

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

2009 Supplement

I. Red Flags rule update

1.1 Deferral of enforcement of Red Flags rule

The Federal Trade Commission's "Red Flags rule" was published on November 9, 2007, and the compliance date was November 1, 2008. However, in response to requests from industry, the FTC twice delayed enforcement of the Red Flags rule: until May 1, 2009, and most recently until August 1, 2009.¹ The extensions only applied to the Red Flags rule, which requires adoption of a written Identity Theft Prevention Program. No extension of enforcement was granted for the regulations published along with the Red Flags rule, which specify obligations of users of consumer reports with respect to address discrepancies², and require card issuers to observe certain safeguards in handling requests for change of address³.

In its statement of enforcement policy extending the deferral of enforcement to August 1, 2009, the FTC noted that the Red Flags rule was drafted to be risk-based, so that entities can tailor their identity theft prevention programs to the level of risk of identity theft they face. Nevertheless, some low-risk entities continue to have concerns about how to comply with the Red Flags rule. The FTC stated it plans to develop a template program for low-risk entities to assist such entities in complying.

1.2 FTC Red Flags compliance resources

To help businesses determine whether they are required to comply with the Red Flags rule, and if so, how they can formulate an identity theft prevention program, the FTC developed a special website with compliance resources.⁴ The FTC's compliance resources include an article with suggestions for health care providers on "red flags" that physicians and other providers may encounter in their practice.⁵ In addition, the FTC provides a "fill in the blank" resource for low risk businesses to establish a written identity theft prevention program.⁶ The resource

¹ *FTC Extended Enforcement Policy: Identity Theft Red Flags Rule, 16 CFR 681.1*, published on the Federal Trade Commission website at

<http://www2.ftc.gov/os/2009/04/P095406redflagsextendedenforcement.pdf>.

² 16 C.F.R. § 641.1.

³ 16 C.F.R. § 681.2.

⁴ <http://www2.ftc.gov/redflagsrule>

⁵ Toporoff, *The "Red Flags" Rule: What Health Care Providers Need to Know About Complying with New Requirements for Fighting Identity Theft*, published online at

<http://www.ftc.gov/bcp/edu/pubs/articles/art11.shtm>.

⁶ *Complying with the Red Flags Rule: A Do-It-Yourself Prevention Program for Businesses and Organizations at Low Risk for Identity Theft*, available at

http://ftc.gov/bcp/edu/microsites/redflagsrule/RedFlags_forLowRiskBusinesses.pdf

allows the business owner to document why he/she believes the business is low-risk, and then to establish a simple written identity theft prevention program, including documentation of:

- Identification of red flags
- How red flags will be detected
- How the business will respond to red flags that are identified; and
- Administration of the program, including training of employees, notification to service providers of their obligations with regard to identity theft prevention, and updates to the program.

II. Health care providers and the Red Flags rule

The issue of whether health care providers, especially physicians, are “creditors” subject to the Red Flags rule has been controversial. In a letter dated February 4, 2009, the FTC took the position that health care providers could be “creditors” and therefore must comply with the Red Flags rule.⁷ The Red Flags rule was published pursuant to the Fair and Accurate Credit Transactions Act of 2003 (FACTA)⁸, which amended the Fair Credit Reporting Act (the FCRA).⁹ The definition of “creditor” in the FCRA refers to the corresponding definition in the Equal Credit Opportunity Act (the ECOA)¹⁰. “Credit” is defined under the ECOA as “the right granted by a creditor to a debtor to defer payment of debt or to incur debts and defer its payment or to purchase property or services and defer payment therefor.”¹¹ The FTC noted that the terms “credit” and “creditor” have been given broad scope in decisions of courts and other federal agencies, and in particular, that the Federal Reserve Board has interpreted the term “creditor” to include any entity that defers payment, even in the normal course of billing processes. The Federal Reserve Board’s Official Staff Commentary to Regulation B states:

If a service provider (such as a hospital, doctor, lawyer, or merchant) allows the client or customer to defer the payment of a bill, this deferral of a debt is credit for purposes of the regulation, even though there is no finance charge and no agreement for payment in installments.¹²

The FTC concluded that health care professionals who regularly bill for services after the services are rendered are “creditors”. Since there is no exception for physicians and other professionals in FACTA’s definition of creditor, they are required to comply with the Red Flags rule. The FTC commented that most physicians would face minimal risk of identity theft, and therefore a simple, streamlined identity theft prevention program should suffice.

