The World Privacy Forum

Red Flag and Address Discrepancy Requirements: Suggestions for Health Care Providers

Robert Gellman and Pam Dixon
World Privacy Forum
September 24, 2008

Brief Summary of Report

This report discusses the applicability of the Federal Trade Commission's *Red Flag and Address Discrepancy Rule* to health care providers. Commonly called the "Red Flag Rule," the regulations provide direction and guidance regarding identity theft detection, prevention, and mitigation programs.

About this Report

This report is published by the World Privacy Forum and is available at <http://www.worldprivacyforum.org>. This report is not legal advice.

About the World Privacy Forum

The World Privacy Forum is a non-profit public interest research and consumer education group. It focuses on a range of privacy matters, including financial, medical, employment, and Internet privacy. The World Privacy Forum was founded in 2003. The World Privacy Forum published the first major report on medical identity theft in 2006, and brought the issue to national attention for the first time. The Forum's materials on medical identity theft may be found at: <http://www.worldprivacyforum.org/medicalidentitytheft.html>.

Table of Contents

Red Flag and Address Discrepancy Requirements: Suggestions for Health Care Providers

Executive Summary

Under recently issued regulations, the Federal Trade Commission requires financial institutions and creditors to develop and implement written identity theft prevention programs. The broad purpose of these *Red Flag and Address Discrepancy Rules* [1] is to require financial institutions and creditors to formally address the risks of identity theft and develop a mitigation plan. Health care providers can be creditors and subject to the new rules, which take effect November 1, 2008. This document focuses in particular on the application of the Red Flag rules to health care providers. It provides suggestions from the World Privacy Forum about how to implement the rules in a health care context, and also discusses best practices. Nothing here constitutes legal advice.

A "Red Flag" is defined as a pattern, practice, or specific activity that could indicate identity theft. A "Notice of an Address Discrepancy" is a notice that a credit bureau sends to a person or business that ordered a credit report about a consumer. The Notice of Address Discrepancy triggers obligation for that person or business under the new regulations. Federal law says generally that entities offering credit to consumers need to look for and pay attention to evidence of identity theft that arises from their dealings with consumers. The new *Red Flag and Address Discrepancy Rules* define these obligations with specificity.

Health care providers – whether they are for-profit, non-profit, or governmental entities – may have obligations under the rules. Medical identity theft – particularly involving insider access to data – is a real concern in the health care sector, and is included expressly in the Red Flag Rules Guidelines.[2] The possibility of medical identity theft

---

[1] See <http://www.ftc.gov/os/fedreg/2007/november/071109redflags.pdf>.

[2] Federal Trade Commission et al., Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003, 72 Fed. Reg. 63718, 63727 (Nov. 9, 2007) "For instance, creditors in the health care field may be at risk of medical identity theft (i.e., identity theft for the purpose of obtaining medical services) and, therefore, must identify Red Flags that reflect this risk." Note that the Red Flag Rule and the Address Discrepancy Rule were published together, but are separate rulemakings, <http://www.ftc.gov/os/fedreg/2007/november/071109redflags.pdf>.

gives rise to a duty to monitor for the potential that patients may be victims. The prudent provider will also oversee employee and vendor access to patient data.

The Red Flag and Address Discrepancy rules are designed to protect consumers. The World Privacy Forum prepared this document to encourage better understanding and application of these rules. Consumers will only realize the protections if health care providers apply the rules robustly and consistently. Previous work by the World Privacy Forum suggests that providers need help in addressing identity theft issues.

Red Flags that the World Privacy Forum recommends for health care providers are:

- **A complaint or question from a patient based on the patient's receipt of:**
  - **a bill for another individual**
  - **a bill for a product or service that the patient denies receiving**
  - **a bill from a health care provider that the patient never patronized**

    or
  - **a notice of insurance benefits (or Explanation of Benefits) for health services never received.**

- **Records showing medical treatment that is inconsistent with a physical examination or with a medical history as reported by the patient.**

- **A complaint or question from a patient about the receipt of a collection notice from a bill collector.**

- **A patient or insurance company report that coverage for legitimate hospital stays is denied because insurance benefits have been depleted or a lifetime cap has been reached.**

- **A complaint or question from a patient about information added to a credit report by a health care provider or insurer.**

- **A dispute of a bill by a patient who claims to be the victim of any type of identity theft.**

- **A patient who has an insurance number but never produces an insurance card or other physical documentation of insurance.**

• A notice or inquiry from an insurance fraud investigator for a private insurance company or a law enforcement agency.

Note: There is a good deal of misunderstanding regarding the role and utility of ID checks in a Red Flag and medical identity theft context. See the Mitigation section in this document for a discussion of this issue.

All of these Red Flags take on greater importance if the patient has also filed a police report regarding identity theft. Health care providers should include questions to determine the presence of a police report in their Red Flag identity theft plans. Another factor that increases the importance of a Red Flag is if the health care provider or other relevant entity in the health care community has had a recent data breach that included the patient's data.

