

Froedtert & Community Health Policy

Title: IDENTITY THEFT PREVENTION PROGRAM

Policy Type: Corporate

Department: Compliance

Policy Number: FCH-COM.0028

Origin Date: 10/20/2009

Date Revised: 11/1/2009

Supercedes: n/a

Topic(s): Safety / Security

Purpose: The purpose of this policy is to outline a written program to identify relevant red flags, and assist in preventing, detecting, and mitigating the impact of identity theft affecting the patients of Froedtert & Community Health (F&CH).

A. Froedtert & Community Health (F&CH) Affiliate – For purposes of this policy only, F&CH Affiliate includes the following F&CH affiliate organizations: Froedtert Hospital, Community Memorial Hospital of Menomonee Falls, St. Joseph's Community Hospital of West Bend, West Bend Clinic, and West Bend Surgery Center.

B. Identity Theft – When someone, without a person's knowledge, acquires a piece of another person's personal information and uses it without authority.

Definitions: C. Medical Identity Theft – the unlawful use of another person's personal identifying information to obtain medical goods, medical services or to make false claims for medical services.

D. For purposes of this policy, the term identity theft will be used as a term to include either identity theft and/or medical identity theft.

E. Red Flag – indicators of a possible identity theft.

- F. Covered Account – means (i) any account F&CH offers or maintains primarily for personal family or household purposes, that involves multiple payments or transactions, including one or more deferred payments; and (ii) any other account F&CH identifies as having a reasonably foreseeable risk to customers or to the safety and soundness of F&CH from Identity Theft. F&CH has identified the following types of accounts as Covered Accounts:

1. Patient Billing Accounts

- A. F&CH has many corporate and department security and privacy policies that assist in the detection, prevention, and mitigation of identity theft. The framework of these policies and practices, when taken together, encourage appropriate handling of protected health information which provide safeguards against identity theft (please refer to the Corporate Policy and Procedure Manual on the Intranet/Shared Drive for complete listing).
- B. F&CH will strive to prevent the intentional or inadvertent misuse of patient names, identities, and medical records.
- C. F&CH will take steps to prevent, detect, and mitigate identity theft.
- D. F&CH will report any criminal activity relating to identity theft to the appropriate authorities.
- E. For patients seeking the evaluation and treatment of an emergent medical condition, the provision of a medical screening examination will not be delayed or refused in order to obtain documents or information verifying their identity.

Policy:

A. Identification of Red Flags:

1. The “F&CH Identity Theft Red Flags” (Attachment A) are those red flags that have been determined to be the most applicable and appropriate for F&CH. These red flags fall within one of the following categories:
- a. Suspicious Documents
 - b. Suspicious Personal Identifying Information

Procedure:

- c. Suspicious or Unusual Use of Covered Account
 - d. Notice from Patients, Victims of Identity Theft, Law Enforcement or Others about possible identity theft in connection with Covered Accounts.
2. A “Confirm ID” flag will be placed on a patient’s record to help alert staff that photo identification is needed from the patient. The reason the flag is on the account is because there is some suspicion or discrepancy related to the identity of the patient. The “Confirm ID” Patient Flag (Patient Type) is located in either Epic Cadence/ Prelude, or in the Invision application. (computer system location is dependent upon which facility system you access).

B. Prevention and Detection of Identity Theft:

Registration & Intake Process

1. **F&CH Emergency Departments (ED) and Inpatient Registration Procedure:**
- a. Use the following script with patients: In effort to protect our patients from identity theft, it is our policy to ask to see a form of photo identification from each patient.
 - b. Request patient to provide a form of photo identification (preferably a government issued form of identification).
 - (1) Validate the photo looks like patient.
 - (2) Use ID to verify against our system, the correct spelling of the name, date of birth and address.

- c. Request patient to provide his/her insurance card, according to the facility's organizational policy and verify the information with the appropriate billing system.

- d. If the patient does not provide a photo ID, ask the patient to answer the following questions, which will help to validate the identity and demographics of the individual. Do not read the demographic information to them, ask the patient to answer the following questions:
 - (1) What is your date of birth?
 - (2) What are the last four digits of your social security number?
 - (3) What is your current home address?