⁷ Letter dated February 4, 2009 from Eileen Harrington, Acting Director of Bureau of Consumer Protection, FTC to Margaret Garikes, Director of Federal Affairs, American Medical Association, reproduced online at <http://www.ftc.gov/os/statutes/redflags.pdf>.

⁸ Pub. L. 108-159.

⁹ 15 U.S.C. § 1681 *et seq.*

¹⁰ 15 U.S.C. § 1681a(r)(5).

¹¹ 15 U.S.C. § 1691a(d).

¹² Official Staff Commentary, 12 C.F.R. § 202.3.

In response, a letter was sent on behalf of 85 specialty professional associations, state medical societies and related organizations to the FTC, continuing to object to application of the Red Flags rule to physicians.¹³ The letter argues that the claims payment process for medical services is not a “deferral” process, and the Federal Reserve Board’s Staff Commentary to the ECOA was not intended to the claims payment process governed by contractual obligations among patients, physicians and insurance carriers. Furthermore, the letter states that to apply the Red Flags rule to physicians, the FTC is required under the Administrative Procedure Act¹⁴ to publish a new rule for public comment.

III. Special implications of identity theft prevention measures for healthcare providers

3.1 EMTALA compliance

Typically, an identity theft prevention program will provide that steps be taken to verify the identity of an individual before credit is extended or services are provided. A modification of this procedure is required for Medicare-participating hospitals, in order to comply with the Emergency Medical Treatment and Labor Act (EMTALA).¹⁵ EMTALA requires that if any individual “comes to the emergency department”¹⁶, the hospital must provide an appropriate medical screening examination (MSE) to determine whether or not an emergency medical condition exists.¹⁷ The hospital may not delay the performance of the MSE in order to inquire about the individual’s method of payment or insurance status.¹⁸ Hospitals may, however, follow reasonable registration procedures as long as there is no delay in the MSE or stabilizing treatment, and the registration process does not unduly discourage individuals from remaining for further evaluation.¹⁹ Registration processes permitted in the emergency department typically consist of collecting demographic, insurance and emergency contact information.²⁰

EMTALA permits a hospital to transfer an individual whose emergency medical condition has not been stabilized in some circumstances, such as when the patient requires specialized services not available at the transferring hospital. When a transfer of an unstabilized patient is

¹³ Letter dated Feb. 23, 2009 to the Hon. William E. Kovacic, Chairman, Federal Trade Commission, available at <http://www.ftc.gov/os/closings/staff/090311amaredflagsrule.pdf>.

¹⁴ 5 U.S.C. § 551 *et seq.*

¹⁵ 42 U.S.C. § 1395dd.

¹⁶ The phrase “comes to the emergency department” is defined to mean that the individual has come to the dedicated emergency department, or presented anywhere on hospital property other than the dedicated emergency department, and requested examination or treatment for an emergency medical condition; is in a hospital-owned ambulance; or is in a non-hospital-owned ambulance located on the hospital property. 42 C.F.R. § 489.24(b). If the patient is registered as an outpatient and presents to a department other than the dedicated emergency department, EMTALA does not apply. State Operations Manual, Appendix V, *Interpretive Guidelines – Responsibilities of Medicare Participating Hospitals in Emergency Cases*, Tag 406.

¹⁷ 42 C.F.R. § 489.24(a)(1).

¹⁸ 42 C.F.R. § 489.24(d)(4)(i).

¹⁹ 42 C.F.R. § 489.24(d)(4)(iv).

²⁰ State Operations Manual, Appendix V, *Interpretive Guidelines – Responsibilities of Medicare Participating Hospitals in Emergency Cases*, Tag 408.

permissible under EMTALA, the receiving hospital may not delay acceptance of the transfer in order to obtain or validate financial or insurance information.²¹

In compliance with EMTALA, standard processes designed to protect against identity theft (such as requiring the individual to present a photo ID before services are rendered) must be suspended for the emergency department until after the MSE is conducted and the patient is stable.