I. Background

The Fair Credit Reporting Act (FCRA) as amended in 2003 requires the Federal Trade Commission and bank regulatory agencies to issue joint regulations and guidelines regarding the detection, prevention, and mitigation of identity theft. The requirement includes special regulations directing debit and credit card issuers to validate notifications of changes of address under certain circumstances. 15 U.S.C. § 1681m(e). Another FCRA amendment calls for additional joint regulations offering guidance regarding reasonable policies and procedures that a user of a consumer report (e.g., a credit grantor) should employ when the user receives a Notice of Address Discrepancy. 15 U.S.C. § 1681c(h).

These Red Flag and Address Discrepancy regulations were published in final form on November 9, 2007, 72 Fed. Reg. 63718 (Nov. 9, 2007). They are separate regulations. The mandatory compliance date for both rules is November 1, 2008. Although six agencies issued common regulations, the regulations that will affect health care providers are those from the Federal Trade Commission. 16 C.F.R. Part 681. The Federal Trade Commission will also be the agency that enforces the rules for the health care sector.

II. How the Red Flag Rule Affects Health Care Providers

The Red Flag Rule applies broadly to financial institutions, credit grantors, and some others, including some health care providers. A health care provider comes under the Red Flag rule if the provider: 1) meets the definition of *creditor* under the Fair Credit Reporting Act (15 U.S.C. 1681a(r)(5)). A health care provider comes under the Address Discrepancy Rule if they: 1) use consumer credit reports.

Creditors

Many of the Red Flag provisions apply mostly to banks, other financial institutions, and debit and credit card issuers. Some of the obligations affect *creditors*, a general term that includes some health care providers. A creditor is:

> any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit. 15 U.S.C. §§ 1691a(e), 1681a(r)(5). 16 C.F.R. § 681.2(b)(4).

Banks, finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies are examples of *creditors*. Accepting credit cards as a form of payment does not by itself make an entity a *creditor*. Where non-profit and government entities defer payment for goods or services, they, too, are considered *creditors*.

Creditors that offer or maintain *covered accounts* have obligations under the Red Flag regulations. A *covered account* is:

> (i) An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account; and
>
> (ii) Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks. 16 C.F.R. § 681.2(b)(3).

Essentially, if a health care provider extends credit to a consumer by establishing an account that permits multiple payments, the provider is a *creditor* offering a *covered account* and is subject to the Red Flag rules. The supplementary information accompanying the final publication of the Red Flag rule explains the application of the rule in the health care world:

> For instance, creditors in the health care field may be at risk of medical identity theft (i.e., identity theft for the purpose of obtaining medical services) and, therefore, must identify Red Flags that reflect this risk. 72 Fed. Reg. 63727 (Nov. 9, 2007).

Appendix 1 of this document includes the full text of the supplementary information.

User of Credit Reports

Health care providers may also be subject to the Address Discrepancy rules that apply to users of consumer reports. (A consumer report is also known as a *credit report*). A *Notice of Address Discrepancy* is a notice sent to a user by a consumer reporting agency (also known as a *credit bureau*) that informs the user of a substantial difference between the address for the consumer that the user provided to request the consumer report and the address in the agency's file for the consumer. 16 C.F.R. § 681.1(b).

The Notice of Address Discrepancy is required by the Fair Credit Reporting Act. Under 15 U.S.C. § 1681c(h), when a person requests a nationwide credit report for a consumer, the request will include the address that the consumer provider to the person. If the address differs substantially from the address in the credit bureau files, the bureau notifies the requester of the existence of the discrepancy.

The Notice of Address Discrepancy triggers obligations under the new rules. Any health care provider that orders a credit report on a consumer must comply with those obligations, which are discussed in more detail in section IV of this document.

III. What are the Obligations for a Health Care Provider Covered by the Red Flag Rule as a Creditor?

If a health care provider falls under the Red Flag Rule as a creditor, the provider must develop and implement a written identity theft prevention program. A key element of the program is the duty to mitigate identity theft.

Basic Organizational Requirements

A health care provider that qualifies as a *creditor* that offers or maintains *covered accounts* must develop and implement a written *Identity Theft Prevention Program*. The purpose of the program is to detect, prevent, and mitigate identity theft in connection with new or existing covered accounts. The Program must be appropriate to the size and complexity of the creditor and the nature and scope of its activities. A large hospital will need a more robust program than a two-doctor office.

What if a creditor does not maintain covered accounts or is not sure if it does? The rule requires a periodic determination as to whether it offers or maintains covered accounts. The required method calls for a risk assessment to make the determination, taking into consideration:

1. The methods it provides to open its accounts;

2. The methods it provides to access its accounts; and

3. Its previous experiences with identity theft.

For those creditors required to have an Identity Theft Prevention Program, there are four required elements. The program must include reasonable policies and procedures to:

1. Identify relevant Red Flags for the covered accounts that the creditor offers or maintains and incorporate those Red Flags into its program;

2. Detect Red Flags that have been incorporated into its program;

3. Respond appropriately to any Red Flags that are detected;

4. Update the program periodically to reflect changes in risks from identity theft to customers and to the safety and soundness of the creditor from identity theft.

