COMPLIANCE PERSPECTIVES

Red Flags Rules: Identity Theft Protections Now Extend to Health Care Providers

Judith Waltz

Jennifer Karron

Andrew Serwin

Judith Waltz, Jennifer Karron, and Andrew Serwin are health care attorneys with Foley & Lardner LLP

Hospitals, clinical laboratories, and other medical care providers may be dangerously unaware that they have a looming deadline for compliance with complex new federal regulations.

These "Red Flags Rules" require the adoption and implementation of a broad identity theft prevention system by Nov. 1, 2008.

Neither the statute nor the implementing regulation issued by the Federal Trade Commission (FTC) expressly states its applicability to health care providers. However, the preamble to the regulations specifically discusses "medical identity theft," making it clear that the governmental entities responsible for enforcing these new provisions (and prosecuting cases of medical identity theft) will expect health care providers to exercise due diligence to conform with the new provisions.

For the health care provider, identity theft may result in unpaid claims, assessments of overpayments, or even allegations that false claims have been submitted.

Medical Identity Theft a Growing Concern

Medical identity theft may occur for purposes of obtaining medical items (including drugs) or services or for purposes of fraudulently obtaining money relating to medical items or services.

As defined by the Department of Health and Human Services (HHS) on its Web site, medical identity theft is a "specific type of identity theft which occurs when a person uses someone else's personal health identifiable information, such as insurance information, Social Security Number, health care file, or medical records, without the individual's knowledge or consent to obtain medical goods or services, or to submit false claims for medical services."

In May 2008, HHS's Office of the National Coordinator for Health Information Technology (ONC) awarded a $450,000 contract to Booz Allen Hamilton to assess and evaluate the scope of the medical identity theft problem in the United States. Its final report is expected to be released sometime during the next six months (late 2008 or early 2009) and will set forth possible next steps for the federal government and other stakeholders to work toward prevention, detection, and remediation of medical identity theft.

Even the federal government is not immune from current scrutiny with respect to its efforts to avoid medical identity theft. HHS's Office of Inspector General indicated in its annual 2009 Work Plan that it will review the efforts of the Centers for Medicare and Medicaid Services (CMS) to deter medical identity theft, including its outreach to beneficiaries.

Medical identity theft may result in insurance claims for items or services that have never been provided, were provided to

different individuals than those whose insurance is billed, or that are billed in exaggerated amounts. Health care plans are obvious targets.

For the health care provider, these scenarios may result in unpaid claims, assessments of overpayments, or even allegations that false claims have been submitted. For the individual whose identity is stolen, there may be credit collection attempts against them for services they never received, as well as consequences for their ongoing health insurance coverage such as higher premiums or even cancellation if maximum benefits are reached.

Perhaps of most concern for individuals is the possibility of inaccurate medical records, which may have adverse clinical implications for ongoing health care. Resolving these medical record inaccuracies in all the multiple places where an individual's medical records are now kept could well become a lifetime pursuit. For society, the costs of medical identity theft may include higher insurance costs, inappropriate use of government programs (including government-provided health insurance as well as costs associated with investigation and enforcement), and an inappropriate distribution of health care resources.

Overview of the Red Flags Rules

In short, the new Red Flags Rules apply to those who are defined as "creditors," which, as discussed below, can include health care entities. These entities are expected to take proactive steps after having identified their "red flags" ("risk areas" to use terminology more familiar in the world of health care compliance), to put in place measures that will minimize the risk of identity theft, and to respond when the red flags suggest an attempt at theft. Involvement by the board of directors (or functional equivalent as defined) is required to approve the plan of action.

Perhaps of most concern for individuals is the possibility of inaccurate medical records, which may have adverse clinical implications for ongoing health care.

'Creditor' Defined

For purposes of the Red Flags Rules, a creditor is defined as "any person or business who arranges for the extension, renewal, or continuation of credit" with a "covered account." An account is defined as a continuing relationship with a creditor to obtain a product or service and includes deferred payments for services or property. A covered account is: 1) an account primarily for personal, family, and household purposes that involves or is designed to permit multiple payments or transactions; and 2) any other account (including an account for business purposes) for which there is 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.

Health care providers may have accounts that satisfy these definitions in various ways. Most health care providers extend credit to at least some patients by offering them extended payment plans. Some may also extend credit to employees or to other parties.

In California, Medi-Cal (the state's Medicaid program) may permit "share of cost" obligations to be paid over time. Each health care provider should, as a first step, think through what types of transactions it offers in the course of business that would meet the definition of a "covered account."

What Types of Activities Could Be Red Flags?

