Compliance Advisory:

Red Flag Identity Theft Compliance Programs

MEADE & ROACH LLP

October 2008

Health Care Providers Can Leverage Existing Compliance Infrastructure

The compliance date for establishing an Identity Theft Prevention Program is November 1, 2008. The Federal Trade Commission (FTC) issued new "Red Flag" regulations in November 2007 but only recently has the health care industry realized that hospitals and other providers fall under the jurisdiction of the Red Flag Rules. Providers can take advantage of their existing compliance infrastructure and HIPAA privacy and security programs to jump start Red Flag initiatives.

"Red Flags" are patterns, practices or activities that raise questions whether a person's identity information may be in jeopardy. The rules require organizations to monitor the account that is subject to suspicion and undertake an "appropriate response" to prevent or mitigate identify theft.

The Red Flag Rules comprise regulations, a set of "guidelines" and a supplement to the guidelines. These three parts of the Red Flag Rules allow a risk-based approach to Red Flag compliance so that each organization can design its own compliance response. However, there are certain features to the administrative requirements that all Red Flag covered entities must meet by the compliance date. The Red Flag Rules were published simultaneously by a number of federal agencies that regulate "financial institutions and creditors." Health care providers (and most businesses) fall under the jurisdiction of the FTC's regulations, which can be found at 16 CFR §681.2.[1]

"These three parts of the Red Flag Rules allow a risk-based approach to Red Flag compliance so that each organization can design its own compliance response."

In order to meet the deadline, many providers are planning a two part approach that establishes an initial program by the compliance date and a planned evolution to comprehensive Red Flag detection and prevention in the immediate future.

In order to understand the Red Flag Rules, providers can think through the rules under four categories:

1. How to identify a Red Flag
2. Information covered by the Red Flag Rules
3. Required elements of a Red Flag Compliance Program
4. Administrative requirements of a Red Flag Compliance Program

This Compliance Advisory will discuss each of these points and provide 12 steps that a health care provider can take to begin its Red Flag compliance initiative.

How to Identify a Red Flag

The FTC regulations loosely define a Red Flag as any "pattern, practice, or specific activity that indicates the possible existence of identity theft."[2] This definition makes a Red Flag Compliance Program a vigilance initiative and requires providers to train their staff to be on the look-out for suspicious activity.

- The Red Flag Rules' Guidelines list 26 types of activities that could be considered Red Flags, such as:
- Alerts and notifications the organization receives from consumer reporting agencies
- Presentation of suspicious documents (for example, appearance of manipulation of the document)
- Suspicious address changes
- Suspicious activity related to a covered account

1 Some commentators have questioned whether the FTC has jurisdiction over non-profit hospitals. However, the FTC stated in a June 2008 notice that '[w]here non-profit and government entities defer payment for goods or services, they, too, are to be considered creditors' under the Red Flag Rules"

2 16 CFR §681.2(b)(9)

The FTC's examples of Red Flags are extremely broad and not meant to be an exhaustive list. Watching for Red Flags will be a front-line activity for staff and will require active awareness training of the workforce. Providers may also decide to do systemic checks for suspicious activity. For example, when a hospital registers a new patient and collects identifying information, current systems may not check to see whether the identifying information is already being used. Regularly running queries for matches in identical names, addresses, and Social Security Numbers is one way to build into the program active monitoring for Red Flags.

When registering new patients, providers may want to consider whether the identification material they now ask for is sufficient and whether to make copies of the original identification and maintain it in the patient's file.

Once a Red Flag is detected, then a covered account should be "flagged" and a determination made whether the incident reasonably poses a risk of identity theft. The organization must respond to the risk, such as contacting the individual to re-confirm identity or alerting the person to suspicious behavior to double check the authenticity of the incident.

Information Covered by the Red Flag Rules

A "Red Flag covered entity" includes any organization that meets the definition of a "creditor" under the rules. A "creditor" is any organization that provides goods or services and allows the purchaser to make "deferred payments" for the goods or services. When a health care provider establishes an account for a patient that is not paid immediately, then the organization will meet the definition of a creditor. Government commentary to the rules refers to these organizations as "covered entities" but this term is not synonymous with a HIPAA covered entity. Although "HIPAA covered entities" are not automatically "Red Flag covered entities," it is likely that most health care providers will trigger the Red Flag Rules.

Not all information maintained by a creditor is subject to the Red Flag Rules. The rules apply to "covered accounts." A "covered account" is any account that involves deferred payment and a "continuing relationship" with the "customer." As a practical matter, health care providers will likely want to consider all patient accounts to be covered accounts. But health care providers, particularly hospitals, could have more than patient accounts as covered accounts. If a hospital offers deferred payments for goods or services provided to medical staff members or to the hospital's own employees, those transactions would also be considered covered accounts. For example, laundry services or food services in which payment is deferred to a revolving account may be considered covered accounts.

