Geisinger

IDENTITY THEFT PREVENTION PROGRAM – RED FLAGS RULE POLICY

PURPOSE

To establish an Identity Theft Prevention and Detection Program designed to detect, investigate and mitigate potential identity theft without impacting appropriate care of patients or compliance with other laws and to cause all business associates to report and respond to red flags which may indicate the possibility of identity theft. This policy establishes procedures for employees to follow to ensure a patient's medical and financial records are protected in compliance with various state and federal laws.

PERSONS AFFECTED

This policy applies to all employees of the Geisinger Health System and all vendors working on site who have direct or indirect patient contact.

POLICY

Geisinger will implement and maintain a program to detect and respond appropriately to red flags that might suggest consumer identity theft. Geisinger will take appropriate measures for disclosure and monitoring of such activities and will educate its employees concerning identity theft and appropriate procedures.

Geisinger will also take steps to ensure that any service providers engaged to perform activity in connection with any covered accounts conduct that activity in accordance with reasonable policies and procedures designed to detect, prevent and mitigate identity theft.

Activities related to this program will be communicated at least annually to Geisinger's Compliance Committees as applicable.

This program shall be reviewed annually and updated as warranted to reflect changes in risk to customers or to the safety and soundness of the organization and the customers it serves.

DEFINITIONS

Business Associate: A person or entity that provides services directly to Geisinger and that is in a position to identify and report a red flag to Geisinger in the normal course of business.

Consumer Reporting Agency: The agency -- whether Experian, Equifax or TransUnion—that collects and sells information regarding the creditworthiness of a particular individual.

Covered Account: A consumer account designed to permit multiple payments or transactions (i.e. installment account), and any other account for which there is a reasonably foreseeable risk of identity theft.

Identifying Information: Any name or number that may be used, alone or in conjunction with any other information, to identify a patient, including, but not limited to, address, social security number, date of birth, driver's license, passport, biometric data such as fingerprint, voiceprint or other unique physical characteristic.

Identity Theft: Fraud committed or attempted using the identifying information of another person without authority.

Red Flag: A pattern, practice or specific activity that indicates the possible existence of identity theft including, but not limited to, the following:

- A consumer report indicates a pattern of suspicious activity.
- A fraud alert is included with a consumer credit report.
- Document identification issues or presentation of altered or suspicious documents.
- Personal information inconsistent with external or internal information sources. For example, address provided does not match consumer report or address on file, Social Security Number is invalid or listed on the Security Administration's Death Master File, lack of correlation between Social Security Number range and date of birth, personal information provided matches that of a known fraudulent application, fictitious address or telephone number provided, authenticating information cannot be provided beyond that available from a wallet or consumer report.
- Unusual use of or suspicious activity related to a covered account.
- Notice from the customer, financial institution, victim of identity theft, law enforcement or internal sources regarding possible identity theft.
- Patient's appearance changes drastically or does not match identification on file.

RESPONSIBILITIES

Finance, Revenue Cycle, Risk Management, Legal Services, Information Security Office

EQUIPMENT/SUPPLIES

Not applicable

PROCEDURE

DETECTION OF RED FLAGS

A. Patient Registration: ***Except in the case of an emergency***, any time a Patient registers with Geisinger to receive health care services, whether as a new or returning patient, Geisinger staff shall:

- Ask for photo identification and current insurance card– for all new patients at the first visit and for all returning patients once every 4 years. Scan a copy of the same into the medical record and compare patient with picture identification on record.
- Ask the patient to verify their current address (make them state their address - do not read it to them and ask if correct).
- Ask the patient for any other identifying information necessary to update the record.
- Review the patient record for the existence of any alerts, notifications or warnings received from a consumer protection agency.

B. Registrars, Health Care Providers and all other Geisinger Employees:

1. **Interactions with Patient and/or Medical Record**

All Geisinger employees should be alert for Red Flags when interacting with a patient or the patient's medical record, including, but not limited to, any suspicious documents or other identifying information, such as the following:

- Documents that appear to have been altered or forged.
- Documents that contain a photograph that is not consistent with the patient's current appearance.
- Documents that contain information that is inconsistent with other identifying information provided by the patient or inconsistent with what is already in the record.
- The Social Security Number furnished by the patient has not been issued, is listed on the Social Security Administration's Death master File, or is otherwise invalid. The following numbers are always invalid:
    - The first three digits are in the 800 or 900 series or "000"
    - The fourth and fifth digits are 00
    - The last four digits are 0000

- The patient's signature does not match a signature already on file.
- The Social Security Number or other information provided is identical to that being used by another patient already in the system.
- The patient looks like a different person from the last visit or has made an impossible physical change since the last visit (such as gaining 100 pounds in one week or shrinking 6 inches).

2. **Notification from Patient or Other Third-Party Purporting to Be Victim of ID Theft**

If a patient or other person reports to be the victim of identity theft (i.e., they received a bill for services they did not receive or their medical record contains information concerning services, diagnosis, etc. that they did not receive), then notify the Information Security Office immediately.

