October 2008

MEMBER BRIEFING

HEALTH INFORMATION AND TECHNOLOGY PRACTICE GROUP

Red Flag Compliance for Healthcare Providers: Protecting Ourselves and Our Patients from Identity Theft

Patricia King, Esquire
Swedish Covenant Hospital
Chicago, IL

Rebecca L. Williams, RN, JD
Davis Wright Tremaine LLP
Seattle, WA

TABLE OF CONTENTS

On November 9, 2007, the Federal Trade Commission (FTC), in conjunction with other agencies, published the Red Flag Rules defining what a creditor and financial institution must do to implement an Identity Theft Prevention Program.[1] The Red Flag Rules require those covered to identify at risk accounts and to define, detect, and respond to Red Flags to prevent or mitigate identity theft. A "red flag" is a suspicious circumstance that should prompt the financial institution or creditor to be alert for possible identity theft. If identity theft is detected, then the financial institution or creditor must take appropriate steps to mitigate the harm. The Red Flag Rules also mandate oversight and administrative requirements. Moreover, a creditor that uses consumer reports must take certain actions to respond to discrepancy notices from a consumer reporting agency. The compliance date for the Red Flag Rules is November 1, 2008.

A goal of the Red Flag Rules is to help detect identity theft sooner. Consumers cannot do it all on their own, especially when the thief uses the stolen information to open a new account. Consumers cannot protect against new account fraud solely by vigilantly reviewing transactions in existing accounts; they can learn about this type of fraud only by picking it up from a credit report. **According to the FTC, 24% of victims of fraud involving new accounts did not find out about it until six months after it started.**[2] Because the potential loss from identity theft increases as the theft remains undetected, new account fraud is a very costly type of identity theft.

Many in the healthcare industry were surprised to discover that the Red Flag Rules actually may apply to them. Most identity theft laws and rules apply mainly to financial institutions, such as banks and credit unions. The Red Flag Rules were published simultaneously by the Department of the Treasury, the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, and the FTC. Although most of these agencies do not have jurisdiction over healthcare providers, the FTC's Red Flag Rules can apply to us. This Member Briefing is written to help healthcare

providers determine whether they are subject to the Red Flag Rules and, if they are, help them create a written Identity Theft Prevention Program.

Healthcare providers and others that meet the qualifying criteria will need to comply with the Red Flag Rules. At the same time, healthcare providers must comply with many other laws specific to the healthcare industry. For example, most healthcare providers already must comply with the administrative simplification provision of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing privacy and security standards, which have significant overlap with the requirements of the Red Flag Rules. Hospitals also are obligated under the Emergency Medical Treatment and Labor Act (EMTALA) to provide a medical screening for anyone seeking emergency medical care, without delaying the screening to obtain registration information. Therefore, healthcare providers must be careful to craft their Identity Theft Prevention Program in a way that helps detect identity theft, without running afoul of other regulatory requirements.

A. The Crisis of Identity Theft

We have all become much more aware of the threat that identity theft poses to our personal finances. A report prepared for the FTC in 2007 estimates that 8.3 million Americans were victims of identity theft in 2005.[3] New identity theft scams that can leave us with damaged credit—and take time and money to fix—constantly are evolving. According to the FTC, identity thieves can use personal information in a number of ways to defraud businesses and service providers and to destroy the reputation and credit standing of identity theft victims, including changing the billing address on a credit card account and then running up charges on the account, opening new credit card accounts in the victim's name and not making payments, establishing phone or wireless service in the victim's name, taking out a car loan, filing bankruptcy, counterfeiting checks, acquiring a driver's license, filling out job applications all in the victim's name, and even providing the victim's name to police during an arrest.[4]

The results of identity theft can be devastating to consumers in terms of damage to their credit, lost time, stolen funds, and out-of-pocket expenses

incurred. Identity theft hurts businesses as well. The company that opened an account, set up utility services, approved a loan, or honored a check for an identity thief most likely will bear much of the financial loss. In many cases, consumers are not responsible for debts incurred in their name due to identity theft.[5] Helping to prevent and detect identity theft is not merely a matter of good citizenship for businesses; they have a direct financial stake in preventing the write-offs that result from this fraud.

B. What Is Different About Medical Identity Theft?

Here is how the World Privacy Forum defines medical identity theft:

> Medical identity theft occurs when someone uses a person's name and sometimes other parts of their identity—such as insurance information—without the person's knowledge or consent to obtain medical services or goods, or uses the person's identity information to make false claims for medical services or goods. Medical identity theft frequently results in erroneous entries being put into existing medical records, and can involve the creation of fictitious medical records in the victim's name.[6]

Identity theft takes a particularly nasty turn in healthcare. First, the potential financial loss tends to be much greater. According to the FTC's 2006 identity theft survey, the median amount obtained by identity thieves for all types of identity theft was $500.[7] In contrast, physicians, hospitals, and others who provide care in good faith can find themselves responsible for thousands of dollars when the patient they have helped turns out to have stolen another's identity. In one egregious recent example, a man needing cardiac surgery was able to get healthcare services totaling $350,000 from a local hospital, using a friend's identity.[8]

A victim of medical identity theft has to contend with the problems common to all identity theft victims: the time, financial harm, out-of-pocket expense, and worry of placing fraud alerts, closing accounts, and replacing

identification. Beyond these time and money issues, the victim also has to worry that his or her medical history can be confused with that of the thief. In the extreme, medical identity theft can prove fatal.

A report in *Business Week* described the dilemmas encountered by a woman whose identity was stolen by a thief who used it to obtain surgery. After sorting out the financial claims, the victim found her problems were not over:

> When Weaver was hospitalized a year later for a hysterectomy, she realized the [identity thief's] medical info was now mixed in with her own after a nurse reviewed her chart and said, "I see you have diabetes." (She doesn't.) With medical data expected to begin flowing more freely among healthcare providers, Weaver now frets that if she is ever rushed to a hospital, she could receive improper care—a transfusion with the wrong type of blood, for instance, or a medicine to which she is allergic.[9]

Identity theft can cause substantial losses to healthcare providers. The healthcare provider probably will not find out about the identity theft until after services have been provided. An alert consumer may spot an unfamiliar entry on an Explanation of Benefit (EOB) from the consumer's insurance company and notify the insurer. Of course, once the insurer or health plan that paid for the service learns that the person receiving it was not covered, it will demand a refund from the provider. If the consumer does not scrutinize his or her EOBs, then it is possible that the fraud will not be uncovered until the personal portion of the account is sent for collection. The individual whose identity was stolen will refuse rightfully to pay because he or she did not receive the services.

The FTC has recognized that healthcare providers are most likely to run into potential identity theft at the time a new account is created (i.e., when we register a new patient).[10] Since new account fraud typically takes longer to detect than fraud involving existing accounts—and the longer it takes to detect the

fraud, the greater the potential loss—this is one of the most dangerous types of identity theft.

We probably have not heard the last about what the healthcare industry will be expected to do to combat medical identity theft. The U.S. Department of Health and Human Services (HHS) and the FTC, among others, have expressed concern about the topic, and particularly how it will affect electronic healthcare information.[11]

C. The Law's Response to the Identity Theft Crisis

The federal government has fought back against identity thieves with two different types of tools: rules that seek to prevent identity theft by increasing protections for confidential information and measures to help consumers detect the crime at an earlier stage. The first type of tool is directed at organizations that hold confidential information and seeks to prevent unauthorized disclosure of confidential information, security breaches through improper disposal of confidential information, and other risks to the confidentiality and integrity of information.

A major tool for protection of confidential information in the financial world has been the Financial Modernization Act of 1999, commonly known as the Gramm-Leach-Bliley Act (GLB Act).[12] Among other things, the GLB Act requires that financial institutions take several actions to protect the privacy and security of consumers' personal information.

