ReedSmith

Reed Smith LLP
1301 K Street, N.W.
Suite 1100 - East Tower
Washington, D.C. 20005-3373
+1 202 414 9200
Fax +1 202 414 9299
reedsmith.com

Carol C. Loepere
Direct Phone: +1 202 414 9216
Email: cloepere@reedsmith.com

MEMORANDUM

TO: American Health Care Association

FROM: Carol C. Loepere
Paul Bond

RE: Red Flag Identity Theft Regulations: Implications for Nursing Facilities and Assisted Living Facilities[1]

DATE: April 17, 2009

I. Introduction: Identity Theft Detection, Prevention and Mitigation

Identify theft has become a top priority for both federal and state governments. Recent federal legislation and regulations have been adopted to deter, detect, and mitigate identity theft. See Fair and Accurate Credit Transactions Act of 2003 ("FACTA"), Pub. L. 108-159, 111 Stat. 1952, codified by amendments to the Fair Credit Reporting Act, 15 U.S.C. 1681 *et seq*. The Federal Trade Commission ("FTC") has created a new division devoted to identity theft. Part of this effort includes the FTC's so-called Red Flag Regulations, 16 C.F.R. § 681.1 and § 681.2 ("Red Flag Regulations"). The Red Flag Regulations have three parts, only the first two of which pertain to the health care industry.[2]

The first part, the address discrepancy portion of the Red Flag Regulations, 16 C.F.R. §681.1, applies to anyone who uses "consumer reports," defined to include credit reports, and requires users of consumer reports to develop and implement reasonable policies and procedures to deal with an address mismatch.[3] The second part pertains to the detection, prevention and mitigation of identity theft in relation to covered accounts by "creditors or financial institutions." These rules became effective **November 1, 2008**, but enforcement of the second rule was delayed until **May 1, 2009**.

---

1 This memorandum is offered for informational purposes only, and does not constitute legal advice.

2 The third part pertains only to debit or credit card issuers.

3 See *Memorandum on the Address Discrepancy Rule* from Reed Smith LLP to the American Health Care Association dated January 31, 2009 providing an explanation of the this requirement, and guidance on developing a policy and task checklist. See AHCA web site at http://www.ahcancal.org/facility_operations/finance/Documents/Address%20Discrepancy%20Memo.pdf

ReedSmith

This memorandum focuses on the second of the Red Flag Regulations, that pertaining to the detection, prevention and mitigation of identity theft in relation to covered accounts by "creditors or financial institutions" and discusses how these rules may impact nursing facilities and assisted living facilities (collectively, "Facilities"). Facilities are clearly not "financial institutions," but under the broad interpretation of FTC staff, Facilities are deemed "creditors" for their private pay and certain payor accounts and therefore are subject to the Red Flag Regulations. Noncompliance, where required, could result in penalties and possibly civil litigation. Therefore, Facilities need to take steps now to develop and implement an identity theft program.

II. The Red Flag Identity Theft Program

The Red Flag Regulations require any business that is a "financial institution or creditor" to "develop and implement a written Identity Theft Prevention Program (Program) that is designed to detect, prevent, and mitigate identity theft[.]"[4] The regulations list more than two dozen examples of "identity theft red flags" a creditor or financial institution might continually look for, both when setting up a new customer account and during the course of a customer relationship.[5] In the long-term care setting, this means that the scope of the duty to protect against identity theft both occurs upon a new admission and is in continuing force for all of the records of residents in the Facility.

A. How to Determine Whether a Facility is a "Creditor"

We normally think of a creditor as someone like a mortgage lender or a credit card company. But, in fact, the FTC has interpreted the term "creditor" to apply to any company that provides goods or services without demanding payment up front. Under agency commentary, "Utility companies, health care providers, and telecommunications companies are among the entities that may fall within this definition, depending on how and when they collect payment for their services."[6]

Our discussions with the FTC staff and FTC staff public statements provide greater clarity for Facilities participating in the Medicare and Medicaid programs. Specifically, if a Facility does not bill residents -- accepts payment in full directly from the Medicare and Medicaid programs, or does not defer payment for services -- then credit is not extended, the Facility is not a "creditor," and the Red Flag Regulations do not apply. However, if a Facility bills residents and defers payment, even for a portion of the cost of services (*e.g.*, for a copayment), the Red Flag Regulations do apply.[7] For example:

---

[4] 16 C.F.R. § 681.2(d)(1).