C. Procedure to Follow if Identity Theft is Suspected

If you suspect identity theft, you should step away from the patient (as applicable) and immediately notify your supervisor. In order to prevent or mitigate identity theft, you or your supervisor may ask for more identifying information and/or question the patient about any discrepancies or inconsistencies. If you and your immediate supervisor still suspect potential identity theft, the Information Security Office should be notified immediately. You may, in your discretion call security and/or the police. As far as treatment of the patient, the supervisor and the treating physician should decide whether: (1) to see the patient but inform him/her that next time they will be required to bring in additional documents to prove their identity and until such time, their file will be marked accordingly; or (2) to cancel the appointment and reschedule pending the outcome of the investigation. All patients should be instructed to visit the emergency room in case of an emergency.

EXCEPTION: If the patient has come to the hospital to request evaluation or treatment of an emergency medical condition, the provision of the medical screening examination shall not be delayed to obtain documents or verify identity pursuant to the Emergency Medical Treatment and Active Labor Act ("EMTALA").

D. Revenue Cycle Operations & Identity Theft in Connection with Installment or other Financial Accounts

1. Revenue Cycle staff shall conduct business in compliance with all organizational and departmental compliance and anti-fraud program provisions.
2. Revenue Cycle staff shall conduct business in compliance with all Information Security Program guidelines.
3. Revenue Cycle staff shall verify the patient's identity through the exchange of questions and answers between the staff member and the customer. The following identifiers are used to authenticate the patient's identity:
    a. Full Name
    b. Date of Birth
    c. Address
    d. Phone Number
    e. Full Social Security Number (last four (4) digits acceptable). Patients reluctant to verbalize their Social Security Number shall have the option to write down this information. Patients unwilling or unable to provide a Social Security Number shall not be required to do so.
4. As installment accounts (payment plans) are established, an initial payment is required and a receipt or confirmation number for that payment is sent or provided to the guarantor on file or to the person making the payment.
5. Suspicious activity and any red flags must be reported to the respective Revenue Cycle designee. Revenue Cycle shall perform a preliminary review of the account in question prior to referral to the Information Security Office.
6. The Revenue Cycle designee will respond to the suspicious activity or red flags as warranted by the particular facts of each case. Responses could include, but are not limited to, the following:
    a. Heightened monitoring of the covered account;
    b. Reopening the covered account with a new account number;
    c. Determine that no response is warranted under the circumstances.

E. Business Associate Notification

All Business Associates shall be notified in writing of this Policy. All Business Associates whose employees will be on-site or who otherwise have access to Protected Health Information must either implement their own Red Flag policy or agree to abide by this Policy. Exceptions to this requirement can only be granted with Legal approval.

INVESTIGATION AND HANDLING OF RED FLAGS

A. Upon suspicion that an established patient's identity has been fraudulently used to obtain care at GHS the following steps shall take place:

1. The Information Security Office should be notified immediately.
2. The Information Security Office shall notify Risk Management, Revenue Cycle and the Legal Services Department of the possibly fraudulent conduct.
3. The Information Security Office shall investigate the patient account in question.
4. The Information Security shall notify Legal Services, Risk Management and Revenue Cycle of their investigative outcomes.
5. Upon notification of suspected identity theft involving a Geisinger patient, the Manager of the Health Information Management Department ("HIM") shall place an identity theft flag on a patient's chart as necessary to alert subsequent health care providers that the record is or may be subject to identity theft and contains or may contain information

concerning the health care of another individual. If the Manager is not available, then the Supervisor of Medical Reports in HIM should be asked to place the flag, and if neither of the above are available, then the Director of HIM should be asked to place the flag.

6. Based on the facts of the case and the outcome of the internal investigation, Legal Services shall decide what action Geisinger will take in terms of notifying various regulatory agencies including local law enforcement.
7. Based on the facts of the case and the outcome of the internal investigation, Legal Services together with other applicable departments within Geisinger, including the Privacy Office, will determine whether the patient should be notified so that (a) Geisinger can comply with relevant laws and its HIPAA policy, and (b) the patient may institute procedures to decrease the risk of any unauthorized access to, use or disclosure of their Identifying Information which may result in identity theft.
8. Based on the facts of the case and the outcome of the internal investigation, HIM may remove the identity theft flag on a patient's chart if there has been no identity theft OR keep the identity theft flag on a patient's chart and mark all the pages of a patient's medical record that don't pertain to that patient through the approved corrections process and/or EHR policy committee review if there has been identity theft.
9. Patient Access shall attempt to obtain photo identification at the time of registration.
10. The appropriate insurance collections unit shall inform customer's insurance, issue insurance refunds where appropriate and perform Administrative Adjustments on the fraudulent charges.

B. If a patient or other person reports to be the victim of identity theft (i.e., they received a bill for services they did not receive or their medical record contains information concerning services, diagnosis, etc., that they did not receive), the following guidelines apply:

1. Notify the Information Security Office.
2. The Information Security Office shall confirm all facts and circumstances with the person as to why they think they are a victim of identity theft.
3. Instruct the person to notify the police for purposes of obtaining a police report and further instruct the person to provide Geisinger with a copy of the police report.
4. Information Security Office, Risk Management and Legal Services shall otherwise proceed as set forth above.