In many ways, the GLB Act is the counterpart in the financial world to HIPAA.[13] As we know, HIPAA requires that health plans, healthcare clearinghouses, covered healthcare providers, and sponsors of Medicare prescription drug cards must implement safeguards to protect the privacy of individually identifiable health information and the security of electronic protected health information. Although HIPAA focuses on confidential health information, HIPAA compliance also helps prevent identity theft. "Protected health information" is defined broadly to include identifiable demographic information and information that relates to payment for healthcare services (in addition to information about an individual's condition and treatment.)[14] Healthcare

providers' records typically contain not only medical information, but also information useful for identity theft, such as date of birth and social security numbers. Accordingly, at least some protected health information needs to be protected in a way to reduce the risk of identity theft.

Besides requiring that organizations holding confidential information must keep the information secure, another way to attack the identity theft problem is to make it easier for consumers to detect it when it has occurred. **The longer the identity theft remains undetected, the greater the problem can become for the consumer.** According to the FTC's 2006 identity theft survey, where the identity theft went undiscovered for six months or more, 31% of the time the thief stole more than $5,000, compared with 10% when the theft was discovered sooner.[15]

The Fair and Accurate Credit Transactions Act of 2003 (FACTA)[16] imposes substantial obligations on credit card issuers, consumer reporting agencies, and financial institutions and also includes some provisions that apply to any creditor. Many provisions of FACTA (e.g., the right of consumers to free credit reports) have been in effect for years and include several provisions directed both at prevention and detection of identity theft—including, among other things, requiring consumer reporting agencies to include a fraud alert in a consumer's file for 90 days after the consumer's good-faith allegation of identity theft (the one-call fraud alert) and mandating consumer reporting agencies, upon request of a consumer who files an identity theft report or the FTC-approved affidavit of identity theft, to include the fraud alert in the consumer's file for seven years (unless the consumer requests removal).

FACTA amended the Fair Credit Reporting Act (FCRA)[17] and mandated the promulgation of identity theft regulations. In response, the FTC and several other federal agencies jointly issued the Red Flag Rules and guidelines[18] governing the detection, prevention, and mitigation of identity theft by financial institutions and creditors.[19]

On November 9, 2007, the agencies published in the *Federal Register* final Red Flag Rules that took effect January 1, 2008, requiring organizations subject to the Red Flag Rules to attain compliance by November 1, 2008.[20]

The FTC's Red Flag Rules consist of three sections, and each of these contains a subsection that defines who must comply. The second part of the Red Flag Rules probably has received the most attention. This is the part that requires development of an Identity Theft Prevention Program.[21]

The Red Flag Rules require a creditor to make reasonable attempts to prevent and detect identity theft through its Identity Theft Prevention Program and to respond appropriately to mitigate the identity theft.[22] For healthcare providers, this may mean reviewing the medical record (of the thief and of the victim as well if the victim is also a patient) to remove false information. The Red Flag Rules include guidelines on how the creditor can identify Red Flags and respond to these Red Flags. The Red Flag Rules also describe what a user of consumer reports must do, if the user receives a notice of address discrepancy.

The Red Flag Rules apply to any healthcare provider that (a) is a creditor, (b) is subject to enforcement under FCRA by the FTC, and (c) has covered accounts (or takes other designated actions). Healthcare providers need to walk through this three-prong test to determine applicability of the Red Flag Rules. The decision tree in Section R may assist in this analysis.

To know whether your organization has to comply with the FACTA Red Flag Rules, the following questions may help:

Are we a creditor? For example, do some of our patients pay on their account over time? Do we let our patients pay after they receive our services?

The Red Flag Rules apply to financial institutions and creditors. Although we may think of creditors as just including banks, credit card issuers, and companies that offer installment payments, the definition is much broader. Credit includes, among other things, the right granted by a creditor to purchase services and defer payment for the services.[23] Any person who regularly extends credit is a creditor.[24] If a healthcare provider allows for payment on medical services

provided to a patient after those services were provided and/or over a period of installment payments, the healthcare provider could be considered a creditor. Accordingly, unless you provide services only on a prepaid basis, you are likely a creditor for Red Flag Rule purposes.

Are we subject to enforcement under the Fair Credit Reporting Act?

The FTC has responsibilities for administration of FCRA,[25] including the amendments to the FCRA made as part of FACTA. Compliance with FCRA is enforced under the FTC Act by the FTC. A violation of any requirement under FCRA constitutes an unfair or deceptive practice in commerce in violation of the FTC Act.[26] The FTC Act generally governs corporations and other entities that operate for profit for themselves or their members.[27] Accordingly, for-profit corporations, partnerships, nonprofit trade associations, and professional societies are subject to FTC enforcement. This does not end the analysis, however. Creditors subject to the administrative enforcement of the FCRA include any person[28] that violates FCRA "irrespective of whether that person is engaged in commerce or meets any other jurisdictional tests in the [FTC] Act."[29] Thus, FCRA grants the FTC authority over entities, regardless of whether those entities otherwise are governed under the FTC Act. Included in that broader group of entities are nonprofit corporations.[30] Accordingly, for example, a nonprofit hospital corporation is subject to FTC enforcement under FCRA.

Do we have covered accounts?

The Red Flag Rules specify that any "creditor that offers or maintains one or more covered accounts must develop and implement a written [Red Flag] Program."[31] A covered account is defined broadly as (a) "[a]n account . . . primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions" or (b) "[a]ny other account . . . for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the . . . creditor from identity theft."[32] An account is further defined as a "continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household or business

purposes. An account includes: an extension of credit, such as the purchase of property or services involving a deferred payment."[33]

Patient accounts are accounts for personal purposes (i.e., consumer rather than business accounts). If multiple payments can be made on the account, it is likely to be a covered account under the Red Flag Rules. Moreover, patient accounts also may present a risk of identity theft. Covered accounts also may include business-to-business relationships such as an outreach laboratory.

If we are covered, what do we do now?

Many healthcare providers will find that they are creditors subject to FTC enforcement with covered accounts. If that includes you or your organization, you will need to implement an Identity Theft Prevention Program as of November 1, 2008. The program should be appropriate to the size and complexity of the organization, and the scope of its activities.[34] For most healthcare providers, an appropriate Identity Theft Prevention Program will consist of carefully developed policies, consistently applied to detect potential identity theft that the provider could encounter in its normal operations.

In addition to the part of the Red Flag Rules requiring an Identity Theft Prevention Program, there are two other sections that could apply to some healthcare providers. These sections apply to users of consumer reports, and issuers of credit cards. To see if either of these sections applies to you, answer the following two questions:

Do we use consumer reports?

Some healthcare providers have begun requesting consumer reports on patients who register for expensive services. If you request consumer reports, then you will need to comply with the first section of the Red Flag Rules. This section requires a user of consumer reports to take certain actions if the consumer's address supplied in the report is different from the address supplied by the consumer.

Do we issue smart cards or other credit cards?

The third section of the FTC's Red Flag Rules is the least likely to apply to healthcare providers (although it may apply to providers that are experimenting

with smart cards for access to services). A credit card includes any card or other credit device used to obtain services on credit.[35] If the healthcare provider issues a card to the patient that allows the patient to pay for services, that device may fall within the definition of "credit card." Under the FTC's Red Flag Rules, card issuers must adopt policies to deal with the scenario that they receive a notice of change address and also, simultaneously or shortly thereafter, a request for a replacement card. The card issuer cannot issue a replacement card until taking appropriate action to confirm the address.