Remind the patient to bring a photo ID to their next visit.

- e. If the patient does not have photo identification, and provides inconsistent information upon questioning, you may proceed with the registration process.
 - (1) Patients will not be refused care because they do not have acceptable identification, or if they provide inconsistent demographic information.
 - (2) Instruct the patient to bring photo identification to their next visit.
 - (3) Report the event to the F&CH Compliance Department as defined in the "Mitigation" section of this policy.

**2. F&CH Outpatient Departments & Other Intake Area's Procedure:
(this does not include the Emergency Departments)**

a. New Patients to the F&CH facility:

- (1) Use the following script with patients: In effort to protect our

patients from identity theft, it is our policy to ask to see a form of photo identification from each patient.

(2) Request a form of photo identification (preferably a government issued form of identification)

- a. Validate the photo looks like patient.
- b. Use ID to verify against our system, the correct spelling of the name, date of birth and address.

(3) Request patient to provide his/her insurance card, according to the facility's organizational policy, and verify the information with the appropriate billing system.

(4) If the patient does not provide a photo ID, ask the patient to answer the following questions, which will help to validate the identity and demographics of the individual. Do not read the demographic information to them, ask the patient to answer the following questions:

- a. What is your date of birth?
- b. What are the last four digits of your social security number?
- c. What is your current home address?

Remind the patient to bring a photo ID to their next visit.

b. **If the "Confirm ID" Patient Flag (Patient Type) is present in Cadence/Prelude or Invision:**

(1) Follow procedures above in steps a (1-4).

- (2) If the patient provides the necessary photo identification and insurance card, photocopy it and forward to the F&CH Compliance Department. Include your name, contact information and an explanation that the confirm ID flag was listed on this patient and that they have provided the necessary photo ID to confirm their identity. The Compliance Department will be responsible for removing the Patient Flag from the account.

- (3) If the patient does not have photo identification, does not provide an insurance card, or there is reason to believe the patient may be providing false information, the registration/check-in staff should follow the department policy on whether the appointment should be cancelled and rescheduled, or whether they should proceed with allowing the patient to be seen.
 - a. If the clinic/department allows the patient to be seen:
 - (i) Instruct the patient to bring photo identification to their next visit.
 - (ii) Report the event to the F&CH Compliance Department as defined in the “Mitigation” section of this policy.

 - b. If the clinic/department’s policy is to cancel the patient’s appointment:
 - (i) Explain to the patient that, we apologize for the inconvenience, but it is our policy to validate identification prior to seeing them.
 - (ii) Report the event to the F&CH Compliance Department as defined in the “Mitigation” section of this policy.

 - c. **For Established or Known Patients to the Clinic/Department:**

- (1) If there is no “Confirm ID” in Cadence/Prelude/Invision, and the person completing the registration is familiar with the patient, they do not need to ask for photo identification and insurance information at each visit.

- (2) It is still good business practice to ask the following questions to verify that we have selected the correct patient:
 - a. What is your date of birth?

 - b. What is your current home address?

- (3) Continue to follow regular registration / check in procedures.

C. Mitigation of Identity Theft:

1. Reporting Identity Discrepancies or Potential Identity Theft

- a. Staff members or hospital/clinic service providers should promptly report discrepancies/red flags as signs of potential identity theft. Refer to Attachment A for a list of red flag examples.

- b. All reports of identity theft, discrepancies or red flags should be promptly reported to the F&CH Compliance Department. The following are the methods by which to report the issue:
 - (1) Email the “Froedtert Compliance Hotline” at comphotl@fmlh.edu. Include the following information in the email:

- a. Staff Name and Contact Information
- b. Patient Name and Medical Record Number
- c. Explain the circumstances of the identity discrepancy or suspected identity theft include pertinent dates, times and locations; or

(2) Complete an Incident Report, Event Report, or QA Variance Report (name of report is as applicable to individual facility). If applicable, select Identity Theft as the category. Include detailed information in the incident report, including:

- a. Staff Name and Contact Information
- b. Patient Name and Medical Record Number
- c. Explain the circumstances of the identity discrepancy or suspected identity theft, include pertinent dates, times and locations.