The Red Flag Rules recognize that every organization will have different types of "covered accounts" and requires that Red Flag covered entities conduct a risk assessment to identify its covered accounts.

In the covered account, the information that must be protected and monitored is "identifying information." This is a very broad term that includes virtually anything that could be connected back to an individual, including particularly sensitive information such as a Social Security Number as well as publicly available information such as an address.

Required Elements of a Red Flag Compliance Program

The Red Flag Rules require the identity theft compliance programs to have policies and procedures addressing four elements:

1. identifying relevant Red Flags
2. detecting Red Flags when they occur
3. responding appropriately to Red Flags
4. obligating the organization to update the program periodically

The elements of a Red Flag Compliance Program focus on policies and procedures but these policies and procedures need to be drafted in the context of the organization's unique risks for Red Flags. Implicit in the discussion is that compliance with the policies and procedures would be monitored and enforced. In order to ensure effectiveness of the policies and procedures, providers should consider incorporating the Red Flag Compliance Program into their HIPAA Compliance Programs which already contain privacy and security safeguards for much of the information that could be subject to a Red Flag in a covered account.

The Red Flag policies and procedures are different from HIPAA compliance policies in that the Red Flag policies and procedures are not focused on when information may or may not be used or disclosed, nor are they about how or when information can be secured from inappropriate access. Rather, the Red Flag policies and procedures require active attention and watchfulness among the workforce for activity that signals risks of identity theft.

The Red Flag Rules allow considerable flexibility as to how an organization identifies Red Flags, what it does to respond to Red Flags and how it designs the assessments that need to be done to identify covered accounts and monitor the covered accounts. The regulations contain "guidelines" that must be considered and an associated supplement which provides suggestions for all of these activities.

Administrative Requirements of a Red Flag Compliance Program

Not unlike HIPAA's organizational requirements, the Red Flag

Rules also contain "administrative requirements." The regulations set out four administrative obligations:

1. Board approval of initial Red Flag compliance plan and identification of how subsequent material changes will be approved

2. Training of staff

3. Oversight of "service providers" that may have access to covered account information

4. Consideration of FTC guidelines

Since the administrative requirements do not detail precise obligations, one of the most important actions a provider can take is to document how it believes the organization is meeting the Red Flag administrative requirements.

The Board approval requirement is the most straight-forward of the obligations. The Red Flag Rules are clear that the organization's Board of Directors, or an appropriate committee of the Board, must approve an initial written Red Flag plan. After the initial approval, any material change to the written plan can be approved by a designated member of senior management that the Board has authorized. Of course the material changes can also be approved by the Board if the organization so chooses.

The FTC Guidelines associated with the Red Flag Rules strongly suggest that at least annually a designated individual should provide a report to the Board that 1) assesses the effectiveness of the existing Red Flag Compliance Program; 2) discusses oversight of service providers; 3) identifies significant incidents; and 4) makes recommendations for material changes to the Compliance Program. While the annual report is not a regulatory obligation, it is advisable to implement this FTC suggestion since it can help demonstrate high level oversight of the identity theft prevention program.

As to which staff should be trained on Red Flags, that is deferred to the organization to assess which personnel will be likely to detect patterns, practices or activities that could be signs of identity theft. Since all workforce members for a health care provider must receive HIPAA training, one approach is to incorporate Red Flag training into the organization's regular HIPAA training. Since the rules require that covered accounts be flagged for monitoring when a Red Flag has been identified, organizations will likely want to think about the workforce as divided between individuals who should immediately flag an account in the system and individuals who do not have immediate access to accounts but should report a possible Red Flag to a central authority as soon as possible.

Oversight of service providers is similar to HIPAA's business associate requirement. A "service provider" is any person or organization that provides direct services to a Red Flag covered entity and originates or has access to covered account information. The Red Flag entity must provide "appropriate and effective oversight" of the service provider's measures to assist the covered entity in detecting Red Flags and protecting covered accounts from identity theft. The FTC does not mandate a single way that Red Flag covered entities should approach their service providers, but it suggests that one manner is to require service providers to agree to adopt identity theft policies and procedures. One way to accomplish this administrative requirement is to incorporate identity theft measures into business associate agreements. It seems that all business associates of a health care provider would likely also meet the definition of a service provider, but since a covered account is not confined to accounts that contain Protected Health Information but includes accounts that more generally contain identifying information, the category of service provider may be broader than a health care provider's business associates.

