the Breach, if known;

2. Description of the types of Unsecured PHI that were involved in the Breach, such as full name, Social Security number, date of birth, home address, account number, diagnosis or disability code. Please note that only the generic type of data should be listed in the notice (e.g., "date of birth" rather than actual date of birth);

3. Any steps the individual(s) should take to protect themselves from potential harm resulting from the Breach;

4. A brief description of what Northwell Health is doing to investigate the Breach, to mitigate harm to individuals, and to protect against further Breaches; and

5. Contact procedures for individual(s) to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, website, or postal address.

New York State Security Breach Notifications

If our investigation of the data breach also reveals that there has been a Security Breach, we shall also follow the following procedures:

1. The Office of Corporate Compliance will coordinate with the Office of Legal Affairs and other applicable departments to notify any other owner or licensee of the information of any Security Breach immediately following discovery, if the Private Information was, or is reasonably believed to have been, acquired by a person without valid authorization;

2. The Office of Corporate Compliance will notify any resident of New York State whose Private Information was subject to a Security Breach in the most expedient time possible

and without unreasonable delay, unless such a notification is determined by law enforcement to impede a criminal investigation;

   a. Notice to affected persons under this section is not required if the exposure of Private Information was an inadvertent disclosure by persons authorized to access Private Information, and Northwell Health reasonably determines such exposure will not likely result in misuse of such information, or financial harm to the affected persons or emotional harm in the case of unknown disclosure of online credentials involving a username or password. Such a determination must be documented in writing and maintained for at least five years. If the incident affects over five hundred residents of New York, the person or business shall provide the written determination to the state attorney general within ten days after the determination.

3. The Office of Corporate Compliance will provide any required notice to the affected persons by one of the following methods:

   a. Written notice;
   b. Electronic notice, provided that the person to whom notice is required has expressly consented to receiving said notice in electronic form and a log of each such notification is kept by Northwell Health in such form;
   c. Telephone notification, provided that a log of each such notification is kept by Northwell Health; or
   d. Substitute notice, after demonstrating to the state attorney general the necessary requirements (cost of notice exceeds $250,000 or affected class of persons to be notified exceeds $500,000 or Northwell Health does not have sufficient contact information).

4. Northwell Health's notification to an individual shall include contact information for Northwell Health, the telephone numbers and websites of the relevant state and federal agencies that provide information regarding Security Breach response and identity theft prevention and protection information, and a description of the categories of information that were, or are reasonably believed to have been, accessed or acquired by a person without valid authorization, including specification of which of the elements of Private Information were, or are reasonably believed to have been, so accessed or acquired.

5. In the event that any New York residents are to be notified, the Office of Corporate Compliance shall also notify the State Attorney General, the Department of State and the Division of State Police as to the timing, content and distribution of the notices and approximate number of affected persons and shall provide a copy of the template of the notice sent to affected persons.

6. In the event that more than five thousand New York residents are to be notified at one time, the Office of Corporate Compliance shall also notify consumer reporting agencies as to the timing, content and distribution of the notices and approximate number of affected persons as soon as possible.

7. In the event that a Northwell entity is required to notify the Department of Financial Services ("DFS") of a Security Breach, the Office of Corporate Compliance will notify any resident of New York State whose Private Information was subject to the Security Breach in the most expedient time possible and without unreasonable delay, provided that such notification shall be made within thirty days after the Breach has been discovered, unless such a notification is determined by law enforcement to impede a criminal investigation. Such determination must be confirmed by the Office of Legal Affairs. Subsequent notification will be made by Northwell to DFS, as required by law.

8. If a Security Breach or similar action occurred that impacted individuals outside the State of New York, the Office of Corporate Compliance will work with the Office of Legal Affairs to determine if any other state notifications are required to be sent to the affected individuals and other out of state government agencies.

Connecticut State Security Breach Notifications

If our investigation reveals that a Security Breach affects applicable Private Information of Connecticut State residents, we shall also follow the following procedures:

1. The breach shall be reported to the Connecticut State Attorney General no later than the date on which the affected Connecticut State residents are notified of the breach.

2. If it is believed that the Social Security number or Taxpayer Identification Number of an affected Connecticut State resident was compromised in the breach, the affected Connecticut State resident will be offered 24 months of free credit monitoring services.

Training

The Office of Corporate Compliance will provide training on HIPAA on, at least, an annual basis.

Document Retention

Any documentation generated in compliance with this policy will be retained for a minimum of six years from the date of its creation.

Reporting and Enforcement

All violations of this policy or questions regarding the access, use, disclosure of PHI shall be reported to the appropriate manager/supervisor/director or to the Office of Corporate Compliance (516-465-8097) for appropriate resolution of the matter. The HelpLine is available 24 hours a day, seven days a week at (800) 894-3226 or online at www.northwell.ethicspoint.com, is accessible and allows for questions regarding compliance issues to be asked and for compliance issues to be reported. Reports of potential fraud, waste and abuse and compliance issues also may be made directly to the Chief Corporate Compliance Officer or designee in person, in writing, via email, mobile device via a QR code, or by telephone.

All reports received by the Office of Corporate Compliance are investigated and resolved to the fullest extent possible. The confidentiality of persons reporting compliance issues shall be maintained unless the matter is subject to a disciplinary proceeding, referred to, or under investigation by Medicaid Fraud Control Unit, Office of Medicaid Inspector General or law enforcement, or disclosure is required during a legal proceeding, and such persons shall be protected under the required provider's policy for non-intimidation and non-retaliation.

Violations of this policy will be subject to disciplinary action as outlined in the Human Resources Policy and Procedure Manual and in the Bylaws, Rules and Regulations of the Medical Staff and/or an entity/individual's contract with Northwell Health.

REFERENCES to REGULATIONS and/or OTHER RELATED POLICIES

- Health Insurance Portability and Accountability Act, 45 CFR Parts 160 and 164
- Health Information Technology for Economic and Clinical Health (HITECH) Act, 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 (Feb. 17, 2009)
- Final HIPAA Omnibus Rule (78 Fed. Reg. 5566)
- Human Resources Policy and Procedure Manual, Part 5, Discipline and Standards of Conduct
- Bylaws, Rules and Regulations of the Medical Staff
- New York State General Business Law § 899-aa, including as amended by the Stop Hacks and Improve Electronic Data Security Act ("SHIELD Act"), S5575B
- Conn. Gen. Stat. § 36a-701b
- Northwell Health Policy #100.97 – Records Retention and Destruction
- Northwell Health Policy #900.19 - IT Security Incident Response Policy
- Northwell Health Policy #900.14 – EDS Asset Theft Reporting Policy
- Northwell Health Policy #900.42 – Information Security Program
- Northwell Health Policy #900.28 – Information Security Reviews of Procured Systems

CLINICAL REFERENCES/PROFESSIONAL SOCIETY GUIDELINES
N/A

ATTACHMENTS
N/A

FORMS
N/A

APPROVAL:	
Northwell Health Policy Committee	07/22/2025❖
System PICG/Clinical Operations Committee	07/22/2025❖

Standardized Versioning History:
Approvals: * =Northwell Health Policy Committee; ** = PICG/Clinical Operations Committee; ⊠ = Provisional; ❖ = Expedited

06/11*	07/13**
06/11*	08/13**
12/18/15*	01/21/16**
08/25/16*	09/15/16**
05/24/18*	06/21/18**
❖ 9/26/19	
09/23/21*	10/21/21**
09/26/23*	10/19/23**
05/21/24*	06/20/24**
03/25/25*	04/16/25**