

SOUTH SOUND RADIOLOGY POLICY/PROCEDURE

POLICY: IDENTITY THEFT PREVENTION PROGRAM- "RED FLAG RULE"

AUTHOR: John Stanley

Date: 12/31/08

Overview:

The Federal Trade Commission's implementation of the Fair and Accurate Credit Transactions (FACT) Act of 2003 requires medical providers to comply with the "Red Flag" rule by June 1, 2010. The FTC maintains that health care providers are considered creditors and are required to establish a program to prevent identity theft in their practices. Patient billing records are considered by the FTC to be "covered accounts".

Red Flags are indicators of possible risk or identity theft. South Sound Radiologists Inc. P.S. employees shall follow the Identity Theft Prevention Program to assist in identifying potential risks within the facility and to identify individuals that may be utilizing techniques related to identify theft. The idea is that if everyone is sensitive to identify theft it will be more difficult for criminals to perpetrate crimes using other individual's identities.

Purpose:

To ensure appropriate handling of all new and existing patients covered accounts in order to reduce the potential for identity theft for our clients.

1. Prevent relevant patterns, practices, or activities that are "red flags" signaling possible identity theft.
 - a. All discarded/disposed material containing patient information shall be shredded using internal shredding devices or the contracted shredding service.
 - b. All staff will use individual log-on's and passwords to enter computer software containing patient information.
 - c. Automatic log off's will be enabled on computers with access to patient information.
 - d. The public will not have access to computer data or paper data with consumer information unrelated to their own account(s). (See HIPAA Policies)
 - e. Personal information will not be shared via telephone or computer unless receiver is verified by the staff member.
 - f. All questionable activity will be handled by supervisor or the administrator, staff shall document and direct any questionable activity relating to potential identity theft to the supervisor and/or administrator.
 - g. Staff will verify Identification on all accounts at time of registration.

2. Identify areas of concern. They include the following:
 - a. Address discrepancy
 - b. Name discrepancy on insurance and ID
 - c. Presentation of suspicious documents
 - d. Personal information inconsistent with information on file
 - e. Unusual or suspicious activity related to an account.
 - f. Appearance of altered ID

- g. Any warning from law enforcement or consumer reporting agency related to a specific account.
 - h. Person demanding services or access to health records with unusual urgency or frequency.
3. Any of the above patterns or practices or activities should be reported to the immediate supervisor.
 - a. A report will be written up.
 - b. Assessment of potential danger will occur.
4. These incidents will be reported to the administrator.
 - a. A written incident report will be turned in
 - b. The administrator will discuss the issue with Executive Committee to decide how to respond to the potential threat.
5. After such incidents, the management personnel will meet to discuss how we can improve our security and prevent any further problems.

Red Flag Examples

- Alerts, notification, or other warnings received from consumer reporting agencies or service providers (credit card processors, etc).
- Presentation of suspicious documents:
 - Documents provided for identification appear to have been altered or forged.
 - The photograph or physical description on the identification is not consistent with the appearance of the individual presenting the identification.
 - Other information on the identification is not consistent with information provided.
 - Other information on the identification is not consistent with readily accessible information that is on file with the practice.
- The unusual use of, or other suspicious activity related to, a covered account:
 - The practice is notified of unauthorized charges or transactions in connection with a patient's covered account.
- Notices from patients, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the practice.
 - The practice is notified by patient, victim of identity theft, a law enforcement authority, or any other person that the practice has an account for a person engaged in identity theft.