There are also four elements to the administration of the Identity Theft Prevention Program. Each creditor required to have a program must:

1. Obtain approval of the initial written program from either its board of directors or an appropriate committee of the board of directors;

2. Involve the board of directors, an appropriate committee thereof, or a designated employee at the level of senior management in the oversight, development, implementation, and administration of the program;

3. Train staff, as necessary, to effectively implement the program;

4. Exercise appropriate and effective oversight of service provider arrangements.

Red Flags and Responses for Health Care Providers

The rule requires a creditor with an Identity Theft Prevention Program to consider the official federal agency Guidelines issued as an appendix to the Red Flag regulations. The Guidelines must be included in a written Red Flag identity theft program as "appropriate." A further Supplement to the Guidelines lists illustrative Red Flags. The Guidelines and the Supplement are reproduced at the end of this document for reference. (See Appendix 1.)

All of this material has some relevance to health care providers, although much of it is more applicable to a financial institution or credit card issuer. The advice about paying attention to an institution's own experience, to notices or alerts about identity theft, and to

suspicious documents is relevant to all. It is also true that health records – which often contain credit card numbers, Social Security Numbers, patients' home address, and financial information – can be rich source material for financial identity thieves. Therefore, attention to the possibility of financial identity theft remains a focus for health care providers just as much as for credit card issuers and merchants.

The purpose here is to focus on identity theft matters specific to health care providers and to medical identity theft. The World Privacy Forum published the first report identifying medical identity theft as a significant national problem. See MEDICAL IDENTITY THEFT: The Information Crime that Can Kill You (May 2006), <http://www.worldprivacyforum.org/pdf/wpf_medicalidtheft2006.pdf>. The report offers this definition of 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 or Social Security Number – without the victim's knowledge or consent to obtain medical services or goods, or when someone uses the person's identity to obtain money by falsifying claims for medical services and falsifying medical records to support those claims.

Based on the findings in that report and subsequent work, the World Privacy Forum offers suggestions for Red Flags that a health care provider should include in any Identity Theft Prevention Program.[3] The Red Flags contained in the official guidelines that pertain to suspicious documents, suspicious personal information, unusual activity, and notices from victims and others all have some relevance for health care providers.

The following annotated list of Red Flags is geared specifically to health care providers and is offered as a focused addition to the official guidelines.

- **A complaint or question from a patient based on the patient's receipt of:**
  - **a bill for another individual**
  - **a bill for a product or service that the patient denies receiving**
  - **a bill from a health care provider that the patient never patronized**

    or

[3] The World Privacy Forum maintains a regularly updated collection of materials and news about medical identity theft, including detailed FAQs, reports, public comments, speeches, news, and other materials. <http://www.worldprivacyforum.org/medicalidentitytheft.html>.

- **an Explanation of Benefits or other notice for health services never received.**

The World Privacy Forum Medical Identity Theft report (page 32 and 35) shows how an unexpected bill or notice of benefits can be one way that a patient can learn that she has been a victim of medical identity theft. "Explanations of Benefits" or EOBs are potentially important tools for patients and providers. For example, hotline information to report possible fraudulent or suspicious activity can be included on an EOB.

• Records showing medical treatment that is inconsistent with a physical examination or medical history as reported by the patient.

In particular, records that show substantial discrepancies in age, race, and other physical descriptions may be evidence of medical identity theft. The World Privacy Forum Medical Identity Theft report (page 33) illustrates how an incorrect blood type was evidence that the patient was a victim of medical identity theft.

• A complaint or question from a patient about the receipt of a collection notice from a bill collector.

The World Privacy Forum Medical Identity Theft report (page 31) shows how a collection notice can be one way that a patient can learn that she has been a victim of medical identity theft.

• A patient or insurance company report that coverage for legitimate hospital stays are being denied because insurance benefits have been depleted, or that a lifetime cap has been reached.

The World Privacy Forum Medical Identity Theft report (page 34) illustrates how members of a family can be victimized by "looping", where a thief uses one family member's benefits and then turns to the next family member when the first victim's benefits have run out.

• A complaint or question from a patient about information added to a credit report by a health care provider or insurer.

The World Privacy Forum Medical Identity Theft report (page 32) shows how an entry in a credit report can be one way that a patient can learn that she has been a victim of medical identity theft.

• A dispute of a bill by a patient who claims to be the victim of any type of identity theft.

Although financial identity theft differs significantly from medical identity theft, a victim of financial identity theft may be more likely to also be a victim of medical identity theft. Victims of financial identity theft may have filed police reports about their case, and these need to be taken into account.

• A patient who has an insurance number but never produces an insurance card or other physical documentation of insurance.

A medical identity thief may succeed by obtaining the medical insurance number and other information about the victim. The absence of an actual insurance card is evidence suggesting that the person being treated may not be the actual insured. **Note:** This particular Red Flag has to be applied with caution because there are other reasons a patient may not have her insurance card.

• A notice or inquiry from an insurance fraud investigator for a private insurance company or a law enforcement agency.

Not all forms of medical identity theft are the result of an individual thief presenting for treatment. The World Privacy Forum Medical Identity Theft report (page 33) illustrates how fraudulent billing by a physician can result in false information in a health record that may affect the treatment of patients. In some cases, clerks, nurses and other hospital employees have exploited their legitimate access to health files to use patients' identity and health information for medical identity theft.[4]

Mitigation

One of the important elements of an Identity Theft Prevention Program is the *duty to mitigate identity theft*. 16 C.F.R. § 681.2(d)(2)(iii). In general, the health care industry has not paid sufficient attention to helping individual victims of medical identity theft. The World Privacy Forum Medical Identity Theft report (beginning on page 40) discusses the problems victims can have when they seek to correct health records and otherwise recover from medical identity theft. The report identified these challenges:

• Lack of enforceable rights to correct medical records in all instances.