An Identity Theft Prevention Program must be approved by an organization's board of directors (or a designated committee of the board) and contain "reasonable policies and procedures" to:

- Identify relevant red flags for covered accounts and incorporate those red flags into the Identity Theft Prevention Program;
- Detect red flags that have been incorporated into the Identity Theft Prevention Program;
- Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and
- Ensure the Identity Theft Prevention Program is updated periodically, to reflect changes in risks to customers or to the safety and soundness of the financial institution or creditor from identity theft.[36]

The Red Flag Rules contain guidelines to assist in the development of an Identity Theft Prevention Program. The recommended steps are summarized here and discussed in detail below:

1. Identify Covered Accounts;
2. Identify Relevant Red Flags;
3. Detect Red Flags;
4. Respond to Red Flags;
5. Oversee the Program;
6. Train Employees;
7. Oversee Service Provider Arrangements;

8. Approve the Identity Theft Prevention Program; and
9. Provide Reports and Periodic Updates to the Identity Theft Prevention Program.

As further assistance, organizations can walk through the Questions to Assist in Developing an Identity Theft Prevention Program found in the Red Flag Toolkit at Section S.

D. Step One: Identify Covered Accounts

The Red Flag Rules require each creditor (who is subject to FTC enforcement) to determine periodically whether it offers or maintains covered accounts under the Red Flag Rules. Most patient accounts will qualify under the first of the types of "covered accounts" in the Red Flag Rules. This type of covered accounts is maintained primarily for personal, family, or household purposes that involve or are designed to permit multiple payments or transactions.[37] Covered accounts also include any other account, including non-consumer (i.e., business accounts) that the creditor determines pose "a reasonably foreseeable risk to customers or the safety and soundness of the . . . creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks."[38]

A healthcare provider may consider the following as possible covered accounts under the Red Flag Rules. A top priority should be on patient accounts and billing records that include patient identifying information. Those accounts likely would contain information sufficient to allow for identity theft to occur if they were lost or stolen. Pharmacy records also are of the type ripe for identity theft. Drug-seeking individuals may be inclined to look for those patients that have prescriptions for narcotics or controlled substances. If the pharmacy records are lost or stolen, then this highly sensitive and dangerous information could fall into the wrong hands. Providers also should look at its business-to-business relationships for possible covered accounts although not all such relationships may present risk of identity theft.

Healthcare providers should remember that traditional medical records are not necessarily the type of information repository that would be subject to

coverage under the Red Flag Rules. The FTC has indicated that accounts, not records are the focus of the Red Flag Rules and that it is not inclined to seek enforcement of the Rules over traditional medical records alone.[39]

E. Step Two: Identify Relevant Red Flags

Identifying appropriate Red Flags that are relevant to a healthcare provider's covered accounts requires review of the types of accounts that are offered and maintained; the methods used to open, provide access to, and collect on these accounts; and previous experience with identity theft. A Red Flag is a pattern, practice, or specific activity that indicates the possible existence of identity theft.[40] The appendices to the Red Flag Rules give numerous examples of Red Flags that could be encountered. Because the Red Flag Rules apply to many industries, not all of the sample Red Flags will apply in the healthcare sector. Red Flags include:

- Alerts, notifications, or other warnings received from consumer report agencies or service providers, such as fraud detection services
    - o A fraud or active duty alert is included with a consumer report
    - o A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report
    - o A consumer reporting agency provides a notice of address discrepancy
    - o A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer (e.g., a recent and significant increase in the volume of inquiries; an unusual number of recently established credit relationships; a material change in the use of credit, especially with respect to recently established credit relationships; or an account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor)

- Suspicious documents (e.g., obvious forgeries, photograph, or physical description not matching person tendering it)
    - 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 applicant or customer presenting the identification
    - Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification
    - Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check
    - An application appears to have been altered or forged—or gives the appearance of having been destroyed and reassembled
- Suspicious personally identifiable information, including suspicious changes of address (also including bogus social security numbers [SSNs] and data points commonly associated with identity theft, such as fictitious/mail-drop/prison addresses and/or pager/answering-service phone numbers, provision of personally identifiable information different from that already on file)
    - Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor (e.g., the address does not match any address in the consumer report, or the SSN has not been issued or is listed on the Social Security Administration's Death Master File)
    - Personal identifying information provided by the customer is not consistent with other personal identifying information

provided by the customer (e.g., a lack of correlation between the SSN range and date of birth)

- Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor (e.g., the address on an application is the same as the address provided on a fraudulent application, or the phone number on an application is the same as the number provided on a fraudulent application)
- Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor (e.g., the address on an application is fictitious, a mail drop, or a prison, or the phone number is invalid or is associated with a pager or answering service)
- The SSN provided is the same as that submitted by other persons opening an account or other customers
- The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers
- The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete
- Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor
- For financial institutions and creditors that use challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond

that which generally would be available from a wallet or consumer report

- Unusual use of, or other suspicious activity related to, a given account (including requests for new/additional/replacement accounts shortly following change of address, mail repeatedly returned as undeliverable, notification that mail is not being received by intended recipient, notice of unauthorized charges)
    - Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account
    - A newly revolving credit account is used in a manner commonly associated with known patterns of fraud patterns (e.g., the majority of available credit is used for cash advances or merchandise that is easily convertible to cash, such as electronics equipment or jewelry, or the customer fails to make the first payment or makes an initial payment but no subsequent payments)
    - A covered account is used in a manner that is inconsistent with established patterns of activity on the account (e.g., nonpayment when there is no history of late or missed payments, a material increase in the use of available credit; a material change in purchasing or spending patterns, a material change in electronic fund transfer patterns in connection with a deposit account, or a material change in telephone call patterns in connection with a cellular phone account)
    - A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage, and other relevant factors)

- Mail sent to the customer is returned repeatedly as undeliverable, although transactions continue to be conducted in connection with the customer's covered account
- The financial institution or creditor is notified that the customer is not receiving paper account statements
- The financial institution or creditor is notified of unauthorized charges or transactions in connection with a customer's covered account

A healthcare provider must identify which of these (or other) Red Flags are relevant to its covered accounts. Again, not all the Red Flags referenced above will apply in a healthcare setting.

F. Step Three: Detect Red Flags

The next step of the Identity Theft Prevention Program is to develop reasonable approaches for detecting the identified Red Flags that have been incorporated into the Program. This may include obtaining identifying information about, and verifying the identity of, persons opening covered accounts and then authenticating patients and customers, monitoring their transactions, and verifying the validity of change of address requests. The policies contained in Section T of the Red Flag Toolkit may prove helpful.

DECISION POINT:
What information and documentation will you require of patients?

The FTC recognizes that, for healthcare providers, the greatest risk of identity theft occurs when the account is established.[41] A person seeking healthcare services may steal the identity of another person to gain access to insurance or coverage under a government program. But identity theft also can involve existing patients.

In addition to identity theft, healthcare providers also can suffer losses from synthetic identity theft. In this fraud, the perpetrator does not use identity information of a single actual person but rather creates a synthetic identity with

fictitious information. The information could be totally fictitious or could combine false information with information from one or more individuals.[42]

Several of the Red Flags mentioned in the FTC's guidance involve discrepancies in personal identifying information. For healthcare providers, the fundamental issue in establishing an appropriate Identity Theft Prevention Program is how much personal identifying information should be collected when a patient is registered. Obviously, it is impossible to detect that the patient's SSN is invalid if the patient does not provide this number.

The Red Flag Rules do not require you to change the information you request from patients at registration. As you develop your Identity Theft Prevention Program, however, this is a good time to revisit your registration procedures in light of the high incidence of identity theft. In particular, consider whether you have experienced losses due to patients providing fraudulent information without documentation of identity.