[5] 16 C.F.R. § 681.2(d). *See also* Supplement A to Appendix A to Part 681 (copy attached at Attachment A).

[6] *See*, Federal Trade Commission, *Fighting Fraud with the Red Flags Rule*, available at http://www.ftc.gov/redflagsrule (*hereafter*, "*Fighting Fraud*"), pp. 9-10.

[7] *Accord*, Federal Trade Commission, Letter from Acting Director of Bureau of Consumer Protection Eileen Harrington to American Medical Association Director of Federal Affairs Margaret Garikes (Feb. 4, 2009) available at http://www.ftc.gov/os/statutes/redflags.pdf (*hereafter*, "*Harrington Letter*").

ReedSmith

- The Smith Home provides services to Mr. Garcia during the month of June, and then sends a bill for those services to Mr. Garcia's insurer in July. By means of that arrangement, the Smith Home has become a creditor to Mr. Garcia within the meaning of the Red Flag Regulations, and subject to the rule's requirements. Similarly, if an ALF provides services to its residents and bills them at the end of the month, the ALF would be considered a creditor to its residents.

- Mr. Jones, a Medicare beneficiary, is a resident of Seaside Manor Skilled Nursing Facility. Seaside Manor bills Medicare for Mr. Jones' care. After 20 days, Mr. Jones is responsible for a copayment, and because he does not have secondary insurance and is not eligible for Medicaid, Seaside Manor bills Mr. Jones directly for the copayment as well as for non-covered services such as his cable television charge. Here, Seaside Manor is a creditor.

In sum, because most Facilities will have some "creditor" relationships under the Red Flag Regulations, Facilities should take steps now to comply with the new rules.

B. Duties Imposed on "Creditors" Under the Regulations

Any creditor has an ongoing duty to protect what are described as "Covered Accounts." An "account" is a continuing relationship established by the resident to obtain services from the Facility.[8] A "Covered Account" is any account offered or maintained by the Facility designed to cover multiple transactions or payments. An account is also a Covered Account if there is a reasonably foreseeable risk to consumers or to the Facility's safety and soundness "from identity theft, including financial, operational, compliance, reputation, or litigation risks."[9] The agreement of a Facility to provide services each month and accept payment after creates a Covered Account. Covered Accounts do not include bank accounts opened and maintained by a financial institution for a resident, even if a Facility is a signatory or has powers as a guardian or conservator for the account. The entity that opens and maintains the account, *i.e.*, the bank, has the obligations under the Red Flag Regulations. In that situation, the Facility's duties are those set forth by contract and by the fiduciary relationship.

C. How "Creditors" Must Protect "Covered Accounts:" Adopt an Identity Theft Protection Program

"Each financial institution or creditor that offers or maintains one or more covered accounts must develop and implement a *written* Identity Theft Prevention Program (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."[10] This written program must be continually reviewed and updated.[11] The written

---

8 16 C.F.R. § 681.2(b)(1).

9 16 C.F.R. § 681.2(b)(3).

10 16 C.F.R. § 681.2(d)(1).

11 *See, e.g.*, *Fighting Fraud*, p. 4 ("because identity theft is an ever-changing threat, you must address how you will re-evaluate your Program periodically to reflect new risks from this crime").

