Corporate Compliance

POLICY TITLE: **Identity Theft Prevention Program**	**SYSTEM POLICY AND PROCEDURE MANUAL**
POLICY #: 800.11	**CATEGORY SECTION: Compliance and Ethics**
System Approval Date: 6/18/18 ❖ **Site Implementation Date: 6/18/18❖**	**Effective Date: 3/26/09** **Last Reviewed/Approved: 5/24/16**
Prepared by: **Office of Corporate Compliance**	**Notation(s):** N/A

GENERAL STATEMENT of PURPOSE

The purpose of this document is to protect patients and Northwell Health from financial loss caused by Identity Theft and to protect patients from having incorrect information included in their medical records as a result of Identity Theft.

POLICY

It is the policy of Northwell Health to take all possible actions to detect, prevent and mitigate the theft of our patients' financial and/or medical identities and to respond quickly and effectively when instances of alleged Identity Theft are reported to Northwell Health or otherwise discovered. Although photographic identification may be required for accurate patient identification, this information is not a part of and shall not be made a part of a patient's medical record. This policy is intended to comply with the Red Flags Rules (72 Fed. Reg. 63718 et seq (Nov. 9, 2007), as amended by 15 U.S.C. 1681m(e)) and the Health Insurance Portability and Protection Act of 1996 and Subtitle D of the Health Information Technology for Economic and Clinical Health Act, which is Title XIII of the American Recovery and Reinvestment Act of 2009 (Public Law 111-5), inclusive of all implementing regulations ("HIPAA").

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 conducting research on behalf of the Zucker School of Medicine

on or at any Northwell Health facility; and the faculty and students of the Hofstra Northwell School of Graduate Nursing and Physician Assistant Studies.

DEFINITIONS

Identifying Information: any name or number that when used individually or in combination with other information identifies a patient, including any name, date of birth, Social Security number or other unique item (e.g., a photograph).

Identity Theft: fraud committed or attempted using the Identifying Information of another person without authority and includes both Medical Identity Theft and Financial Identity Theft. Medical Identity Theft occurs when an individual uses the Identifying Information of another patient to obtain treatment or other services in the name of the patient. Financial Identity Theft may occur when the Identifying Information of a Northwell Health patient, such as a Social Security number, which is contained in such patient's medical record documentation maintained by Northwell Health, is improperly obtained by a third party and used for fraudulent financial purposes, including, without limitation, to obtain or increase credit, open a fraudulent credit card or account or purchase goods or services in the name of the Northwell Health patient without authorization.

Red Flags: a pattern, practice or specific activity that could indicate Identity Theft.

Social Security number: the number issued by the Federal Social Security Administration and any number derived from such number.

PROCEDURE

1. **<u>Circumstances Suggesting Potential for Medical Identity Theft</u>**:

   In the following circumstances, Northwell Health staff will be alerted to the possibility of Medical Identity Theft:

   A. The patient submits a driver's license, insurance card or other identifying information that appears to be altered or forged; or

   B. The photograph on a driver's license or other photo ID card submitted by the patient does not resemble the patient; or

   C. Information on one form of identification submitted by the patient is inconsistent with information on another form of identification, or with information already in Northwell Health's records; or

   D. The Social Security number furnished by the patient has not been issued, is different than the one issued in a previous visit, or is otherwise invalid. The following numbers are known to be invalid:
      - The first three digits are in the 800, 900 or 000 range, are in the 700 range above 772, or are 666;
      - The fourth and fifth digits are 00; or

- The last four digits are 0000; or

E. The address given by the patient does not exist, or is a post office box; or

F. The phone number given by the patient is invalid or is associated with a pager or an answering service; or

G. The patient fails to provide appropriate Identifying Information or documents; or

H. The patient's signature does not match a signature on file in Northwell Health's records; or

I. The Social Security number or other Identifying Information furnished by the patient is the same as Identifying Information in Northwell Health's records furnished by another individual; or

J. Altered or forged credit cards; or

K. Family members or friends call the patient by a name different than that provided by the patient at registration.

L. If information received from the insurance carrier is different than the information supplied by the patient at the time of registration.

