Closer Look at the Red Flag Rules

Save to myBoK

Chris Apgar, CISSP, consults on information security to the healthcare and financial services industries. He offers this overview of the Federal Trade Commission's red flag rules regarding identity theft protection programs.

* * *

Healthcare organizations must be in compliance with the FTC's red flag rules by May 1, 2009. The rules, which require financial institutions and creditors to establish identity theft protection programs, were included in the Fair and Accurate Credit Transactions Act passed by Congress in 2003.

The final rules were published in the *Federal Register* November 9, 2007, with an original compliance date of November 1, 2008. In October the compliance date was extended to May 1, 2009. The good news for most healthcare organizations is that the requirements represent only a modest expansion of the security incident response teams they have already formed to meet the HIPAA security rule.

Who Must Comply?

Although some recent coverage of the rules has suggested that the inclusion of healthcare entities is a new FTC interpretation, the FTC expected healthcare entities comply with the requirements at least since the final rule was published. Healthcare is specifically referenced in the preamble to the rules with concerns related to medical identity theft.

Under the rules, organizations are considered creditors if they meet either of two criteria. The first is if they maintain "covered accounts." From a healthcare perspective, this would include most patient accounts. A covered account is, in this case, a patient account where the patient is not required to pay for medical services or care at the time of service. A covered account is not just one where the healthcare entity and the patient have entered into an agreement that allows a patient to pay for services over time.

Organizations are also considered creditors if they offer or maintain multiple accounts that involve or permit multiple payments or transactions. This includes a common arrangement in which the provider charges the patient the co-pay at the time of service, submits the claim to the health plan, and later bills the patient for any remaining balance.

What Is Required?

Given that many healthcare entities are under state requirements to respond to breaches of certain patient information (such as Social Security number), they should already be in the business of identity theft protection. The FTC rules, in effect, are intended to ensure this.

Most state identity theft protection laws only address notification of breaches. The red flag rules raise the bar by instituting federal requirements that entities formally implement protection programs, rather than leaving them to implement such programs because they are implied by state notification laws.

The new federal rules are called "red flag" rules because one requirement in building a successful protection program is to identify warnings that a potential identity theft has occurred or is occurring. In other words the program must be preventive.

Identity theft red flags fall into the following categories:

- Alerts, notifications, or warnings from a consumer reporting agency
- Suspicious documents
- Suspicious personally identifying information, such as a suspicious address

- Unusual use of, or suspicious activity relating to, a covered account
- Notices from customers, victims of identity theft, law enforcement authorities, or other businesses about possible identity theft in connection with covered accounts

This list is representative, not inclusive. The bottom line is that healthcare entities must develop and implement policies, procedures, and practices that define events that would trigger an identity theft investigation. They must establish what actions will be taken, how damages would be mitigated, and what steps would be followed to reasonably ensure a similar event does not occur in the future. This also requires formally identifying the flags that would trigger action on the part of the healthcare organization.

No New Teams Needed

It is not necessary for healthcare organizations to form yet another team to comply with the rules. The requirements can be looked on as a modest expansion of the scope of the organization's security incident response team. Covered entities under the HIPAA security rule are already required to have such a team and to have developed and implemented the appropriate policies, procedures, and practices that govern its actions.

Identity theft investigation, for the most part, includes the same steps that a security incident response team must follow—investigate, mitigate, and protect against future occurrences. In most cases the flags that would trigger identity theft investigation represent security breaches that would trigger a response from the security incident response team, regardless.

General guidelines are available from the FTC, the federal banking agencies, and the National Credit Union Administration that may be helpful in developing and implementing a compliant red flag rules program. The FTC indicated it will provide more detailed guidelines in the future. The FTC Web site is a good resource for additional information and to periodically check for updated implementation guidelines.

Original source:
Apgar, Chris. "Closer Look at the Red Flag Rules" (Journal of AHIMA website), November 21, 2008.