[4] See, e.g., the Department of Justice criminal actions against Fernando Ferrer and Isis Machado. Machado, who worked at the Cleveland Clinic, accessed and sold patient information to Ferrer, who used the information to file false Medicare claims. Press Release, U.S. Department of Justice, *Two Defendants Sentenced in Health Care Fraud, HIPAA, and Identity Theft Conspiracy*, (May 7, 2007), (U.S. Attorney's Office, Southern District of Florida), <http://www.usdoj.gov/usao/fls/PressReleases/070503-01.html>.

• Lack of a government agency dedicated to help victims of medical identity theft.

• Lack of enforceable rights to delete misinformation from medical records.

• Lack of ability in most cases to find all instances of medical records.

• Lack of information resources about the unique needs of medical identity theft victims.

The federal health privacy rules issued under the authority of the Health Insurance Portability and Accountability Act (HIPAA) do not mention medical identity theft, and the rights provided to patients by the HIPAA health privacy rule are not sufficient to help all patients who are victims. The World Privacy Forum offers suggestions to victims in using existing HIPAA and other remedies. See Access, Amendment, and Accounting of Disclosures: FAQs for Medical ID Theft Victims at <http://www.worldprivacyforum.org/FAQ_medicalrecordprivacy.html>. For more on the HIPAA health privacy rule, see <http://www.hhs.gov/ocr/hipaa>.

The Red Flag rules impose a separate and independent duty on health care providers subject to the regulation to help victims mitigate the consequences of medical identity theft. **Health care providers subject to the rules need to go beyond the provisions in HIPAA to assist victims**. For several years, the World Privacy Forum has urged the health care community to do a better job of addressing this issue.

Best Practices for Responding to Medical Identity Theft

The World Privacy Forum has been researching and working in the area of medical identity theft since 2005. Over time, several key best practices have emerged. The World Privacy Forum published specific ideas regarding these best practices. See Responses to Medical Identity Theft: Eight Best Practices for Helping Victims of Medical Identity Theft at <http://www.worldprivacyforum.org/medicalidtheftresponses.html>. Not all of the recommended best practices can be implemented by health care providers on their own. Some require national, legislative, or regulatory attention. Nevertheless, these best practices include actions that can be implemented by most health care providers.

Best practices include:

National level procedures

There needs to be a national level set of procedures to standardize how providers and insurers should handle medical identity theft. The procedures should come from a consensus process that includes health

information management professionals, patient representatives, consumer groups, insurers, privacy groups, and others. The standards need to address how to help ***victims*** recover from this crime.

There needs to be uniform but appropriately flexible answers to these questions:

- What do we do when a patient claims fraud is in their files?
- What do we do when a patient says the bills are for services she did not receive?
- What do we do for patients and other impacted victims when we uncover a fraudulent operation?
- When we have a real case of medical identity theft, how can we work with patients to fix the records and limit future damages?
- What do we do when a provider has altered the patient records?
- How do we handle police reports and requests for investigation from victims?

The answers to these questions need to viewed not just from the provider's perspective, but also from the victim's perspective, which can differ substantially.[5]

Red Flag alerts

Red Flag alerts in the financial sector context make financial institutions affirmatively react to the potential presence of fraud in order to protect consumers and themselves. A Red Flag alert in this context is any mechanism or tool that makes all relevant employees aware that there may be a problem. In some cases, the alert may be requested by the customer. Financial sector types of "Red Flag alerts" have applicability to the health care sector and medical identity theft.

[5] The Red Flag rules do not contemplate situations where a *provider* becomes a victim of medical identity theft. Because of this report is focused on the Red Flag regulations, this issue has not been discussed in this report. However, we note that individual doctors may also be victims of identity theft, and this can have impacts on consumers (and the doctor) that are deleterious. See for example Associated Press, *Couple accused of bilking $1 million in health care fraud scheme*, May 14, 2003.

In the medical identity theft context, a “Red Flag alert” could be placed in a victim's health care records to warn providers, insurers, and consumers of potential fraudulent activity in the past or present. This could include the ability to flag a file on paper or electronically for the presence of Red Flag indicators. The health care sector needs to create specific and thoughtful Red Flag alert guidelines, procedures, and tools for use in the medical identity theft context.

It is not unusual for some victims of medical identity theft to be told they cannot completely delete fraudulent information from one or more segments of their health care files. These victims are good candidates for a Red Flag alert or notice in their records that would highlight the potential presence of incorrect information in the patient file.

John or Jane Doe file extraction

Health information managers may be familiar with this concept already. The basic concept is that if fraud or medical identity theft can be substantiated, the victim's file is purged of all information that was entered as a result of the fraudulent activity, and is left with a brief cross-reference and explanation of the deletion.

In the operation of medical identity theft, sometimes fraudulent information may be added to a pre-existing health file. In other cases, the contents of an entire health file may refer only to the thief’s health conditions, but under the victim’s name and other identifying information. In either case, the fraudulent activity has the end result of having the potential to introduce errors into the file of the victim. Many times the errors entered into a victim’s file resulting from activities of a medical identity thief can be medically significant. This is one of the core harms of medical identity theft.