3.2 Impact on patient referral relationships

In many cases, patients come to health care providers not directly, but through referral from other providers. In some cases, such as lab tests performed on specimens drawn elsewhere, there is no direct contact with the individual patient and the provider is relying on the referring provider to authenticate patient identity. In developing identity theft prevention procedures, consideration should be given to communicating with referral sources what documentation the provider will require in order to establish a new account.

3.3 Application of other laws

When the provider becomes aware that identity theft has occurred, the response must take into account federal and state security breach notification laws, and the obligation to mitigate harm under the Health Insurance Portability and Accountability Act (HIPAA). The HIPAA privacy regulations require a covered entity to mitigate, to the extent practicable, any harmful effect known to the covered entity of an inappropriate use or disclosure of protected health information (PHI).²² In the case of identity theft, false PHI may have been disclosed to a payor, for example. This is probably not the type of harm that HIPAA was intended to prevent, since the HIPAA privacy and security regulations are directed toward protection of the actual PHI of patients.

In many cases, identity theft may be reported to the provider by the victim (who becomes aware of the identity theft because he/she receives an EOB or a bill reflecting services he/she did not receive). If the provider uncovers the identity theft before it is known to the victim, counsel should review the provider's obligations under state security breach notification laws, and the new federal requirements established under the Health Information Technology for Economic and Clinical Health Act provisions of the American Recovery and Reinvestment Act.²³

IV. Medical identity theft

4.1 What is medical identity theft

²¹ *Id.*

²² 45 C.F.R. § 530(f).

²³ H.R. 1, S. 1, American Recovery and Reinvestment Act of 2009, Health Information for Economic and Clinical Health Act (the HITECH Act), § 13001, et seq.

In 2008, the U.S. Department of Health and Human Services, Office of the National Coordinator for Health Information Technology (ONCHIT) engaged Booz Allen Hamilton for a project on medical identity theft. The first phase of the project was an “environmental scan”, to capture what was currently known about the scope of the problem of medical identity theft, and existing resources to address the issue. The environmental scan was released on October 15, 2008 – the same day as a “Town Hall meeting” held with stakeholders to discuss the role of health information technology in addressing medical identity theft. The final report of the project was released on January 15, 2009.²⁴

The environmental scan used the following definition of medical identity theft:

Medical identity theft refers to the misuse of another individual’s PII [personally identifiable information] such as name, date of birth, SSN, or insurance policy number to obtain or bill for medical services or medical goods.²⁵

While acknowledging that data on the incidence of medical identity theft is sparse, the environmental scan noted that according to the FTC’s 2006 identity theft report, 3% of identity theft victims (about 250,000 Americans) reported that their identity was used fraudulently to obtain medical services. The difficulty of estimating the incidence of medical identity theft is compounded by the fact that medical identity theft can arise from health care fraud (when a provider fraudulently uses an individual’s information to bill for services not provided), from misappropriation of an individual’s PII, or from misuse of an individual’s PII with that individual’s consent to fraudulently obtain health care services.

The final report notes that health care providers are frequently confused about how to handle access to the medical record in the case of identity theft. Under HIPAA, individuals are entitled to access to their own health information. Some providers are concerned that giving the patient access to a record which may have been contaminated through medical identity theft violates HIPAA, because the patient would then have access to medical information of another individual. The report recommends development of additional FAQs or other guidance under HIPAA to educate providers on how to handle access to the record in instances of suspected medical identity theft. This is particularly important because patients are likely in the best position to verify the accuracy of data in their records.²⁶

4.2 Best practices in responding to medical identity theft

Medical identity theft requires a two-pronged response: investigation and mitigation of identity theft in accordance with the Red Flags rule, and restoring the integrity of the medical record. If the identity theft victim has never received services from the provider, the problem is somewhat less complicated: a fraud alert can be placed on the record. If the victim has been a patient, then medical information of the identity thief must be separated from the victim’s

²⁴ The environmental scan, transcript of the Town Hall meeting, and final report are available at <http://healthit.hhs.gov/portal/server.pt?open=512&mode=2&cached=true&objID=1177&PageID=15441>.