M. If a patient calls and states that they are receiving invoices for services they did not have.

If an employee believes that Medical Identity Theft has occurred or may be occurring, the employee must immediately notify the on-site Security Department, which will investigate the matter in accordance with this policy, each other applicable policy of Northwell Health and applicable law and regulation. At the facilities where there is no on-site presence of Security, you may call Corporate Security directly at 516-465-3078.

2. **Verification of Identity of Patient**:

In order to ensure that the patient presenting for treatment is the person the patient claims to be and to preserve the integrity of Northwell Health medical records, Northwell Health will request the following information at time of registration:

- A photo issued by a local, state, or federal government agency (e.g., driver's license, passport, military ID); and
- Date of birth; and
- Residence address and telephone number; and
- Insurance card (if available).

If the patient does not provide a government-issued photo ID, the patient will be asked for two forms of other identification. One form of other identification must be issued by a state or federal agency (e.g., Social Security card). The second form of identification can be a utility bill or company/school identification. Unless required or permitted by law, Northwell Health shall not require a patient to produce or disclose his or her Social Security number.

When the patient is under 18, to produce identification, the patient's legal guardian's identification shall be requested, unless the minor patient is receiving treatment to which the minor patient is legally authorized to give consent, including, but not limited to, treatment related to mental health, alcohol or drug abuse, sexually transmitted diseases, or pregnancy.

A. **No Copying of Photo Identification**. To safeguard the privacy and identity of Northwell Health patients, the photo identification presented by the patient (such as a passport, a driver's license, a non-driver's state identification or military identification card shall not be copied or scanned, unless it is determined the photo identification is necessary for clinically-related identification purposes. In such cases, all non-photo information must be redacted using an appropriate method, such as blocking the non-photo area of the identification card when making a copy or using a permanent black marker.

B. **Requirements for Use of Photo Identification**.

- Northwell Health employees who need to verify a patient's identification shall request photo identification, examine it, verify the identification and then return it to the patient, unless it is determined the photo identification is necessary for clinically-related identification purposes. In such cases, all non-photo information must be redacted using an appropriate method, such as blocking the non-photo area of the identification card when making a copy or using a permanent black marker.
- If a copy of a patient's photo identification is contained in a patient's medical record, the copy shall be removed and disposed of pursuant to the procedures set forth in the Disposal Policy for Protected Health and Confidential Health System Information #800.47, unless it is determined the photo identification is necessary for clinically-related identification purposes. In such cases, all non-photo information must be redacted using an appropriate method, such as blocking the non-photo area of the identification card when making a copy or using a permanent black marker.

C. **Emergency Care – No Delay**. Providing identification is not a condition for obtaining emergency care. The process of confirming a patient's identity must never delay the provision of an appropriate medical screening examination or necessary stabilizing treatment for emergency medical conditions.

D. **Lack of Identification.** No one will be refused care because they do not have acceptable identification with them. Patients will be asked to bring appropriate

documents to their next visit and registration staff may offer to take a photograph of the patient in accordance with any approved registration staff photograph policy. Appropriately document in the EMR or chart that the patient has not provided proper identification.

E. **Refusal to Provide Identification.** If a patient refuses to provide appropriate identification, the supervisor/designee or administrator on-site must consult with a clinician and determine whether it is appropriate to provide medical services or refer the patient to an alternate provider or reschedule the appointment. Unless required or permitted by law, Northwell Health may not refuse to provide services to any patient who refuses to produce or disclose his or her Social Security number. Appropriately document in the EMR that the patient has not provided identification.

F. **Responding to Questions**. If a patient asks for the reason for the identifying procedures, Northwell Health employee shall explain that the procedures are designed to protect the patient and prevent Identity Theft.