In a John or Jane Doe file extraction, if the thief is an unknown individual, the fraudulent information is completely removed from the victim's file and held separately so there is no danger of mistreatment due to factual error in the file. That separate file is the Jane or John Doe file. The victim's file and the extracted file are then cross-referenced, allowing for a retraceable data trail for any audits. If the thief is a known individual, the victim’s file can undergo the same kind of data extraction. The only difference is that the provider will have a name to file the purged file information under.

Dedicated, trained personnel available

Dedicated personnel who are trained to respond to this crime should be available at each facility. Small providers can have dedicated regional

personnel to help. It is in the providers' or insurers' best interest to resolve this crime, and it is in the victims' best interest to be able to actually talk to a person about what has happened. A designated person trained in the complexities of medical identity theft should be on hand to help both the victim and the institution.

Focus on the right approach: Insider, not just outsider

The preponderance of medical identity theft occurs through insider methods that are extremely difficult for providers to detect, even after the fact. Even when internal file browser controls and other controls are in place, unless there are safeguards with extensive checks, then bad actors on the inside of institutions can commit this crime on a grand scale. For example, in the Cleveland Clinic/Machado case, there were existing controls on downloads of files. The criminal still was able to exceed her download limit regularly, and she sold in excess of 1,100 patient files.[6]

Unsecured and unencrypted patient information on laptops, thumb drives, and other portable data devices can also pose significant risks, some of them unintentional, such as when workers legitimately take home laptops with patient information, and then lose or misplace the laptop.

Some institutions have been focusing on checking or scanning and storing patient IDs as a primary solution to the risk of medical identity theft. While checking patient IDs may potentially help with the one-to-two person and familial types of medical identity theft, the research does not support that this is where the bulk of the crime is. There is significant variability between providers and situations, it is therefore crucial to accurately assess and focus on all aspects of where the crime is occurring. **Checking patient IDs will not stop insiders, and this needs to be taken into careful consideration by stakeholders.**

Some providers have used the excuse of medical identity theft to institute intrusive identity check procedures, for example, biometrics collection or digital scans of government-issued IDs. It is our observation that these additional data collections increase risk for data breach, and also increase data risk for insider use. (Please see the heading “Caution about checking and storing patient identification documents and biometrics” in this document for a more detailed discussion of this.)

Risk assessments specifically for medical identity theft

Most health care institutions already have security risk assessments in place. Risk assessments need to be expanded to consider medical identity

[6] Id.

theft scenarios. A complete assessment should evaluate outsider threats, but it should also have a strong focus on the insider threat scenario as well.

Insider threat scenarios can include ascertaining the risk factors for large datasets containing patient identity documents such as scans of government IDs or biometrics, risks in any collections of patient information stored on laptops or other portable devices, access control and oversight of access control, and so forth. A risk assessment that evaluates the level of segregation of patient health data from financial data can be helpful to the provider in determining risk for identity theft.

Training materials and education for the health care sector

Many individuals and institutions working in the health care sector are not yet aware of medical identity theft. Health care sector leaders need to begin health care sector-focused education focused on increasing awareness of the crime, its operations, and how it impacts victims. Ideally, an education plan would be able to also discuss a national set of standards for dealing with the aftermath of medical identity theft with the purpose of helping victims. Again, many materials have a focus on the provider, not on what needs to be done for mitigation of the problems that individual victims have.

Provider education and training should also focus on increasing awareness of the need for provider laptops, desktops, and other computing devices to have security features, and on increasing education on best practices in the protection of patient information. This goes beyond the Red Flag rules per se, however, it is a best practice and a prudent step for providers.

Education for patients and victims

Providers and other stakeholders in the health care sector need to begin patient and victim education regarding medical identity theft. The education should focus on increasing:

- Awareness of the crime
- Awareness of the benefits of requesting a full copy of the health care files from all providers proactively
- Awareness of the need to guard insurance and Medicare/ Medicaid card numbers as carefully as Social Security Numbers
- Awareness of the need to proactively request an annual listing of all benefits paid by insurers

- Awareness of the need to educate data breach and financial identity theft victims about the potential for medical identity theft variations of the crime.

- Patient education and training on how to handle their health and insurance records securely, and on increasing awareness of the need for laptops, desktops, and other computing devices they are using that contain their sensitive health or financial information to have security features.

Some of these best practices discussed above are now part of the new Red Flag rules, others are part of a canon of best practices regarding medical identity theft. The World Privacy Forum specifically calls attention to the best practice of having dedicated, trained personnel available to help victims.

Determining that a patient has been a victim of medical identity theft can be a difficult task. Once it has been established that a health record contains information resulting from the medical identity theft, sorting through that health record to isolate the information that is actually about the patient from the information that is about the thief is harder still.

Health care providers are understandably reluctant to change or remove information from a health record. Yet that will sometimes be the proper remedy. It will take trained personnel to assist the victim and the provider (who may be a different type of victim) sort out the records. Another of the World Privacy Forum's best practices – John or Jane Doe file extraction – may be the proper technique.

Caution about Checking and Storing Patient Identification Documents and Biometrics

One of the most significant misunderstandings to arise following the release of the World Privacy Forum's 2006 report on medical identity theft is the idea that simply checking patient identification (such as a drivers' license) will effectively mitigate medical identity theft. Regrettably, this solution is neither as useful nor as simple it might appear on the surface.