Some healthcare providers have operated largely on the honor system when accepting a new patient. Usually, we ask the patient to present his or her insurance card—but it is less common to require other forms of identification, such as a driver's license or passport. Sometimes consumers resist attempts to require more identification and, in particular, resist providing SSNs because of fear that the information can be used for identity theft. For each type of personal identification you require, you should weigh the usefulness of the information in protecting against identity theft versus the burden to the patient in providing the information and the burden to your organization in maintaining and protecting the information. Of course, legal restrictions also will play a part of the analysis.

SSN/Social Security Card

The SSN still is used to identify Medicare (and many other health plan) beneficiaries. For other patients, the number is not needed to confirm eligibility, but it is useful for identity verification. Most people will have an SSN, and credit reports most easily are obtained with the consumer's SSN.

There is a significant downside to using the SSN for verifying identity. Many consumers are aware that the more times the consumer discloses his or

her SSN, the more likely it is that someone possessing this information will misuse it. The FTC has commented that "the challenge is to find the proper balance between the need to keep SSNs out of the hands of identity thieves and the need to give businesses and government entities sufficient means to attribute information to the correct person."[43]

From time to time, Congress has introduced legislation that would limit the circumstances in which a business can ask a consumer to provide his or her SSN. Some state laws contain restrictions on use of the SSN. In particular, several states prohibit requiring an individual to transmit his or her SSN over the Internet unless the connection is secure or the SSN is encrypted.[44]

One advantage of requiring patients to furnish the SSN for identity verification is that there are certain SSN numbers that are invalid on their face. The SSN consists of three fields: the area number (first three digits), group number (fourth and fifth digits), and serial number (last four digits). No valid SSN will have a group number of 00 or a serial number of 0000. The area numbers 666, 772 or above in the 700 series, or 800 or 900 series also are invalid. There are commercial services available that can screen for validity of a SSN.

If you decide to ask patients for their SSN at time of registration, be prepared to address the concerns of those who are reluctant to provide the number for fear that its dissemination makes them more vulnerable to identity theft.[45]

Driver's License or Other Photo ID

Some healthcare providers may consider requiring that adult patients provide a driver's license, passport, or other photo ID at time of registration. The downside is that some patients may not have this identification or may not have it with them at the time of service. If the patient has called to make an appointment over the phone, he or she can be reminded at that time to bring a photo ID with them.

Insurance Card

Your contracts with insurance companies and other payors may require you to ask patients to present an insurance card at time of service. Patients,

however, frequently misplace or forget to bring their cards, and it may be difficult to tell if a card is forged.

Verification of Residence

A current utility bill with the patient's name and address can help verify that the patient lives at the address claimed. This may be a secondary means of verification for a patient who does not have a driver's license.

DECISION POINT:
What responsibilities will your organization's workforce undertake in detecting red flags?

When you have decided what identity verification you will require at time of registration, the next step is to scrutinize this information to detect any Red Flags. Your policies should state that the person registering the patient should be alert for any conflicting information (e.g., the photograph on a driver's license does not appear to be that of the patient, or the address on a driver's license does not match the address given by the patient). If the healthcare provider has an existing record of the patient, the identifying information should match. The employee should ask the patient to explain any discrepancies.

Even if no Red Flags are identified when the patient is registered, a claim of identity theft may arise at a later time. This can happen if the individual whose name is on the account later resists paying the bill, claiming that he or she never received the services.

G. Step Four: Respond to Red Flags

Responding to Red Flags requires preventing and mitigating identity theft through appropriate responses such as:

- Monitoring covered accounts for evidence of identity theft;
- Contacting the patient/consumer, if necessary;
- Changing passwords and security codes;
- Reopening, as appropriate, a covered account with a new account number, declining to open a new account, or closing an existing account;

- Not attempting to collect on an account or selling it to a debt collector; or
- Notifying law enforcement.

A possible appropriate response may include concluding that, all things considered, no action is necessary. To respond appropriately, it is necessary for a healthcare provider to assess whether the Red Flag that was detected evidences a risk of identity theft. If nothing is done in response to the Red Flag, the healthcare provider must have a reasonable basis for concluding that the Red Flag did not evidence a risk of identity theft.[46] The healthcare provider also should take into account aggravating factors that may heighten the risk of identity theft. Examples of such aggravating factors include situations such as a data security incident that results in unauthorized access to a customer's account records held by the healthcare provider or such as receipt of notice that a patient has provided information related to a covered account held by the healthcare provider to someone fraudulently claiming to represent the healthcare provider or to a fraudulent website.[47]

Red Flags may be detected at numerous times, including when an individual tries to register as a patient. If there are discrepancies in the identification presented by the patient, and they cannot be explained, what action will you take?

DECISION POINT:
What will you do if the patient does not have all the identifying information you request?

It may be appropriate in some cases to deny services or tell the patient that he or she cannot be seen until more documentation is provided. (This option is not available for hospital emergency departments. Under EMTALA, hospitals must provide anyone seeking evaluation or care of an emergency medical condition with a medical screening exam. If the patient does have an emergency medical condition, then the hospital must either stabilize the condition or arrange for an appropriate transfer.)

DECISION POINT:
How will you respond to concerns, questions, and complaints?

Your Identity Theft Prevention Program should address how you will investigate a claim of identity theft that arises after services were provided. It is appropriate to ask the individual to provide identifying information that can be compared with the identification obtained from the patient at the time of service. You can ask the individual to report the identity theft to local police and provide you with a copy of the police report. Also, the FTC has developed an ID Theft Affidavit for the identity theft victim to submit to companies that claim they are owed money if the victim believes these claims resulted from identity theft.

When you receive the individual's documentation of the claimed identity theft, you should review the information to determine whether it is credible. If you find that the individual has been a victim of identity theft, you should take appropriate steps to mitigate the harm caused to the individual by identity theft. This would include ceasing collection activity on accounts that were created as a result of identity theft and correcting adverse credit information relating to these accounts.

Sometimes an individual may claim identity theft to avoid payment of the bill but not provide information to support this claim. If you find that the individual's claim of identity theft is not credible and decide to resume collection activity, you should send the patient a written explanation.

Some states have special requirements for creditor investigation of claims of identity theft.[48]

H. Step Five: Oversee the Program

The board of directors, an appropriate committee of the board, and/or a designated member of senior management should oversee, develop, implement, and administer the Identity Theft Prevention Program.

I. Step Six: Train Employees

Appropriate workforce training must occur. For example, there may be general training of all employees to sensitize them to the issues surrounding

identity theft. Then, staff involved with patient registration and with patient accounts may be trained on the requirements of the Identity Theft Prevention Program. A sample training presentation is included in Section V of the Red Flag Toolkit.

J. Step Seven: Oversee Service Provider Arrangements

For any third party granted access to the covered accounts in providing services to a healthcare provider, the healthcare provider must take steps to ensure that the activity is carried out in compliance with its Identity Theft Prevention Program. This may be accomplished through a business associate contract, or the service agreement, or otherwise if the service provider has adopted necessary policies and procedures for itself which would amount to contractually obligating the service provider to comply with such requirements. It may be prudent to revisit and update your business associate contract template or contract requirement checklists.

K. Step Eight: Approve the Identity Theft Prevention Program

The Red Flag Rules require that the Identity Theft Prevention Program be approved by the board of directors or an appropriate committee of the board.[49] A sample resolution is found at Section U of the Red Flag Toolkit. For an entity not having a board of directors, the Program should be approved by the highest executive authority (e.g., the president, management committee, owner of a sole proprietorship). The board, an appropriate committee, or a senior executive must have responsibility for ongoing administration of the Program.

L. Step Nine: Provide Reports and Periodic Updates to the Identity Theft Prevention Program

On at least an annual basis, staff should provide a written report to the board, a board committee, or the designed senior management representative. This report should address material matters concerning the Identity Theft Prevention Program, such as:

- Effectiveness of policies and procedures in addressing the risk of identity theft in opening new accounts
- Service provider arrangements

- Significant incidents involving identity theft and management's response
- Recommendations for material changes to the Program

The responsible manager should review the Program periodically and make appropriate changes based on the organization's experience in encountering identity theft.