G. **Documentation of Identification within the Electronic Registration System**. Staff shall document and confirm their review of the patient's identification in the appropriate field of the applicable electronic registration system. For example, in the Invision patient registration system, staff shall check the box beside "ID Seen," which confirms that they have reviewed the patient's identification documents.

H. **Patient Identifiers in Medical Records**. The patient's name, date of birth and medical record number will be used as primary patient identifiers. If another patient identifier is required, the patient's zip code, gender, city, phone number, middle name or county may be used. If available, the last four numbers of the patient's Social Security number may be used as a patient identifier.

- Whenever a medical record is provided pursuant to a request from outside Northwell Health, the patient's Social Security number must be redacted from the medical record before the record is sent out, unless disclosure of the Social Security number is necessary for payment, as required or permitted by law, regulation or legal process. When redacting a Social Security number, the number must be rendered illegible, which may be accomplished by covering it using a black permanent marker.

3. **<u>Circumstances under which the Health System May Learn of Financial Identity Theft:</u>**

A. Northwell Health may learn of known incidents or allegations of Financial Identity Theft directly from Northwell Health patients or former patients, law enforcement officials, Northwell Health employees, retail and credit card security personnel, among other sources. In accordance with Section 4 of this policy, Corporate Security and Corporate Compliance shall be notified of each incident or allegation of Financial Identity Theft involving or potentially involving Northwell Health.

4. **<u>Responding to Complaints and Suspected Incidents of Identity Theft:</u>**

A. If an individual claims to be a victim of Identity Theft or if Northwell Health otherwise learns or suspects Identity Theft may have occurred at or using the patient records of Northwell Health, Corporate Security, or its designee, will investigate the claim. Corporate Security shall timely notify Corporate Compliance of each incident of suspected Identity Theft. Corporate Security shall be responsible for confirming alleged Identity Thefts and notifying Corporate Compliance of such conclusions.

B. When an individual suspects that he or she may be the victim of Identity Theft, the following procedures shall apply, unless Northwell Health has actual knowledge that Identity Theft has occurred at Northwell Health:

- The individual will have filed a police report for Identity Theft.
- The individual must complete the following documents to the extent feasible:

i. The Identity Theft Victim's Complaint and Affidavit, including supporting documentation. (A copy of the Affidavit is attached as Exhibit A to this policy.)

ii. A written statement including the following information to the extent feasible or they may fill out the attached affidavit:
- A statement that the individual is a victim of Identity Theft and a description of the Identity Theft experienced;
- Any other identification document that supports the statement of Identity Theft;
- Specific facts supporting the claim of Identity Theft, if available;
- A telephone number for contacting the individual;
- A statement that the individual did not authorize the use of his/her name or personal information; and,
- A statement certifying that the representations are true, correct, and contain no material omissions of fact to the best knowledge and belief of the person submitting the certification.

The returned affidavit must be notarized and a copy placed in the non-clinical portion of their chart. A scanned copy of the affidavit will be sent to Corporate Security.

iii. If the Identity Theft suspected is Medical Identity Theft, the written statement will, to the extent feasible, also include the following information:
- An explanation that the individual did not incur the debt;
- Any available correspondence disputing the debt;

- Documentation of the residence of the individual at the date of service, including copies of utility bills, tax statements, or other statements from business sent to the individual at his/her residence; and
- Any information that the individual may have concerning the person who registered in their name.

5. **Medical Identity Theft:**

A. Once a Medical Identity Theft allegation is supported by an ID Theft Affidavit, if applicable, Northwell Health shall flag the account of the patient alleging Identity Theft so that medical personnel are alert to the issue that the medical record may contain inaccurate information about the patient. The Directors of Revenue Cycle and Patient Access, or their designee, shall also notify the applicable HIM Department Director to coordinate flagging the applicable medical records.