Individual entities must conduct their own self-scrutiny to determine what types of behavior or events they may have experienced (or to which they may be susceptible) that

would suggest the potential for medical identity theft. Possibilities may include situations involving the exhaustion of lifetime benefit limits, denials for duplicate or excessive services for one individual, identified fraudulent reimbursement or insurance submissions, or discrepancies in information collected at the time of providing services.

Some provisions of HIPAA may be implicated in the event of actual, suspected, or attempted medical identity theft.

Patient and insurer complaints about bills for items or services never received should be taken very seriously, even though many such complaints turn out to be without merit due to understandable patient confusion about their bills or about the multiplicity of providers of services involved in their care. To properly define and implement their Red Flags program, health care organizations must learn lessons from others, keeping abreast of the identity theft environment and tapping sources such as literature and information from credit bureaus, financial institutions, other creditors, designers of fraud detection software, and from their own prior experience.

Red Flags Rules Require More Than HIPAA Compliance

While all health care providers are used to the privacy and security rules applicable under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), these new provisions are likely to require some enhanced steps with respects to covered accounts, as defined above. Obviously, some HIPAA-protected information might serve as a basis for medical identity theft.

In addition, though, the health care provider must consider what other identifying information it might have in its possession which, even if arguably not protected health information, might be used for improper purposes leading to a possibility of medical identity theft.

Identifying information means any name or number that may be used alone or in conjunction with any other information to identify a specific person, including: Social Security number; date of birth; official state- or government-issued driver's license or identification number; passport number; alien registration number; unique biometric data; unique electronic identification number, address, or routing code; or telecommunication identifying information or address device and so forth.

Thus, under the Red Flags Rules, the creation of a fictitious identity using any single piece of information belonging to a real person falls within the definition of identity theft.

Some provisions of HIPAA may be implicated in the event of actual, suspected, or attempted medical identity theft. These include HIPAA's provisions that a patient should have an opportunity to correct false information in his or her records and that a patient may request an accounting of what information has been disclosed, to whom it was disclosed, and why it was disclosed. Both provisions have limitations that presumably are addressed in the health care provider's HIPAA compliance program, which may merit a second look in light of the Red Flags Rules.

Genesis of the Red Flags Rules

The 2003 Fair and Accurate Credit Transactions Act (FACT Act), which created these Red Flags Rules, was one of the first federal financial privacy laws that applied to nonfinancial institutions. As new rules implementing the FACT Act have been implemented, the burdens placed upon nonfinancial institutions have only grown and recently enacted rules have added to the burdens placed upon companies, whether they are financial institutions or not.

The new provisions actually became effective on Jan. 1, 2008, although there is a phased-in compliance date of Nov. 1, 2008.

What to Do to Meet the New Requirements

At a minimum, health care entities should take the following steps to strive for compliance with the Red Flags Rules:

1. Periodically identify covered accounts. Each creditor must periodically determine whether it offers or maintains covered accounts. As a part of this determination, the creditor must conduct a risk assessment to determine whether it offers or maintains covered accounts, taking into consideration:

- The methods it provides to open its accounts;
- The methods it provides to access its accounts; and
- Its previous experiences with identity theft.

2. Establish an Identity Theft Prevention Program. Creditors that offer or maintain one or more covered accounts must develop and implement a written Identity Theft Prevention Program that is designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. The program must be appropriate to the size and complexity of the creditor and the nature and scope of its activities. The program must include reasonable policies and procedures to:

- Identify relevant Red Flags for the covered accounts that the creditor offers or maintains and incorporate those Red Flags into its program;
- Detect Red Flags that have been incorporated into the program of the creditor;
- Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft; and
- Ensure the program (including the Red Flags determined to be relevant) is updated periodically to reflect changes in risks to customers (i.e., a person that has a covered account with a financial institution or creditor) and to the safety and soundness of the creditor from identity theft.

3. Administer the Red Flags Program. Creditors, if required to implement a Red Flags Program, must also provide for the continued administration of the program and must:

- Obtain approval of the initial written program from either its board of directors (or functional equivalent, as defined) or an appropriate committee of the board of directors;
- 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;
- Train staff, as necessary, to effectively implement the program; and
- Exercise appropriate and effective oversight of service provider (i.e., a person that provides a service directly to the financial institution or creditor) arrangements.

4. Consider any pertinent state laws that may be implicated by your Red Flags Program.

Conclusion

The Red Flags Rules impose significant new challenges for health care providers, with a short time for turnaround. Even health care providers with robust compliance programs should review what protections are in place to protect against medical identity theft and assure that it knows what its "red flags" might be.

- *Judith Waltz can be reached at 415-438-6412, jwaltz@foley.com; Jennifer Karron can be reached at 414-297-5610, jkarron@foley.com; and Andrew Serwin can be reached at 619-685-6428, aserwin@foley.com.*