(3) The F&CH Compliance Department will investigate all identity theft warnings received.

- c. All communication with patients, victims of identity theft, law enforcement or others about potential identity theft in connection with covered accounts should be addressed under the direction of, or in consultation with, the F&CH Compliance Department.

2. Updating the Program

- a. F&CH will evaluate the effectiveness of the program periodically and will update the program as necessary to reflect changes in risks to patients or to the hospital/clinic from identity theft, based on factors such as:

- (1) The experiences of the hospital/clinic with identity theft;
- (2) Changes in methods of identity theft;
- (3) Changes in methods to detect, prevent, and mitigate identity theft;
- (4) Changes in the types of accounts that F&CH offers or maintains; and
- (5) Changes in the business arrangements of F&CH, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

3. Program Administration

- a. The Chief Compliance Officer of F&CH shall assume primary administration of the program, subject to oversight and approval by the Finance Committee of the Board of Directors.
- b. The program effectiveness, significant incidents involving identity theft, and any material changes to the program will be reported to, and monitored by the Chief Compliance Officer.
- c. Any modification or amendment to this policy shall be adopted and approved by the Chief Compliance Officer.

4. Training

- a. Staff identified as responsible for following the Identity Theft Program Policy will be trained on the applicable requirements.

5. Service Provider Arrangements

- a. Whenever F&CH engages a service provider to perform an activity in connection with one or more covered accounts, the service provider will by contract, be required to have an identity theft prevention program in place that is in compliance with all federal rules and regulations and includes policies and procedures designed to prevent, detect and mitigate red flags for identity theft.

- b. Service providers will report to F&CH, any relevant red flags that may arise in the performance of activities, and shall take appropriate steps to prevent or mitigate identity theft.

All applicable F&CH Staff Members

Scope:

F&CH Corporate Policy & Procedure Manual

Distribution:

_____ Date: 10/19/09
Nancy Schallert, Director-Corp.Compliance & Audit
Froedtert & Community Health

_____ Date: 10/20/09
Mary Wolbert, VP-Chief Compliance Officer
Froedtert & Community Health

_____ Date: 10/20/09
Authorization: Blaine J. O'Connell , Sr. VP, Chief Financial Officer
Froedtert & Community Health

_____ Date: 10/21/09
William D. Petasnick, Chief Executive Officer
Froedtert & Community Health

Approved by the F&CH Finance Committee: 10/19/2009

Attachment A- FCH-COM.0028 Identity Theft Prevention Program

All staff members or hospital/clinic service providers should report the following occurrences as signs of potential identity theft:

- a) A patient presenting photo identification that does not look like the patient.
- b) You know or recognize the patient under a different name.
- c) A patient giving a social security number different than the one used on a previous visit or is listed as belonging to another person.
- d) A patient giving information that conflicts with information in the patient's file or received from third parties, such as insurance companies.
- e) A complaint or question from a patient about a bill or collection notice for services that they claim they did not receive.
- f) Records showing medical treatment that is inconsistent with a physical exam or medical history of the patient.
- g) A complaint that coverage for legitimate hospital/clinic services is being denied because insurance benefits have been depleted, but patient denies the use of these services.
- h) A complaint from a patient about information added to a credit report by a health care provider.
- i) A notice or inquiry from an insurance fraud investigator or law enforcement agency.
- j) A fraud, active duty alert, or credit freeze is included with a consumer report.
- k) The hospital/clinic receives notice of address discrepancy from a third party or repeatedly has mail returned.
- l) Documents provided for identification appear to have been altered or forged.
- m) It has been reported that there has been a stolen, missing, or lost portable device that may have had patient names on it.
- n) Hospital/clinic receives notification that a staff member or contracted vendor has been accessing hospital/clinic information to perform identify theft.
- o) Hospital/clinic identifies that the security of PHI has been compromised through unauthorized access or disclosure.

Attachments:

p) Patient states their identity has been stolen.