Identity proofing and the range of issues attached to it are exceptionally complex. Identity management and identity proofing are the subject of significant research and scientific inquiry as well as policy debate at all levels.[7] The point is that it is a serious topic, and identity proofing should not be entered into lightly. By simply scanning a patient drivers' license and storing it, a provider sets foot into these difficult areas.

---

[7]See, e.g, National Research Council, *Who Goes There? Authentication Through the Lens of Privacy* (2003) (National Academies Press), <http://www.nap.edu/openbook.php?record_id=10656&page=R1>.

Just because customer identity proofing is commonplace in the financial sector does not mean that it has translated perfectly or even well to the health care sector. The two sectors have different regulatory requirements, approaches to access points, security, and information flows. Banks and health care providers also have different competencies, staffing capacities, training, and in many cases even procedures when it comes to reviewing and managing customer identification documents.[8]

Patient identity proofing, particularly in some implementations, can expose patients to increased risk of medical and other forms of identity theft. It can also expose actual victims of medical identity theft to significant problems when they try to demonstrate their innocence. Depending on the implementation, it can potentially increase the liability of a health care provider.

When patients are, for example, asked for a drivers' license when checking in to hospitals for surgery, the license itself may be copied or scanned and added into the actual patient file. This can give hospital insiders with criminal tendencies access to a treasure trove of photographic, biometric, and other information that may have been unavailable to them before. The result can be more identity theft (medical and otherwise). In some cases, providers collect additional patient biometrics and link that data to the drivers' license, patient ID and medical chart. Unfortunately, when a criminal ties his or her own biometrics to a fake or stolen ID – including a digitally reconstructed ID from a patient file – it is extremely difficult for the actual victim of medical identity theft to show that he or she is the real Jane or John Smith. In effect, the fake ID becomes an additional barrier to unraveling the criminal activity.

Patient ID checking and proofing is not a silver bullet. It is actually a potentially significant point of risk for health care providers and should be handled with great care. If that data is also allowed to be stored on portable devices, the risk the portable device presents should also be managed with care.

To summarize mitigation issues, the duty to mitigate the effects of medical identity theft is an important element of any Identity Theft Prevention Program. Health care providers should, among other mitigation techniques contemplated by the Red Flag rules:

- Provide trained and dedicated staff to help medical identity theft victims (including the provider itself) confirm the crime and determine its scope.

- Use John or Jane Doe file extraction techniques when appropriate to segregate records about the patient from records about the medical identity thief.

[8] See Testimony of the World Privacy Forum on Patient Identity Proofing before the Confidentiality, Privacy & Security Workgroup of the American Health Information Community, Sept. 29, 2006, (Department of Health and Human Services) <http://www.dhhs.gov/healthit/ahic/materials/meeting09/cps/P2-PHR-Dixon.pdf>.

• Undertake or adapt existing risk assessments specifically for medical identity theft.

Any mitigation plan should have a strong focus on helping all victims of the crime.

IV. What are the Address Discrepancy Obligations for a Health Care Provider That Uses Credit Reports?

The Address Discrepancy rule requires a user of a consumer report (credit report) to develop and implement reasonable policies and procedures to enable the user to deal with an address discrepancy. These requirements are narrower than the Red Flag rule for creditors. However, applicability of the address discrepancy requirement may affect a broader class of health care provider (and health insurers) than the Red Flag rule.

The address discrepancy requirement attaches to any user of a nationwide credit report. The user must be prepared to take appropriate action when a request to for a credit report results in a Notice of Address Discrepancy. When the address supplied by the user differs substantially from the address in the credit bureau files, the bureau notifies the requester of the existence of the discrepancy.

When the user receives a notice, it must have reasonable policies and procedures designed to enable the user to form a reasonable belief that a consumer report relates to the consumer about whom it has requested the report. The rule provides these examples of reasonable policies and procedures:

> (i) Comparing the information in the consumer report provided by the consumer reporting agency with information the user:
>
> (A) Obtains and uses to verify the consumer's identity in accordance with the requirements of the Customer Information Program (CIP) rules implementing 31 U.S.C. 5318(l) (31 CFR 103.121);
> (B) Maintains in its own records, such as applications, change of address notifications, other customer account records, or retained CIP documentation; or
> (C) Obtains from third-party sources; or
>
> (ii) Verifying the information in the consumer report provided by the consumer reporting agency with the consumer. 16 C.F.R. § 681.1(c)(2).

The user of a credit report must develop and implement reasonable policies and procedures for furnishing to the consumer reporting agency from whom it received the Notice of Address Discrepancy an address for the consumer that the user has reasonably confirmed is accurate Notice of Address Discrepancy when the user:

(i) Can form a reasonable belief that the consumer report relates to the consumer about whom the user requested the report;
(ii) Establishes a continuing relationship with the consumer; and
(iii) Regularly and in the ordinary course of business furnishes information to the consumer reporting agency from which the notice of address discrepancy relating to the consumer was obtained. 16 C.F.R. § 681.1(d)(1).

