North Shore-LIJ Health System is now **Northwell Health**

POLICY TITLE: HIPAA and State Privacy Breach Notifications	**ADMINISTRATIVE POLICY AND PROCEDURE MANUAL**
POLICY #: 800.17	**CATEGORY:** Compliance and Ethics
System Approval Date: 9/15/16 **Site Implementation Date:** 10/28/16	**Effective Date:** 6/11 **Last Reviewed/Approved:** 1/16
Prepared by: Office of Corporate Compliance	**Superseded Policy(s)/#/Notations:** N/A

GENERAL STATEMENT of PURPOSE

The purpose of this policy 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 has occurred.

POLICY

It is the policy of Northwell Health and Health Plan 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.

SCOPE

This policy applies to all members of the Northwell Health workforce including, but not limited to: employees, medical staff, volunteers, students, physician office staff, and other persons performing work for or at Northwell Health; faculty and students of the Hofstra Northwell School of Medicine conducting Research on behalf of the School of Medicine on or at any Northwell Health facility; and the faculty and students of the Hofstra Northwell School of Graduate Nursing & Physician Assistant Studies.

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:

- The nature and extent of the PHI involved, including types of identifiers and the

likelihood of re-identification;
- The unauthorized person who used the PHI or to whom the disclosure was made;
- Whether the PHI was actually acquired or viewed; and
- The extent to which the risk to the PHI has been mitigated.

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

The term Breach does not include:

- 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
- Any inadvertent disclosure of PHI by a person who is authorized to access PHI at a Northwell Health facility or Business Associate, or organized health care arrangement in which the Northwell Health participates to another person authorized to access PHI at the same Northwell Health facility or Business Associate, or organized health care arrangement in which the 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
- 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.

Protected Health Information or "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 past, present or future physical or mental condition of an individual. 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/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.

Security Breach: an unauthorized acquisition of computerized data which compromises the security, confidentiality or integrity of Private Information.

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

Private Information: any information in combination with any one or more of the following data elements, when either the personal information or the data element is not encrypted, or is encrypted with an encryption key that has also been acquired;

1) Social Security number; or
2) driver's license number or non-driver identification number; or
3) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial 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.

PROCEDURES/GUIDELINES

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 10 days after discovering the Breach.

The Office of Corporate Compliance will coordinate with the Office of Legal Affairs, The Office of Chief Information Officer (OCIO) Security, and Information 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 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 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 Northwell Health website home page 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 **500 or more** individuals of any one state or jurisdiction, in conjunction with the Office of Corporate Compliance Office, 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. See Appendix A.

The Office of Corporate Compliance shall maintain a log of all reported Breaches of Unsecured PHI (See Appendix B) and shall submit required reports of such to the Secretary of HHS 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 the Compliance Director and Privacy Officer assigned to the case, as well as the 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 Director and Privacy Officer to have a meeting with the Corporate Privacy Officer. Any case that is open 40 days or more requires the Compliance Director and Privacy Officer to have an additional meeting with the Chief Corporate Compliance Officer and the Corporate Privacy Officer.

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 and Corporate Security on a weekly basis and other departments, as applicable. Also, Corporate Security shares a report of all incoming cases to their department with Compliance weekly.

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 all Compliance Directors and Privacy Officers, the Chief Corporate Compliance Officer and the Corporate Privacy Officer to ensure all cases that involve the improper disclosure 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 Committee, the Executive Audit and Corporate Compliance Committee, and the Investigations Committee at each meeting.

Audit

In order to ensure all applicable patients and government agencies are notified of an improper disclosure of PHI, the Office of Corporate Compliance will conduct an audit at the end of the reporting year to ensure all 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 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.

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:

- 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;

- The Office of Corporate Compliance will coordinate with the Public Relations Department, or its designee, to notify any resident of New York State whose Private Information was, or is reasonably believed to have been, acquired by a person without valid authorization in the most expedient time possible and without unreasonable delay, unless such a notification is determined by law enforcement to impede a criminal investigation;

- The Office of Corporate Compliance will coordinate with the Public Relations Department, or its designee, to 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);

- Northwell Health's notification to an individual shall include contact information for Northwell Health and a description of the categories of information that were, or are reasonably believed to have been, 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 acquired;

- 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 consumer protection board, and the state office of cyber security and critical infrastructure coordination as soon as possible as to the timing, content and distribution of the notices and approximate number of affected persons (See Appendix C);

- In the event that more than five thousand New York residents are to be notified at one time, the Public Relations Department 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; and

- 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.

Training

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

Sanctions

In compliance with the HIPAA Privacy Rule, 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.

Document Retention

Any documentation generated in compliance with this policy will be retained for a minimum of 6 years from the date of its creation.

Questions related to the access, use, disclosure of PHI should be directed to the Privacy Officer, Office of Corporate Compliance, 516.465.8097.

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
- Bylaws, Rules and Regulations of the Medical Staff
- New York State General Business Law § 899-aa
- Northwell Health Policy #900.19 - Security Incident Management Policy
- Northwell Health Policy #900.14 - IS Asset Theft Reporting Procedure

CLINICAL REFERENCES
N/A

ATTACHMENTS
N/A

FORMS
N/A

APPROVAL:	
System Administrative P&P Committee	8/25/16
System PICG/Clinical Operations Committee	9/15/16

Standardized Versioning History:
*=Administrative Policy Committee Approval; ** =PICG/Clinical Operations Committee Approval
6/11;* 7/13**
6/11;* 8/13**
12/18/15*; 1/21/16**