B. For alleged Medical Identity Theft patients, as soon as practicable, the HIM Director will place the medical record in a secure location and will place a "Potential Medical Identify Theft Victim" form in the medical record until the allegation of Identity Theft is investigated. See Exhibit B. The "Potential Medical Identity Theft Victim" form will be removed and a "Medical Identity Theft Victim" form will be placed in the medical record if the patient is confirmed to be a victim of medical Identity Theft by Corporate Security. See Exhibit C for a copy of the "Medical Identity Theft Victim" form. If applicable, HIM shall scan the applicable forms into the Electronic Medical Record system.

C. Revenue Cycle will put all patient accounts affected by the confirmed Medical Identity Theft on hold pending the outcome of the investigation.

D. If following investigation, the individual is confirmed to have been a victim of Identity Theft stemming from services received at Northwell Health, Northwell Health will take the following actions:

- Revenue Cycle will cease collection on open accounts that resulted from confirmed cases of Medical Identity Theft. If the accounts had been referred to a designated vendor, the designated vendor will be instructed to cease collection activity.

- Northwell Health will cooperate with any law enforcement investigation relating to the Identity Theft.

- If an insurance company, government program or other payer has made payment on the account, Northwell Health will notify the payer and refund the amount paid, if appropriate.

- Corporate Security will immediately notify the Office of Corporate Compliance. The Office of Corporate Compliance will be responsible for

handling any HIPAA-related or other legal requirements, such as breach analysis and patient notification.

- Northwell Health will provide the patient with Request for Amendment Form, to request modification to their medical record, if applicable.

E. If following investigation, Corporate Security cannot confirm that the individual has been a victim of Medical Identity Theft stemming from services they received at Northwell Health, the Revenue Cycle Department, or its designee, will provide written notice to the individual that he/she is responsible for payment of the bill. Corporate Compliance will notify the HIM Department to remove any notification flags placed on the alleged victim's medical records and the Patient Accounts will be notified to remove flags placed on patients' accounts.

6. **Financial Identity Theft:**

A. If, after the investigation, an incident of alleged Financial Identity Theft appears more likely than not to have resulted from improper use of a patient's Identifying Information contained in the patient's medical record documentation maintained by Northwell Health, Corporate Compliance shall determine whether such incident constitutes a "breach" under HIPAA.

B. If, after the investigation, Corporate Security determines that any alleged Financial Identity Theft of which an individual complained to Northwell Health is unlikely to be related to any services provided by or interaction of the individual with Northwell Health, then Corporate Security or Corporate Compliance, as appropriate, shall inform the individual of such conclusion.

C. Northwell Health will cooperate with any active investigations of law enforcement into alleged and confirmed incidents of Financial Identity Theft.

7. **Handling of Medical Records in Cases of Identity Theft:**

A. Northwell Health will mitigate, to the extent practicable, any harmful effect that is known to Northwell Health as a result of unlawful use or disclosure of Protected Health Information and shall follow Northwell Health's applicable HIPAA policies.

B. If the Corporate Security investigation confirms that a patient record was created as the result of Medical Identity Theft, the "Medical Identity Theft Victim" form will be placed in the medical record.

C. The applicable HIM Department will determine whether any other records are linked to the record found to be created through Medical Identity Theft. HIM shall place the appropriate form concerning the Identity Theft in all such linked records.

D. In some cases, Medical Identity Theft may involve an identity thief receiving care under the name of another person, who has been a patient. In such a case, the patient's file will be reviewed and any information relating to the identity thief will be removed and segregated by the applicable HIM Director, or his or her designee.

8. **Employee Identity Theft:**

When a Northwell Health employee reasonably suspects or knows that Identity Theft has been committed by another employee or any other person or entity, the employee aware of the Identity Theft must immediately notify Corporate Security. Corporate Security will then immediately notify the Office of Legal Affairs and the Office of Corporate Compliance. By the next business day, Corporate Compliance will notify Risk Management and the relevant Executive Director. The Executive Director, or his or her designee, will notify the HIM Director, Registration Director, Human Resources Director, and Patient Accounts Director.