However, you are not quite done yet. The Red Flag Rules also include additional obligations if your organization uses credit reports and/or issues credit or smart cards.

M. Responding to a Notice of Address Discrepancy

Do you request credit reports on prospective patients in some circumstances? If you do, you need to develop policies and procedures:

- To compare information from the consumer reporting agency with information you have in your files or have obtained from the patient; or
- If you have received a notice of address discrepancy, to provide to the consumer reporting agency an address that you have reasonably confirmed is accurate.

When you request a consumer report and the address you provide in your request differs from the address the consumer reporting agency has on file for the consumer, the agency is required to send you a notice of address discrepancy. If you receive such a notice and it appears to relate to the person about whom you requested the report, you should notify the consumer reporting agency of the address reported by the individual.

N. Duties of Card Issuers

Some large healthcare providers may issue a card to the patient that the patient can present at point of service. The card is linked to the patient's demographic and patient record information, so that when the patient presents the card, the service will be billed to the guarantor as listed in the patient record.

If the patient's card is lost or stolen, a person possessing the card could conceivably use it to obtain healthcare services fraudulently. The Red Flag Rules

require that if a card issuer receives notice of a change of address and then, within a short period of time, a request for an additional or replacement card, the card issuer cannot issue the new card until the change of address is determined to be valid.

O. What to Do with the Medical Record

Once your Identity Theft Prevention Program is up and running, your organization must have policies and procedures in place to ensure the integrity of the medical record. When an individual's identity is stolen to obtain healthcare services, this can cause even more harm than the financial repercussions of identity theft. Inclusion of false or inaccurate information in the medical record can result in the patient getting inappropriate treatment. A false or inaccurate medical history also may mean that the individual's applications for health or life insurance are denied, or health insurance claims could be denied due to pre-existing conditions that the individual never had.

P. Relationship to HIPAA

The preamble to the final Red Flag Rules indicates that an Identity Theft Protection Program may be part of an existing compliance program. Although a GLB Act compliance program specifically was mentioned, many healthcare providers may choose to incorporate an identity theft program into a HIPAA compliance program. Know, too, that insider criminal activity creates the risk of identity theft, as does lost or stolen laptops. If unencrypted patient identifying information falls into the wrong hands, it can be used for identity theft.[50]

HIPAA compliance is beyond the scope of this Member Briefing, but it is important to be aware of how HIPAA ties into identity theft prevention. Some healthcare providers may decide to request additional identifying information as part of their Red Flag policies. The more identifying information that goes into patient files, the more critical it is to protect the information entrusted to us through effective HIPAA compliance. A strong HIPAA compliance program is essential to prevent or promptly detect misappropriation of personal information that can be used for identity theft.

Q. Moving Forward

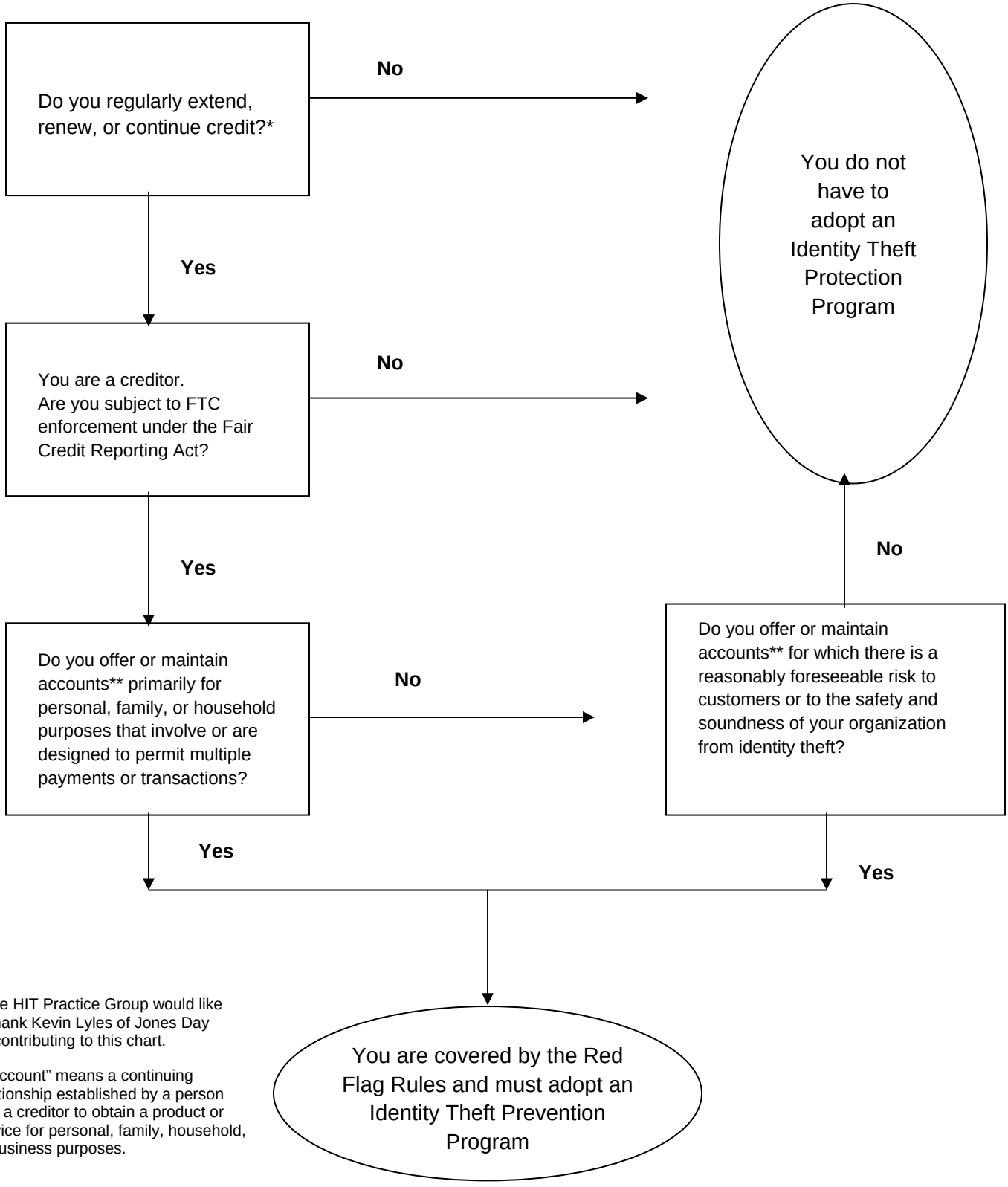
Medical identity theft is an emerging issue, and definitive guidance on how to handle potential medical identity theft does not yet exist. In May 2008, the National Coordinator for Health Information Technology of HHS awarded a contract to Booz Allen Hamilton to assess the scope and impact of medical identity theft in the U.S. HHS also announced a town hall meeting on October 15, 2008, to get input from healthcare experts on this problem.

The World Privacy Forum is conducting research into medical identity theft, and has identified eight best practices to combat medical identity theft.[51] The World Privacy Forum recommends:

- Development of a national level set of procedures to standardize handling of medical identity theft;
- Specific “red flag” guidelines for medical identity theft;
- John or Jane Doe file extraction, to remove fraudulent information from files of the identity theft victim;
- Dedicated personnel to respond to medical identity theft;
- Focus on insider medical identity theft as well as outsider threats;
- Risk assessments for medical identity theft;
- Training for healthcare sector leaders creating awareness of the crime; and
- Education for patients and victims.