The rule again provides examples of confirmation methods. A user may reasonably confirm an address is accurate by:

(i) Verifying the address with the consumer about whom it has requested the report;
(ii) Reviewing its own records to verify the address of the consumer;
(iii) Verifying the address through third-party sources; or
(iv) Using other reasonable means. 16 C.F.R. § 681.1(d)(2).

Again, applicability of the address discrepancy requirement may affect a broader class of health care providers and health insurers than the Red Flag rule.

V. Conclusion

The Red Flag rule represents an important opportunity for the health care sector to protect consumers and patients from the impacts of medical and other forms of identity theft.

Until this point, victims of medical forms of identity theft have had very little help in getting relief in the provider context. While a few providers may have mitigation plans in place, many do not. It is not unusual for victims of this crime to report being victimized multiple times in multiple provider settings, sometimes across one or more states. As a result, as consumers work to clean up their health care files, they can experience differing levels of help and support due to variability of provider practices.

One thing has become less variable, though; that is, the scanning and storing of government-issued patient identification and sometimes biometrics. The World Privacy Forum cannot emphasize enough that patient identity proofing is one small aspect of preventing this crime. Improper collection, handling and storage of patient identity documents such as drivers' licenses and biometrics can increase rather than decrease patient *and provider* risk, depending on the system.

The Red Flag and Address Discrepancy rules, if implemented robustly, may ease some of the problems consumers have been experiencing with medical identity theft. It is an opportunity to help consumers that should not be wasted or treated lightly.

About the Authors

Robert Gellman is a privacy and information policy consultant based in Washington, DC. <http://www.bobgellman.com>.

Pam Dixon is the executive director of the World Privacy Forum. <http://www.worldprivacyforum.org/aboutus.html>.

For More Information

PDF version of full report is located at:
<http://www.worldprivacyforum.org/pdf/WPF_RedFlagReport_09242008fs.pdf>

For updates to this report and other documents related to medical identity theft, see the World Privacy Forum's Medical Identity Theft page at:
<http://www.worldprivacyforum.org/medicalidentitytheft.html>.

Contact

World Privacy Forum
www.worldprivacyforum.org
+1 760.436.2489

The World Privacy Forum is a 501 (c)(3) non-profit, tax-exempt organization. Its focus is on public interest research and consumer education relating to privacy topics.

Appendix 1: Reproduction of the Red Flag and Address Discrepancy Guidelines and Supplement

Following is a reproduction of the Guidelines and Supplement to the Red Flag and Address Discrepancy Rules. The rulemakings may be found at Federal Trade Commission et al., Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003, 72 Fed. Reg. (Nov. 9, 2007), <http://www.ftc.gov/os/fedreg/2007/november/071109redflags.pdf>.

Appendix A to 16 CFR Part 681 -- Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation

Section 681.2 of this part requires each financial institution and creditor that offers or maintains one or more covered accounts, as defined in § 681.2(b)(3) of this part, to develop and provide for the continued administration of a written Program to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. These guidelines are intended to assist financial institutions and creditors in the formulation and maintenance of a Program that satisfies the requirements of § 681.2 of this part.

I. The Program

In designing its Program, a financial institution or creditor may incorporate, as appropriate, its existing policies, procedures, and other arrangements that control reasonably foreseeable risks to customers or to the safety and soundness of the financial institution or creditor from identity theft.

II. Identifying Relevant Red Flags

(a) Risk Factors. A financial institution or creditor should consider the following factors in identifying relevant Red Flags for covered accounts, as appropriate:

(1) The types of covered accounts it offers or maintains;
(2) The methods it provides to open its covered accounts;
(3) The methods it provides to access its covered accounts; and
(4) Its previous experiences with identity theft.

(b) Sources of Red Flags. Financial institutions and creditors should incorporate relevant Red Flags from sources such as:

(1) Incidents of identity theft that the financial institution or creditor has experienced;
(2) Methods of identity theft that the financial institution or creditor has identified that reflect changes in identity theft risks; and
(3) Applicable supervisory guidance.

(c) Categories of Red Flags. The Program should include relevant Red Flags from the following categories, as appropriate. Examples of Red Flags from each of these categories are appended as Supplement A to this Appendix A.

(1) Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;

(2) The presentation of suspicious documents;

(3) The presentation of suspicious personal identifying information, such as a suspicious address change;

(4) The unusual use of, or other suspicious activity related to, a covered account; and

(5) Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the financial institution or creditor.

III. Detecting Red Flags

The Program's policies and procedures should address the detection of Red Flags in connection with the opening of covered accounts and existing covered accounts, such as by:

(a) Obtaining identifying information about, and verifying the identity of, a person opening a covered account, for example, using the policies and procedures regarding identification and verification set forth in the Customer Identification Program rules implementing 31 U.S.C. 5318(l) (31 CFR 103.121); and

(b) Authenticating customers, monitoring transactions, and verifying the validity of change of address requests, in the case of existing covered accounts.