Program must be reviewed and approved by a Board of Directors, a Committee of the Board, or another senior-level employee.[12] "Because your employees have a role to play in preventing and detecting identity theft, your Program must include appropriate staff training."[13]

Significantly, the Red Flag Regulations expressly state that the Program should be "appropriate to the size and complexity of the…creditor, and the nature and scope of its activities."[14] The FTC has indicated that the Rule's obligations are risk-based, meaning that the steps covered entities must take to address potential identity theft should be commensurate with the risks they encounter. Accordingly, as a practical matter, the rules should not impose significant burdens on most providers where the risk of identity theft is low.[15] Red flag risks in some settings may not be present in long-term care. Like HIPAA, there is no "one size fits all" program.

In short, the responsibilities and duties under this final rule boil down to the following:

Upon admission the Facility must:

- Be sure that individuals at the time of admission are who they say they are; [16]
- Develop a set of red flags to alert the Facility to the effect that an individual upon admission does not appear to be who he says he is.[17] Examples of red flags include:
  - Person presenting at admission is not who he/she claims to be;
  - Person using an insurance card that is not their own;
  - Person providing a billing address that is not theirs; and
  - Person presents an insurance card or government program card that appears to be altered or forged.

At that point, the Facility should consider this information in proceeding with the admission.

---

12 *Id.*

13 *Id.* at pp. 4-5.

14 16 C.F.R. § 681.2(d)(1).

15 "For example, for most physicians in a low risk environment, an appropriate program might consist of checking a photo identification at the time services are sought and having appropriate procedures in place in the event the office is notified - say by a consumer or law enforcement - that the consumer's identity has been misused." *Harrington Letter*, p. 8.

16 16 C.F.R. § 681.2(d).

17 16 C.F.R. § 681.2(d).

ReedSmith

There is no duty under the Red Flag rules to report to the FTC or another agency. However, as discussed below, a Facility's response to a forged government program card could be to alert the applicable payor. Also, the Facility may choose to refuse the admission, depending on any restrictions that may apply under state law. In short, the Facility should develop a protocol about how to address these circumstances. This becomes part of the Facility Medical Identity Theft Prevention Program.

On an ongoing basis, the Facility must:

- Be sure that the records of residents – both financial and medical information – are protected from identity theft;[18]
- Develop a set of red flags to alert the Facility that either the financial or medical information of a resident has been or may be about to be stolen; and
- Develop standard responses of what to do in the event of potential medical identity theft. In some cases, the response might be "Contact the Administrator."

D. Ten Steps to Establish an Identity Theft Prevention Program

The following are ten suggested steps extracted from the FTC final rule to assist Facilities prepare and implement a written identity theft program.

1. *Form A Risk Assessment Team*. Before drafting the Program, a Facility may wish to consider assembling a team to perform a risk assessment. The Risk Assessment Team should include individuals from the different departments of the Facility involved in admitting residents, determining medical coverage, safeguarding information about residents, and billing for services (*e.g.*, the admissions department, the business office, the HIPAA Privacy Officer, and the like). Once assembled, the Risk Assessment Team should review how residents' identity is verified on admission, what information is gathered, how that information is stored, and what steps could be taken to augment security.

A Risk Assessment Team is not a regulatory requirement. If one employee is well-versed in all aspects of a Facility's operation, that employee could perform the risk assessment. On balance, however, we believe the assessment would be most effective if the Facility (or the Facility's larger organization) draws from the experience of several departments. The Team should think of every way a would-be identity thief could take advantage of the Facility's relationship with its resident.

2. *Identify Red Flags*. A Facility's written program policy statement should identity theft Red Flags.[19] A Red Flag is a pattern, practice, or specific activity that indicates the possible existence of identity theft. For example, the following are common Identity Theft Red Flags:

[18] 16 C.F.R. § 681.2(d).

[19] *Fighting Fraud*, pp. 17-22.

presentation of documents which look forged, altered, or fake; a suspicious address change; and a resident demanding services or access to health records with unusual urgency or frequency. Of course, any warning from law enforcement or a consumer reporting agency that a resident may be an imposter should be taken seriously. A Facility should also include additional Red Flags from its own experiences with identity theft. Attached is a list of Red Flag suggestions from the Regulations.