This Briefing provides sample policies and other tools to get you started in establishing the Identity Theft Prevention Program. An Identity Theft Prevention Program regrettably does not lend itself to a one-size-fits-all approach. Use the sample documents as guides only. You should customize them to your own operations.

R. Decision Tree*



* The HIT Practice Group would like to thank Kevin Lyles of Jones Day for contributing to this chart.

**"Account" means a continuing relationship established by a person with a creditor to obtain a product or service for personal, family, household, or business purposes.

S. Questions to Assist in Developing an Identity Theft Prevention Program*

Answers to the questions below, which were distilled from 16 C.F.R. Part 681and its appendices, may be used to form the basis of an Identity Theft Protection Program as required by the FTC's Red Flag Rules for most healthcare providers.

I. Identification of Relevant Red Flags

A. Risk factors: what risk factors do we face?

1. What types of covered accounts do we offer or maintain? Examples include not only patient accounts but also any other accounts—such as leases to third parties of office space, equipment, or personnel that are either (a) an account for personal or household purposes involving multiple transactions or (b) any account for which there is a reasonably foreseeable risk of identity theft (including financial, operational, compliance, reputation, or litigation risks)?
2. What methods do we use to open covered accounts? Do any of these methods involve risks of identity theft?
3. What methods do we provide for access to covered accounts? Do any of these involve risks of identity theft?
4. What previous experiences have we had with identity theft that may inform our identification of risk factors?
5. Are there any other potential sources of risk that should be considered?

B. Sources of red flags: how can we incorporate the following sources of potential red flags into the program?

1. Are there any past incidents of identity theft? What can be done to prevent similar incidents in the future?
2. What are methods of identity theft that have been used against other organizations? Are there any new methods of identity theft that reflect changes in identity theft risks? How can they be addressed?

---

* The HIT Practice Group wishes to thank Kent B. Thurber, Davis Wright Tremaine LLP (Portland, OR), for contributing this document.

3. What other guidance has been issued by regulatory agencies or other organizations?

C. Categories of red flags: what procedures have we instituted to assure that appropriate responses are made to the following categories of red flags?

1. Alerts, notifications or other warnings received from consumer reporting agencies and similar providers, including but not limited to:
    a. Fraud or active duty alerts;
    b. Notices of credit freeze;
    c. Notices of address discrepancy;
    d. Patterns of activity that are inconsistent with prior history;
    e. Recent increases in the volume of inquiries;
    f. Unusual numbers of new credit relationships;
    g. Material changes in the use of credit; and
    h. Accounts closed for cause.
2. The presentation of suspicious documents or information, or other suspicious activity, including but not limited to:
    a. Information that is inconsistent with external sources (e.g., address, date of birth, or social security number);
    b. Personal identifying information identified by third-party sources as having been associated with known fraudulent activity;
    c. Personal identifying information of a type commonly associated with fraudulent activity (e.g., fictitious address, use of mail drop, or phone number that is invalid or associated only with a pager or answering service);
    d. SSNs duplicating those of other patients (or customers);

e. Address or telephone numbers that are the same or similar to other patients (or customers), particularly recent ones;

f. New customers who fail to provide all required personal identifying information, especially if they have been notified that the application is incomplete;

g. Persons attempting to access an account who cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report;

h. Requests for additional authorized users on an account shortly following change of address;

i. Uses of an account that are inconsistent with established patterns of activity (e.g., nonpayment when there is no history of late or missed payments or a material increase in the use of the account);

j. Unexpected inactivity for a reasonably lengthy period of time;

k. Repeatedly returned mail from the patient (or customer) despite continued activity in the account; and

l. Unauthorized transactions.

II. Detecting Red Flags

A. What policies and procedures do we need to detect red flags in connection with new and existing accounts? Examples include:

1. Obtain information verifying the identity of any person opening a new account (e.g., name, date of birth, residential or business street address [if unavailable, obtain such information for next of kin or other contact individual], taxpayer identification number, passport number and country of issuance, alien identification card number, or other government-issued document indicating nationality and bearing a photograph or similar safeguard) and

2. In the case of existing accounts, authenticating customers, monitoring transactions, and verifying the validity of change of address requests.

III. Preventing and Mitigating Identity Theft

A. What policies and procedures would provide us with appropriate responses to red flags commensurate with the degree of risk posed? How should we address aggravating factors, such as actual instances of unauthorized access to an account or when someone fraudulently claiming to represent us has obtained information from one of our patients or debtors? Appropriate responses may include:

1. Monitoring accounts for evidence of identity theft;
2. Contacting the patient;
3. Changing passwords or security codes;
4. Reopening an account with a new account number;
5. Refusing to open, or closing a covered account;
6. Forbearing from collection on a covered account;
7. Notifying law enforcement; and
8. Determining that no response is necessary under the circumstances.

IV. Updating the Program

A. How will we periodically update the red flag program to reflect changes in risks to customers? Factors that may affect our need to update the Program include:

1. Actual instances of identity theft;
2. Changes in methods of identity theft;
3. Change in methods of detection, prevention, and mitigation of identity theft;
4. Changes in the types of accounts that we maintained; and
5. Changes in our business arrangements, including mergers, acquisitions, joint ventures, etc.

V. Methods for Administering the Program

A. Who has ultimate authority for oversight of the Program (e.g., board of directors, appropriate board committee, or designated

senior management)? Oversight should include assigning specific responsibility for implementation, reviewing periodic reports at least annually, and approving changes to the Program as necessary to address changing identity theft risks. Contents of periodic reports should address and evaluate the effectiveness of the Program in addressing the risk of identity theft, reporting significant incidents of such theft and management's response to it, and recommendations for material changes to the Program.

B. When third-party service providers are engaged to perform activities in connection with our accounts (e.g., coding, billing or accounting activities), what steps do we take to ensure that those activities are conducted in accordance with the Program?

T. SAMPLE POLICIES

Policy 1: Verifying Patient Identity at Time of Registration

Purpose: **To verify patient identity at time of registration**

Policy: **The provider will, to the extent feasible, request documentation of the patient's identity, residence address, and insurance coverage at time of registration as part of the Identity Theft Prevention Program.**

Procedure:

1. When a patient calls to request an appointment, the patient will be asked to bring the following at the time of the appointment:
   - Driver's license or other photo ID
   - Current insurance card
   - If the photo ID does not show the patient's current address, utility bills or other correspondence showing current residence

   If the patient is a minor, the patient's parent or guardian should bring the information listed above.
2. When the patient arrives for the appointment, the patient will be asked to produce the information listed above. This requirement may be waived for patients who have been seen within the last six months.
3. If the patient has not completed the registration form within the last six months, a new registration form must be completed.
4. **EXCEPTION [for hospitals]: If the patient has come to the hospital to request evaluation or treatment for an emergency medical condition, the provision of a medical screening examination will not be delayed to obtain documents verifying identity.**

Policy 2: Identity Theft Red Flags

Purpose: **To detect attempted identity theft or fraud**

Policy: **Provider staff will be alert for discrepancies in documents and patient information that suggest risk of identity theft or fraud.**

Procedure:

In the following circumstances, staff should be alert for the possibility of identity theft:

1. The patient submits a driver's license, insurance card, or other identifying information that appears to be altered or forged.
2. The photograph on a driver's license or other photo ID submitted by the patient does not resemble the patient.
3. Information on one form of identification submitted by the patient is inconsistent with information on another form of identification, or with information already in the provider's records.
4. The SSN 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, 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.
5. The address given by the patient does not exist or is a post office box.
6. The phone number given by the patient is invalid or is associated with a pager or an answering service.
7. The patient fails to provide identifying information or documents.
8. Personal identifying information given by the patient is not consistent with personal identifying information in the organization's records.
9. The patient's signature does not match a signature on file in the organization's records.
10. The SSN or other identifying information furnished by the patient is the same as identifying information in the provider's records furnished by other individuals.

