Origination:	*01/2016*
Effective:	*01/2016*
Last Approved:	*01/2016*
Last Revised:	*01/2016*
Next Review:	*12/2018*
Owner:	*David Behinfar: HCS-Privacy Dir*
Policy Area:	*HIPAA - Privacy*
Policy Tag Groups:	
Applicability:	*UNC Medical Center*

Identity Theft Prevention, Red Flag Program

I. Description

Program Guidelines to identify, detect, and mitigate the potential threats ("red flags") posed by identity thieves using illicitly obtained personal information with the UNC Health Care System.

II. Rationale

The UNC Health Care System recognizes its obligation to establish and administer reasonable measures to detect, prevent, and mitigate identity theft in connection with patient accounts. The Federal Trade Commission's regulations at Part 681 of Title 16 of the Code of Federal Regulations have specific guidelines for achieving this objective through a Red Flag Program. This policy, based on those guidelines, describes UNC Health Care's Red Flag Program and references relevant entity policies and procedures.

III. Policy

A. Definitions

1. Identity Theft: Fraud committed or attempted using the identifying information of another person without authority.
2. Covered Account: (1) In the context of health care services, an account that is designed to permit multiple payments or transactions, or (2) any other account for which there is a reasonably foreseeable risk to account holders or to the safety and soundness of UNC Health Care from identity theft.
3. Red Flag: A pattern, practice or specific activity that indicates the possible risk of identity theft.

B. Procedure

1. **Identified Red Flags for Covered Accounts**
   UNC Health Care staff should note the following "red flags" and follow up and report as indicated in this policy, where warranted:
   a. Presentation of altered, out of date, or otherwise suspicious documentation of identity or financial status, such as insurance, credit, or UNC Health Care Medical Record cards, altered W-2 forms, or photo identification that does not show a reasonable likeness to the person presenting;
   b. Presentation of suspicious personal information, such as:

i. Frequent address or phone number changes

ii. Documents returned for bad address

iii. Information that is not consistent with information on file with UNC Health Care

iv. SSN that is the same as one recorded as in use by another patient or account holder

v. Address or phone number that is similar or identical to that given by other patient(s) or account holder(s);

c. Provision of an insurance number while failing to provide an insurance card or other documentation of coverage, or receipt of notice from the insurer that the patient is not insured;

d. Failure to provide documentation or personal information requested by UNC Health Care in connection with patient registration or as otherwise needed to verify identity or investigate possible identity theft;

e. Receipt of notice from patients, guarantors, law enforcement authorities, victims of identity theft, or other credible sources, regarding identity theft in connection with a covered account; and

f. Discovery of records showing medical treatment that is inconsistent with findings from a physical examination or with a medical history as reported by the patient.

2. **Issues Specific to Patient Financial Services Departments**
Staff of UNC Health Care's Patient Financial Services Departments (UNC Hospitals, UNC Faculty Physicians, and UNC Physician's Network) shall consider the following incidents appearing in their operations, shall perform research sufficient to satisfy concerns of possible identity theft, and if warranted shall report as provided in this Policy:

a. A patient questions or complains regarding his/her receipt of information such as the following:

i. a bill, collection notice, explanation of benefits or credit report for another individual

ii. information regarding a service the patient denies having received

iii. notice from the insurer of denial of coverage because of depletion of benefits or reaching lifetime cap, which the patient asserts is incorrect;

b. A patient disputes a bill, claiming to be the victim of any type of identity theft;

c. Receipt of a notice of inquiry from an insurance fraud investigator for a private insurance company or a law enforcement agency regarding possible identity theft; or

d. Other unusual use of, or suspicious activity related to, a covered account.

3. **Detecting Red Flags**
UNC Health Care staff shall be trained in red flag detection procedures and in reporting responsibilities. Staff shall utilize the following procedures already in place to detect the red flags identified above:

a. Verify identity: at the time of scheduling, registration, check in, or a call in to the Hospital or UNC Faculty Physicians Call Centers, or UNC Faculty Physicians clinics, all patients will be asked for their medical record number and will be requested to answer two questions such as date of birth and address to verify their identity. Patients who cannot provide a medical record number will be asked to provide a social security number and, if they have one, their drivers' license (or other official photo identification) in addition to answering two identity-verifying questions. Upon application for Medicaid, the patient will be required to verify identity and financial status according to Medicaid guidelines for application; and upon application for UNC Charity Care, all patients will be required to verify identity and financial status by submitting required documentation according to the UNC Health Care's

Financial Assistance Policy.

b. Authenticate patients: at the time of scheduling, registration and check in, the medical record number will be used to identify the patient in UNC Health Care's Enterprise Master Person Index (EMPI) and to validate that the information provided by the patient matches the information in the EMPI.

c. Monitor transactions: all transactions will be observed for indications of unusual activity, such as frequent address change, frequent name change, inconsistencies in date of birth, or any other activity that is inconsistent with historical usage.

d. Verify validity of address changes: all bad addresses will be flagged in the GE Enterprise Wide Scheduling System (EWS). In preparation for scheduling, registration, or check-in, the patient will be requested to bring a postmarked utility bill envelope or other type of postmarked business envelope bearing the patient's current name and address.

e. Patient's North Carolina driver's license or other North Carolina issued identification cards may be copied and retained in patient files. However, in accordance with North Carolina State law, copies will only be made in black and white and not color.

4. **Responding to Detected Red Flags**

UNC Health Care staff shall report detected red flags to UNC Health Care's Chief Privacy Officer, or other administrative official designated by amendment to this Policy. Report concerns by calling the Privacy Office at 984-974-1126 or the Confidential Hotline at 1-800-362-2921.

a. Depending on the circumstances presented, the designated official may respond in one or more of the following ways:

   i. Contact the patient

   ii. Notify law enforcement authorities

   iii. Document the incident in a database to determine patterns and frequency

   iv. Determine that no response is necessary.

b. The designated official may also confer with the appropriate department director to effect the following, as appropriate:

   i. Assign a new medical record number to the patient

   ii. Cease collection efforts on the account

   iii. Reopen a covered account with a new account number

   iv. Not open a new covered account

   v. Close an existing account

   vi. Correct medical, payment, and other records of identity theft victims

   vii. Flag records that have been affected by identity theft

   viii. Mitigate, to the extent possible, any harmful effect known to UNC Health Care as a result of identity theft

   ix. Account for an improper disclosure in accordance with UNC Health Care's Privacy/ Confidentiality of Protect Health Information Policy (HIPAA).

5. **Program Administration**

a. Approval of this Red Flag Program was obtained from the UNC Health Care Board of Directors.

IV. Related Policies

UNC Health Care's Information Security Policy
UNC Health Care's Identity Theft Protection Policy
UNC Health Care's Privacy/Confidentiality of Protect Health Information Policy (ADMIN 0139)
UNC Health Care's Confidentiality of Patient Information Policy (ADMIN 0026)
UNC Health Care's Business Associates Policy (ADMIN 0022)
UNC Health Care's Patient Name Identification Policy
UNC Health Care's Medical Information Management Department's Policy on Release of PHI from the Patient's Medical Record
UNC Health Care's ISD Security Administration Policy (p. 53 of ISD Policy Guide)
UNC Health Care's ISD Security Policies (pp. 159-164 of ISD Policy Guide)

Excludes Rex Healthcare and Chatham Hospital

Attachments:

No Attachments

Applicability

UNC Medical Center