3. *Assess the Risk Level.* When the Risk Assessment Team develops a list of the hypothetical ways that imposters could take advantage of the identity of the Facility's residents, the Team should then consider the real-life likelihood of each particular risk coming to pass.[20] Some routes to identity theft are more likely than others. A resident who is being admitted involuntarily is not very likely to be stealing someone else's identity. A resident or family member who is unusually active in demanding treatment or access to medical records deserves a second look.

4. *Determine the Appropriate Response.* Taking into consideration the relevant Red Flags the Facility has identified and the potential risk level for identity theft, including medical identity theft, the Team must then determine the appropriate response to those Red Flags. If the Red Flag is suspicious medical billing on a Covered Account, the response may be to contact the individual to request more information and alert them that someone is using their identify. If the identify theft resulted in billing to a payor for an individual who did not in fact have insurance coverage, the response may be to refund the appropriate payor. If the Red Flag is an address discrepancy, the response may be to ask for additional identification. The response will vary as appropriate to the risk level and the Red Flag detected.

5. *Document Results of the Risk Assessment.* For compliance purposes, it is important for the Facility to document the results of the risk assessment. A well-documented and thought out risk assessment process will help satisfy regulators and may potentially save money by avoiding security breaches and costly litigation and compliance issues.

6. *Prepare the Identity Theft Prevention Program and Assign Responsibility for Oversight*. The next step is to incorporate the findings from the risk assessment and prepare the written Program. Although some of the policies and procedures may already be documented in existing Information Security, HIPAA or other policies, it is a best practice to have a separate document that either sets out separately the Identify Theft Prevention Program or points to the specific places in existing policies that comply with the regulations.

A great program of risk mitigation on paper is only worthwhile if someone actually implements it. Under the Red Flag Rules, the Program is to be overseen by the organization's Board of Directors or a designated committee of the Board, or if no Board, then a designated employee at the level of senior management (collectively "Administrator"). The Administrator may delegate responsibilities but ultimately is responsible for overseeing the Program. For example, the Administrator may delegate

[20] *Id. at* p. 25 ("Your response will depend on the degree of risk posed.").

responsibility for training of employees to a designated person and oversight of service provider arrangements to another.

7. *Obtain Board Approval*. Next, the Board of Directors or a designated committee of the Board, or if no Board, then a designated employee at the level of senior management must review, approve and oversee the Program. Oversight of the Program includes assigning responsibility for the Program's implementation and compliance, reviewing reports prepared by staff, training staff as necessary to effectively implement the Program, overseeing service provider arrangements as appropriate and approving material changes to the Program.

8. *Train Staff*. All staff who open and access Covered Accounts must be trained as necessary regarding the policies and procedures that are applicable to their job function. This would include training upon hiring, refresher training as needed, and training on new policies or procedures when the Program is updated. [21]

9. *Review Service Provider Arrangements.* If a Facility engages service providers to perform services in connection with Covered Accounts (e.g., a billing agent or management company), the Facility must take steps to ensure that the service provider has reasonable policies in place to detect, prevent, and mitigate the risk of identity theft. This can be accomplished by requiring the provider via contract to have policies and procedures to detect relevant Red Flags that may arise in connection with the provision of services and either to report the Red Flags to the Facility or to take appropriate steps to prevent, detect and mitigate identity theft. One approach is to amend HIPAA Business Associate Agreements to include a provision on compliance with the Red Flag Rules.

10. *Annual Report.* Facility staff who has the designated responsibility of development, implementation, and administration of the Program must report to the Administrator at least annually regarding compliance with the Red Flag Regulations. The annual report should address such items as the policies and procedures of the Program, service provider arrangements, significant incidents or identity theft and the responses taken to same as well as recommendations for material changes to the Program. This is likely similar to compliance reports prepared by Facilities.