Policy 3: Investigation of Suspected Identity Theft

Purpose: **To investigate potential identity theft or fraud**

Policy: **The provider will investigate situations in which an individual claims to be a victim of identity theft.**

Procedure:

1. If an individual claims to be a victim of identity theft, the provider or its collection agency will investigate the claim. The following guidelines apply:
   - 1.1 The individual must have filed a police report for identity theft.
   - 1.2 The individual must complete one of the following documents:
     - The ID Theft Affidavit developed by the FTC, including supporting documentation;
     - An ID theft affidavit recognized under state law; or
     - A statement including the following information:
       - A statement that the individual is a victim of identity theft;
       - A copy of the individual's driver's license or identification card;
       - Any other identification document that supports the statement of identity theft;
       - Specific facts supporting the claim of identity theft, if available;
       - Any other 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 businesses sent to the individual at his or her residence;
       - A telephone number for contacting the individual;

- Any information that the individual may have concerning the person who registered in his or her name;
- A statement that the individual did not authorize the use of his or her name or personal information for obtaining services; or
- 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.

1.3 The individual must cooperate with comparing his or her personal information with information in the Provider's records.

2. If following investigation, it appears that the individual has been a victim of identity theft, the provider will take the following actions:

2.1 The provider will cease collection on open accounts that resulted from identity theft. If the accounts had been referred to collection agencies or attorneys, the collection agencies/attorneys will be instructed to cease collection activity.

2.2 The provider will cooperate with any law enforcement investigation relating to the identity theft.

2.3 If an insurance company, government program or other payor has made payment on the account, the provider will notify the payor and refund the amount paid.

2.4 If an adverse report had been made to a consumer reporting agency, the provider will notify the agency that the account was not the responsibility of the individual.

3. If following investigation, it does not appear that the individual has been a victim of identity theft, the Provider or the collection agency will give written notice to the individual that he or she is responsible for payment of the bill. The notice will state the basis for determining that the person claiming to be a victim of identity theft was in fact the patient.

Policy 4: Disposition of Medical Record When Identity Theft Is Confirmed

Purpose: **To correct errors in medical records resulting from identity theft**

Policy: **Inaccuracies in medical records resulting from identity theft will be isolated and corrected.**

Procedure:

1. If it is confirmed that a patient record was created as the result of identity theft, a notation concerning the identity theft will be placed in the record. All demographic information will be removed from the record.
2. Medical records staff will determine whether any other records are linked to the record found to be created through identity theft.
3. In some cases, identity theft may involve an identity thief receiving care under the name of another person, who has been a patient. In such a case, other files relating to the patient will be reviewed and any information relating to the identity theft will be removed and segregated.

U. Sample Resolution Approving the Identity Theft Prevention Program

WHEREAS:

(a) Identity theft is a serious problem for businesses, consumers, and law enforcement in the United States, causing consumers to lose time and money and businesses to incur millions of dollars in losses.

(b) In response to the risks posed by identity theft to consumers and to the financial soundness of businesses, the United States Congress enacted the Fair and Accurate Credit Transactions Act of 2003 (FACT Act).

(c) The Federal Trade Commission (FTC), along with federal bank regulators, adopted regulations implementing the FACT Act (the Red Flag Rules) that require creditors to adopt a written Identity Theft Prevention Program.

(d) The organization is a creditor subject to the FTC's Red Flag Rules.

(e) The organization has developed an Identity Theft Prevention Program that identifies certain irregularities in information and documents submitted by patients as red flags; delineates procedures for detection of red flags; and specifies actions to be taken for investigation of potential identity theft and response to findings of such investigations.

BE IT RESOLVED:

1. This board of directors approves the Identity Theft Prevention Program (the program) submitted by management.

2. The _____ of the organization is delegated responsibility for oversight, ongoing development, implementation, and administration of the program and shall have the responsibility to develop periodic updates to the program to reflect changes in risk to customers and to the safety and soundness of the organization.

V. Sample Training Presentation

Identity Theft Prevention Program

Training for registration and patient account staff

What is Identity Theft

- Identity theft is fraud committed or attempted by using identifying information of another person (individual or entity) without authority.
- Medical identity theft is a growing problem with potentially fatal results.
- Data taken by identity thieves can include SSNs, account numbers, and other personal information.
- Consumers are victimized by identity thieves because they have to spend time and incur out of pocket expenses to correct their personal information and repair their credit.
- Businesses are victimized by identity thieves because they cannot collect amounts owed for their goods and services.

Red Flags for Identity Theft

- To help prevent identity theft, watch out for suspicious documents:
  - Insurance card that appears to be altered or forged
  - Photograph on the driver's license that does not look like the patient
  - Physical description on the driver's license that does not match the patient's appearance
  - Signature on the driver's license or other documents that does not match the patient's signature

Red Flags

- Be alert for suspicious personal identifying information:
  - The address, phone number etc. does not match existing records
  - The address given does not exist or is a PO box
  - The Social Security Number is invalid
  - The patient refuses to provide personal identifying information or documents

Handling Claims of Identity Theft

- If an individual claims that they did not receive services on their bill due to identity theft, ask the person to submit the following:
  - Police report
  - Federal Trade Commission ID Theft Affidavit
  - Similar statement including copies of his/her driver's license or other identification, documentation of the person's residence address, any facts known about the identity theft, and other related information

If Identity Theft Occurred -

- Charges relating to the identity theft will be removed from the bill
- If any adverse credit report has been made, consumer reporting agencies will be notified of a correction
- Medical record information resulting from the identity theft will be removed and segregated in a Jane/John Doe record

American Health Lawyers Association's Health Information and Technology Practice Group would like to thank: Patricia King of Swedish Covenant Hospital (Chicago, IL) and Rebecca L. Williams, RN, JD, of Davis Wright Tremaine LLP (Seattle, WA) for authoring this Member Briefing ; Dina B. Ross of Dina B. Ross Law Offices (Oak Park, IL) and Gerald "Jud" DeLoss of Gray Plant Mooty (Minneapolis, MN) for editing this Member Briefing ; and Kevin Lyles of Jones Day (Columbus, OH); and Kent B. Thurber of Davis Wright Tremaine LLP (Portland, OR) for contributing content to the Toolkit.

Disclaimer

This Member Briefing provides general information only and is not intended as legal advice. If you need legal advice, you should consult a licensed attorney in your jurisdiction. Also, the samples provided in the toolkit are not sufficient, on their own, to comply with the Red Flag Rules. They should be customized and used in conjunction with other analyses and documents to form an organization's Identity Theft Protection Program.

---

[1] 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).

[2] Federal Trade Commission 2006 Identity Theft Report, prepared for the Federal Trade Commission by Synovate, November 2007, at page 24, *available at* www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf.

[3] Federal Trade Commission 2006 Identity Theft Report, *supra* note 2.

[4]Take Charge: Fighting Back Against Identity Theft, Federal Trade Commission, February 2006, *available online* at www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.pdf.

[5] For example, the Truth in Lending Act, 15 U.S.C. § 1601 et seq., limits consumer liability for unauthorized credit card charges to a maximum of $50.00.

[6] Lost in Translation: Consumers' risk-benefit perspectives on electronically mediated healthcare initiatives, services and related issues, presentation of the World Privacy Forum for the FTC Healthcare Innovations Workshop, April 24, 2008.

[7] Federal Trade Commission 2006 Identity Theft Report, *supra* note 2.

[8] *Man Stole Pal's Identity to Pay for Bypass Surgery, Police Say*, CHICAGO TRIBUNE, August 22, 2008.

[9] *Diagnosis: Identity Theft*, BUS. WEEK, Jan. 8, 2007, www.businessweek.com/magazine/content/07_02/b4016041.htm

[10] 72 Fed. Reg. at 63727.