IV. Preventing and Mitigating Identity Theft

The Program's policies and procedures should provide for appropriate responses to the Red Flags the financial institution or creditor has detected that are commensurate with the degree of risk posed. In determining an appropriate response, a financial institution or creditor should consider aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a customer's account records held by the financial institution, creditor, or third party, or notice that a customer has provided information related to a covered account held by the financial institution or creditor to someone fraudulently claiming to represent the financial institution or creditor or to a fraudulent website. Appropriate responses may include the following:

(a) Monitoring a covered account for evidence of identity theft;

(b) Contacting the customer;

(c) Changing any passwords, security codes, or other security devices that permit access to a covered account;

(d) Reopening a covered account with a new account number;

(e) Not opening a new covered account;

(f) Closing an existing covered account;

(g) Not attempting to collect on a covered account or not selling a covered account to a debt collector;

(h) Notifying law enforcement; or

(i) Determining that no response is warranted under the particular circumstances.

V. Updating the Program

Financial institutions and creditors should update the Program (including the Red Flags determined to be relevant) periodically, to reflect changes in risks to customers or to the safety and soundness of the financial institution or creditor from identity theft, based on factors such as:

(a) The experiences of the financial institution or creditor with identity theft;

(b) Changes in methods of identity theft;

(c) Changes in methods to detect, prevent, and mitigate identity theft;

(d) Changes in the types of accounts that the financial institution or creditor offers or maintains; and

(e) Changes in the business arrangements of the financial institution or creditor, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

VI. Methods for Administering the Program

(a) Oversight of Program. Oversight by the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management should include:

(1) Assigning specific responsibility for the Program's implementation;

(2) Reviewing reports prepared by staff regarding compliance by the financial institution or creditor with § 681.2 of this part; and

(3) Approving material changes to the Program as necessary to address changing identity theft risks.

(b) Reports.

(1) In general. Staff of the financial institution or creditor responsible for development, implementation, and administration of its Program should report to the board of directors, an appropriate committee of the board, or a designated employee at the level of senior management, at least annually, on compliance by the financial institution or creditor with § 681.2 of this part.

(2) Contents of report. The report should address material matters related to the Program and evaluate issues such as: The effectiveness of the policies and procedures of the financial institution or creditor in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts; service provider arrangements; significant incidents involving identity theft and management's response; and recommendations for material changes to the Program.

(c) Oversight of service provider arrangements. Whenever a financial institution or creditor engages a service provider to perform an activity in connection with one or more covered accounts the financial institution or creditor should take steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. For example, a financial institution or creditor could require the service provider by contract to have policies and procedures to detect relevant Red Flags that may arise in the performance of the service provider's activities, and either report the Red Flags to the financial institution or creditor, or to take appropriate steps to prevent or mitigate identity theft.

VII. Other Applicable Legal Requirements

Financial institutions and creditors should be mindful of other related legal requirements that may be applicable, such as:

(a) For financial institutions and creditors that are subject to 31 U.S.C. 5318(g), filing a Suspicious Activity Report in accordance with applicable law and regulation;

(b) Implementing any requirements under 15 U.S.C. 1681c–1(h) regarding the circumstances under which credit may be extended when the financial institution or creditor detects a fraud or active duty alert;

(c) Implementing any requirements for furnishers of information to consumer reporting agencies under 15 U.S.C. 1681s–2, for example, to correct or update inaccurate or incomplete information, and to not report information that the furnisher has reasonable cause to believe is inaccurate; and

(d) Complying with the prohibitions in 15 U.S.C. 1681m on the sale, transfer, and placement for collection of certain debts resulting from identity theft.

Supplement A to Appendix A

In addition to incorporating Red Flags from the sources recommended in section II.b. of the Guidelines in Appendix A of this part, each financial institution or creditor may consider incorporating into its Program, whether singly or in combination, Red Flags from the following illustrative examples in connection with covered accounts:

Alerts, Notifications or Warnings from a Consumer Reporting Agency

1. A fraud or active duty alert is included with a consumer report.

2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.

3. A consumer reporting agency provides a notice of address discrepancy, as defined in § 681.1(b) of this part.

4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:

a. A recent and significant increase in the volume of inquiries;

b. An unusual number of recently established credit relationships;

c. A material change in the use of credit, especially with respect to recently established credit relationships; or

d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

Suspicious Documents

5. Documents provided for identification appear to have been altered or forged.

6. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

7. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.

8. 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.

9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

10. Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example:

a. The address does not match any address in the consumer report; or

b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.

11. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.

12. 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. For example:

a. The address on an application is the same as the address provided on a fraudulent application; or

b. The phone number on an application is the same as the number provided on a fraudulent application.

13. 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. For example:

a. The address on an application is fictitious, a mail drop, or a prison; or

b. The phone number is invalid, or is associated with a pager or answering service.

14. The SSN provided is the same as that submitted by other persons opening an account or other customers.

15. 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.

16. 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.

17. Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.

18. 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 Suspicious Activity Related to, the Covered Account

19. 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.

20. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example:

a. The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); or

b. The customer fails to make the first payment or makes an initial payment but no subsequent payments.

21. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:

a. Nonpayment when there is no history of late or missed payments;

b. A material increase in the use of available credit;

c. A material change in purchasing or spending patterns;

d. A material change in electronic fund transfer patterns in connection with a deposit account; or

e. A material change in telephone call patterns in connection with a cellular phone account.

22. 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).

23. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.

24. The financial institution or creditor is notified that the customer is not receiving paper account statements.

25. The financial institution or creditor is notified of unauthorized charges or transactions in connection with a customer's covered account.

Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection With Covered Accounts Held by the Financial Institution or Creditor

26. The financial institution or creditor is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.