III. Consequences of Non-Compliance

Under FACTA, the FTC is authorized to bring civil actions in federal court for violations for up to $2,500 for each separate violation. Additionally, the State Attorney Generals are authorized to bring civil actions for their state residents and may recover up to $1,000 per violation and attorney's fees if successful. At least one court has held there is a right to a private cause of action under most of the applicable sections of FACTA.[22] However, the U.S. Court of Appeals for the Seventh Circuit recently

---

[21] The FTC notes that staff only need to be trained as necessary. "Remember, though, that employees at many levels of your organizations can play a key role in identity theft deterrence and detection." *Fighting Fraud*, p. 27.

[22] *See Barnette v. Brook Road, Inc.*, 429 F.Supp.2d 741 (E.D. Va. 2006).

held there was no private right of action.[23] Nonetheless, some states may permit private actions by individuals under various state laws. To our knowledge, there are no plans to actively audit organizations; however, historically, a negative event, such as a security breach, an employee reporting noncompliance or a patient complaint could lead to an investigation by the FTC, which is typically how the FTC operates. Once the FTC finds noncompliance, fines, future audits and ongoing obligations of reporting are possible. Additionally, class actions under state law could follow.

* * *

Please contact us with any questions or comments on this memorandum.

Attachments: Red Flag Suggestions

CCL:rf

[23] *See Perry v. First National Bank*, 459 F.3d 816 (7th Cir. 2006).

ReedSmith

ATTACHMENT A
STATUTORY RED FLAG SUGGESTIONS

In addition to incorporating Red Flags from your Facility's experience with identify theft, applicable regulatory guidance and from your Facility's knowledge of changing identity theft risks, each Facility may consider incorporating into its Program, whether singly or in combination, Red Flags from the following illustrative examples that are set out in the Regulations.[24]

Although all of the following Red Flags may not be applicable to your Facility at this time, it is important that it is documented that the each of the suggested Red Flags below was considered and that periodically the Red Flags mentioned below are reviewed to determine whether as methods of business change, they may be applicable at a future time.

A. 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.
4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of a resident, 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.

B. Suspicious Documents

1. Documents provided for identification appear to have been altered or forged.
2. The photograph or physical description on the identification is not consistent with the appearance of the resident or relative presenting the identification.
3. Other information on the identification is not consistent with information provided by the person opening a new Covered Account or relative presenting the identification.
4. Other information on the identification is not consistent with readily accessible information that is on file with the Facility.
5. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

[24] *See* Supplement A to Appendix A, 72 Fed. Reg. 637441 (Nov. 9, 2007).

ReedSmith

C. Suspicious Personal Identifying Information

1. Personal identifying information provided is inconsistent when compared against external information sources used by the Facility. 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.
2. Personal identifying information provided by the resident, relative or other party responsible for the Covered Account is not consistent with other personal identifying information provided regarding the resident. For example, there is a lack of correlation between the SSN range and date of birth.
3. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the Facility. 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.
4. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the Facility. 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.
5. The SSN provided is the same as that submitted by other persons opening an account or other customers.
6. 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 residents.
7. The person opening the Covered Account or the resident fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
8. Personal identifying information provided is not consistent with personal identifying information that is on file with the Facility.
9. For Facilities that use challenge questions, the person opening the Covered Account or the resident cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

D. Unusual Use of, or Suspicious Activity Related to, the Covered Account

1. Shortly following the notice of a change of address for a Covered Account, the Facility receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.

2. 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 resident, relative or other party responsible for the Covered Account fails to make the first payment or makes an initial payment but no subsequent payments.
3. 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.
4. 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).
5. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the resident's Covered Account.
6. The Facility is notified that the person paying the Covered Account is not receiving paper account statements.
7. The Facility is notified of unauthorized charges or transactions in connection with the Resident's Covered Account.

E. Notice from Residents, Relatives or other parties responsible for the Covered Account , Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection With Covered Accounts Held by the Facility

1. The Facility is notified by a resident, relative or other party responsible for the Covered Account, 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.