[11] HHS scheduled a "town hall meeting" on October 15, 2008 to address the topic of medical identity theft. Announcement of the meeting can be found *at* www.hhs.gov/healthit/privacy/identytheft.html.

[12] Pub. L. No. 106-102.

[13] Pub. L. No. 104-191.

[14] HIPAA requires that protected health information be protected against inappropriate uses and disclosures and its confidentiality, integrity and availability be protected.

[15] Federal Trade Commission 2006 Identity Theft Report, *supra* note 2, at page 24.

[16] Pub. L. No. 108-159.

[17] 15 U.S.C. § 1681.

[18] 72 Fed. Reg. 63718; 16 C.F.R. § 681.2, implementing 15 U.S.C. § 1681m(e). The Red Flag Rules also provide guidelines that apply to savings associations, federal credit union, issuers and users of consumer reports, national banks, and issuers of credit or debit cards. For the purposes of this Members Briefing, reference to the Red Flag Rules will be in regard only to 16 C.F.R. § 681.2, which applies to financial institutions' and creditors' duties to detect, prevent, and mitigate identity theft.

[19] *See* 15 U.S.C. § 1681m(e).

[20] 72 Fed. Reg. 63718.

[21] 16 C.F.R. § 681.2.

[22] 16 C.F.R. § 681.2(d)(2)(iii).

[23] 15 U.S.C. § 1681a(r)(5), referring to 15 U.S.C. § 1691a(d).

[24] 15 U.S.C. § 1681a(r)(5), referring to 15 U.S.C. § 1691a(e).

[25] 15 U.S.C. § 1681 et seq.

[26] *See* 15 U.S.C. § 1681s(a)(1).

[27] 15 U.S.C. § 44. The FTC Act likewise grants the FTC authority over entities, including "persons, partnerships, or corporations." 15 U.S.C. § 45(a)(2). Under the FTC Act, a person "means any natural person, partnership, corporation, association, or other legal entity, including any person acting under color or authority of State law" (15 U.S.C. § 57b-1(6)), and a corporation means any "company, trust, so-called Massachusetts trust, or association, incorporated or unincorporated, that is organized to carry on business for its own profit or that of its members." 15 U.S.C. § 44. The Supreme Court has held that nonprofit trade associations and professional societies that provide economic benefits to their for-profit members are subject to FTC jurisdiction

under the FTC Act because they operate for the profit of their members. *California Dental Ass'n v. FTC*, 526 U.S. 756, 767-69 (1999).

[28] A "person" is defined as "any individual, partnership, corporation, trust, estate, cooperative, association, government or governmental subdivision or agency, or other entity." 15 U.S.C. § 1681a(b).

[29] 16 C.F.R. § 681.2(a).

[30] Although not legally authoritative, the FTC issued a business alert specifically noting that "[w]here non-profit and government entities defer payment for goods or services, they, too, are to be considered creditors" under FCRA and, therefore, must comply with the Red Flag Rules. See Federal Trade Comm'n, FTC Business Alert, June 2008, available at www.ftc.gov/bcp/edu/pubs/business/alerts/alt050.shtm.

[31] 16 C.F.R. § 681.2(d)(1); *see also* 72 Fed. Reg. at 63719 ("only those . . . creditors that offer or maintain 'covered accounts' must develop and implement a written [Red Flags] Program").

[32] 16 C.F.R. § 681.2(b)(3).

[33] 16 C.F.R. § 681.2(b)(1).

[34] 16 C.F.R. § 681(d)(1).

[35] 15 U.S.C. § 1602(k).

[36] 16 C.F.R. § 681.2(d).

[37] *See* 16 C.F.R .§ 681.2(b)(3)(i).

[38] *See* 16 C.F.R. § 681.2(b)(3). It is unclear whether this means identity theft resulting from use of information in the creditor's covered accounts, or identity theft in which the creditor is victimized by providing goods/services to an imposter. The latter, however, seems more apropos given the types of criteria in the "risk assessment" and the commentary's reference to such things as the ability to open accounts remotely or through other methods not involving face-to-face contact, and the need to "factor [ ] experiences with identity theft" into the equation for "accounts that have been the **target** of identity theft." 72 Fed. Reg. at 63723-24.

[39] *See Red Alert—Red Flag Rules May Apply to You*, AHLA Teleconference, October 1, 2008, Comments by FTC Representative Naomi Lefkovitz.

[40] 16 C.F.R. § 681.2(b)(9).

[41] 72 Fed. Reg. 63718, 63727.

[42] Synthetic ID theft is mentioned in the FTC's 2006 Identity Theft Report, *supra* note 2, at page 4, but not included in the totals for reported identity theft.

[43] Prepared Statement of the Federal Trade Commission before the Subcommittee on Social Security, House Committee on Ways and Means, June 21, 2007.

[44] A 2005 report of the Government Accountability Office lists the following states as having this or other requirements restricting use or display of SSNs: Arizona, Arkansas, California,

Connecticut, Illinois, Maryland, Michigan, Minnesota, Missouri, Oklahoma, Texas and Virginia. GAO-05-1016T (Sept. 15, 2005).

[45] Here is the advice that the Social Security Administration provides to consumers about providing their SSNs:

> The Social Security number was originally devised to keep an accurate record of each individual's earnings, and to subsequently monitor benefits paid under the Social Security Program. However, use of the number as a general identifier has grown to the point where it is the most commonly used and convenient identifier for all types of record-keeping systems in the United States . . . .
>
> The Privacy Act regulates the use of Social Security numbers by government agencies. When a federal, state, or local government agency asks an individual to disclose his or her Social Security number, the Privacy Act requires the agency to inform the person of the following: the statutory or other authority for requesting the information; whether disclosure is mandatory or voluntary; what uses will be made of the information; and the consequences, if any, of failure to provide the information.
>
> If a business or other enterprise asks you for your number, you can refuse to give it. However, that may mean doing without the purchase or service for which your number was requested. For example, utility companies and other services ask for a Social Security number, but do not need it; they can do a credit check or identify the person in their records by alternative means.
>
> Giving your number is voluntary, even when you are asked for the number directly. If requested, you should ask why your number is needed, how your number will be used, what law requires you to give your number and what the consequences are if you refuse. The answers to these questions can help you decide if you want to give your Social Security number. The decision is yours.

[46] *See* 72 Fed. Reg. at 63729.

[47] 16 C.F.R. Part 681, Appendix A (IV).

[48] For example, Illinois law requires that a debt collector must cease collection activity when a consumer presents the collector with the FTC Identity Theft Affidavit, the Illinois Attorney General ID Theft Affidavit, or a statement containing similar information. The debt collector must investigate the claim of identity theft and can only recommence collection activity after notifying the consumer of the reasons why the debt collector does not believe the debt resulted from identity theft.

[49] 16 C.F.R. § 681.2(e)(1).

[50] Work of the World Privacy Forum and others has suggested that more medical identity theft may be caused by misuse of confidential information by healthcare insiders, than by isolated instances of identity thieves seeking healthcare services. There have been several incidents of

identity theft traced to HIPAA and other violations by healthcare provider employees. Examples include:

- Theft of more than 1,100 patient records by a scheduling clerk at the Cleveland Clinic hospital in Weston, Florida, in 2006. A clerk gave the data to her cousin, who used it to submit $2.8 million in false Medicare claims.

- Theft of over 49,000 records by a patient admission representative at New York Presbyterian Hospital in 2008, who sold the records to identity thieves.

[51] Responses to Medical Identity Theft: Eight best practices for helping victims of medical identity theft, World Privacy Forum, Oct. 16, 2007, *available at* www.worldprivacyforum.org/medicalidtheftresponses.html.