²⁵ Medical Identity Theft Environmental Scan, Oct. 15, 2008, p. 4.

²⁶ Medical Identity Theft Final Report, Jan. 15, 2008, p. 9.

health information. Under HIPAA, individuals have the right to request amendment of their PHI.²⁷ A resource developed by the American Health Information Management Association (AHIMA) describes the process as follows:

If the healthcare entity knows the health information was never used in any treatment or payment decisions related to the victim, the healthcare entity can “separate” the information and create a new record for the perpetrator. In effect, the erroneous information is deleted from the victim’s medical record. This is generally accomplished more easily with paper records. For electronic records, it may be very costly, cumbersome, and sometimes impossible to separate the data.

An amendment problem arises when the perpetrator’s health record is used to make treatment or payment decisions related to the victim. In these situations, the record cannot be separated because, rightfully or wrongfully, a decision was made using the erroneous information. Instead, healthcare entities must follow longstanding requirements of striking through or amending erroneous information without actually deleting the misinformation from the victim’s record. Healthcare entities can and should link the amendment directly to the erroneous information in a very noticeable manner.²⁸

Covered entities are also obligated under HIPAA to send the amended information to other parties (e.g., other providers, health plans, etc.) in certain cases.²⁹

V. Related issues

5.1 The good idea that wouldn’t fly: the Unique Patient Identifier

In 2008, the Rand Corporation released a study of the costs, benefits and privacy implications of adopting a unique patient identifier (UPI) for each individual.³⁰ The study concludes that broad adoption of a UPI “is clearly desirable for reducing errors, simplifying interoperability, increasing efficiency, improving patient confidence, promoting NHIN [National Health Information Network] architectural flexibility, and protecting patient privacy.”³¹ The authors acknowledge that protection of privacy and security is inadequate under existing law, but that the real issue is moving forward with interoperability while legal protections evolve.

²⁷ 45 C.F.R. § 164.526.

²⁸ Smith, *Applying HIPAA to Identity Theft*, in *Medical Identity Theft*, American Health Information Management Association, 2008 (Nichols, Ed.) p. 65.

²⁹ 45 C.F.R. § 164.526(c)(3).

³⁰ Rand Corporation, *Identity Crisis: An Examination of the Costs and Benefits of a Unique Patient Identifier*, available at http://www.rand.org/pubs/monographs/MG753/?ref=homepage&key=t_stethoscope_keyboard.

³¹ *Id.*, p. xviii.

There are two main approaches to linking patients with their health information: use of a single unique patient identifier (UPI), or statistical matching based on more than one personal attribute, such as name, address and social security number. When HIPAA was adopted, it called for development of a UPI, in addition to adoption of identification numbers for providers (the National Provider Identifier, or NPI) and employers. While the NPI and employer identifier are in use, development of the UPI ran into substantial opposition. HHS published proposed rules in 1997, and subsequently the National Committee on Vital and Health Statistics held hearings at which various parties opposed adoption of a UPI based on privacy concerns. In reaction, Congress prohibited HHS from pursuing development of a UPI without express Congressional authorization. As a result, the health care industry has relied on statistical matching.

When statistical matching is used, errors can arise because the personal data used may not be unique to the individual (e.g., multiple individuals share the same name), change over time, and are subject to data entry errors. Errors can lead to records which relate to different people being considered to relate to one person, or to some records of a single individual being deemed to relate to different people. Estimates of such errors average around 8%.

Existing systems frequently rely on the Social Security Number (SSN) as one identifier. The SSN is subject to data errors, because it does not include check digits (numbers formed from an arithmetical process on other digits in the number that allow for automated detection of errors). Also, widespread use of the SSN increases the risk of identity theft.

Authors of the Rand Corporation study estimate that while adoption of a UPI would cost between \$1.5 to \$11.1 billion, the cost is justified by removing the systemic potential for medical error due to inadequate record retrieval systems.