9. **Notifying Victims of Identity Theft When the Patient Does Not Know Identity Theft Has Occurred:**

Victims of Identity Theft will be notified by Corporate Compliance pursuant to all relevant legal requirements. In appropriate cases, the Corporate Compliance shall consult with law enforcement about the timing and the content of any victim notification

10. **Recoveries from Identity Theft Suspect:**

Northwell Health may bill the Medical Identity Theft suspect for unlawfully obtained services. The Office of Legal Affairs must be consulted before pursuing such a claim.

11. **Oversight of the Identity Theft Prevention Program:**

The Identity Theft Prevention Program will be reviewed and updated periodically by the Chief Corporate Compliance Officer, or his or her designee. As part of this periodic review, the Identity Theft Program shall be updated to include additional Red Flags identified by Northwell Health and to incorporate and respond to changes in the risk of Identity Theft at Northwell Health. Material changes to the Identity Theft Program will be reported to the Board of Trustee's Executive Audit and Corporate Compliance Committee, as appropriate. Applicable training for employees regarding Northwell Health's Identity Theft Prevention Program shall be provided on a periodic basis. The training shall include a description of Northwell Health's compliance with the Red Flags Rules and HIPAA as each relates to Identity Theft.

A. **Identity Theft Log:**

- All alleged and confirmed identity theft cases that are reported are tracked in the Identity Theft Log maintained by Corporate Compliance.
- Cases received through our Compliance HelpLine are reviewed weekly to ensure all cases that involve the improper disclosure of PHI are also being tracked on the HIPAA Log and Identity Theft Log.
- The Identity Theft Log is 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.
- Detailed provisions regarding Northwell Health's review and tracking of identity theft logs are described in Northwell Health System Policy # 800.17.

REFERENCES to REGULATIONS and/or OTHER RELATED POLICIES

Red Flag Program Clarification Act of 2010, 15 U.S.C. § 1681m(e) (Dec. 18, 2010)

Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003; Final Rules, 72 Fed. Reg. 63718 (Nov. 9, 2007).

Interagency Guidelines on Identity Theft Detection, Prevention and Mitigation, 16 C.F.R. § 681, appendix A.

Health Insurance Portability and Accountability Act of 1996, Public Law 104-191.

Subtitle D of Health Information Technology for Economic and Clinical Act, which is Title XIII of the American Recovery and Reinvestment Act of 2009, Public Law 111-5.

45 C.F.R. Parts 160 and 164.

Northwell Health Policy #800.17 – HIPAA and State Privacy Breach Notifications

Northwell Health Policy #800.46 - Patients' Rights to Request Confidential Communications, Restrictions, Amendments, and Accountings of Disclosure of Protected Health Information

Northwell Health Policy #800.47 - Disposal Policy for Protected Health and Confidential Health System Information

CLINICAL REFERENCES/PROFESSIONAL SOCIETY GUIDELINES:

N/A

REFERENCES to REGULATIONS and/or OTHER RELATED POLICIES:

N/A

ATTACHMENTS:

N/A

FORMS:

- HS038 Identity Theft Affidavit
- Appendix B- Potential Medical Identity Theft Form
- Appendix C- Medical Identity Theft Victim Form

APPROVAL:	
Northwell Policy Committee	6/18/18 ❖
System PICG/Clinical Operations Committee	6/18/18 ❖

Standardized Versioning History:
*=Northwell Policy Committee Approval; ** =PICG/Clinical Operations Committee Approval

*7/13/10 **9/23/10
*7/25/13 **8/15/13
*11/20/15 **12/17/15
*4/28/16 **5/24/16 (e-vote)

❖ Expedited Approval Granted by:
Winifred Mack, SVP/Operations – Chair, Northwell Policy Committee
Morris Rabinowicz, MD, Co-Chair, - System PICG/Clinical Operations Committee