> "This definition makes a Red Flag Compliance Program a vigilance initiative and requires providers to train their staff to be on the look-out for suspicious activity."

The Red Flag Rules have a peculiar fourth administrative requirement. Covered entities must "consider" the FTC's guidelines for detecting, protecting and responding to identity theft and incorporate the suggestions into their programs as may be appropriate. The rules do not mandate incorporation of the guidelines but it would be prudent for providers to adopt as many of the guidelines as feasible since the FTC suggestions create a defensible posture for a Red Flag Compliance Program if it is ever audited.

Steps Providers Can Take to Achieve Compliance

The following are suggestions that health care providers can consider for responding to the Red Flag Rules:

1. Identify who will lead the initiative. While the Chief Compliance Officer or Privacy/Security Officer is not required to be the liaison to the Board under the Red Flag Rules, it may make practical sense for the Compliance Office to lead the initiative since a health care provider compliance program already contains many of the elements needed for Red Flag programmatic compliance. Identifying the Red Flag Official should be one of the first steps an organization takes.

2. Develop a timeline strategy for Board of Directors approval. The organization should determine its capability of constructing a comprehensive plan by the compliance date, or whether the organization should undertake a two part strategy that initially considers all patient accounts as covered accounts, appoints a Red Flag Official, sends a strategic plan to the Board for approval, and issues notices to the

workforce reminding them to be on guard for Red Flags and to report any Red Flags immediately to the Red Flag Official (or his or her designee).

Develop a plan to assess what types of covered accounts the provider maintains. For an initial plan to meet the compliance deadline, providers may want to consider all patient accounts as covered accounts and then undertake a risk assessment to identify other covered accounts they may maintain. Multi-facility providers should consider surveying all facilities and controlled entities to determine what type of covered accounts are being maintained on the local level. Compliance offices should not assume that their only covered accounts are patient accounts or that all patient accounts are covered accounts.

Develop a plan to identify service providers. A vendor that does not interact with covered account information will not be a service provider. A health care provider may want to consider all of its business associates to be service providers so that a more focused review can be done of vendors who have not been identified as business associates.

1. Identify Red Flag categories that are based on the type of covered accounts the organization maintains. A provider should think about past experiences with identity theft as well as HIPAA privacy and security incidents which could inform the organization on the type of suspicious activity that poses a threat to information.

2. Develop a list of specific Red Flags that workforce should be on the look-out for. While Red Flags cannot be limited to specific types of suspicious activity, the more concrete examples the organization can give the workforce, the stronger its compliance initiative will be.

3. Consider mandating responses for certain high risk Red Flags. For instance, if a patient at registration presents a clearly falsified document, the provider may wish to mandate that the registration staff not accept the documentation. Providers may also need to enhance it HIPAA authentication processes.

4. Determine how covered accounts will be flagged for monitoring. Some mechanism must be developed to flag a covered account for review and monitoring. For some organizations this could be achieved with existing technology systems; for others there may need to be a planned upgrade of account systems so that an account can be flagged. Interim measures while technology is being assessed should at least include an immediate report to a designated individual, such as the Privacy/Security Officer who will then work with the appropriate department to review the account and suspicious activity.

5. Draft policies and procedures. The policies and procedures must address identifying, detecting, and responding to identity theft. There must also be a policy and procedure for regular updates to the program.

6. Organize staff training. Since the Red Flag Rules do not require all staff to be trained the same way, nor are timelines set out for training, the provider may want to consider folding Red Flag training into the annual HIPAA training. At the start of the program, the organization should consider informing staff through email alerts to watch for Red Flags. If systems are not in place yet for individuals to "flag" an account for monitoring, then the staff member should report the suspicious activity immediately to a designated individual.

7. Document plan development. Since the Red Flag Rules are risk-based, it is essential that a Red Flag covered entity document its activities and its reasoning in order to defend its choices.

8. Develop an update plan. Part of the initial written plan should include how the organization will monitor for updates to plan and perform a periodic effectiveness check. Organizations should strongly consider committing itself to an annual report to the Board on the effectiveness of the Red Flag Compliance Program.

This is not an exhaustive list of activities that need to be done for Red Flag compliance, but it allows health care providers a place to start and leverages existing compliance infrastructure.

If you have any questions about clinical research compliance, please contact:

Ryan D. Meade at 312.498.7004 or
RMeade@MeadeRoach.com

Michael C. Roach at 312.255.1773 or
MRoach@MeadeRoach.com

Steven W. Ortquist at 312.285.4850 or
SOrtquist@MeadeRoach.com