AHANews®

American Hospital Association www.ahanews.com Vol. 44, No. 18 • September 1, 2008

Compliance Deadline for FTC's Identity Theft Provision Fast Approaching

By Mary Ellen Callahan and Daniel Meade

The Federal Trade Commission (FTC) last November issued a "Red Flags Rule" that requires financial institutions and creditors holding consumer or other "covered accounts" to develop and implement an identity theft prevention program. The rule may affect hospitals in several ways; compliance is required by Nov. 1.

The rule is actually three different but related rules:

- Debit and credit card issuers must develop policies and procedures to assess the validity of a request for a change of address that is followed closely by a request for an additional or replacement card. These rules likely apply to few, if any, hospitals.
- Users of consumer reports must develop reasonable policies and procedures to respond to any notice of an address discrepancy they receive from a consumer reporting agency. Hospitals, to the extent they use consumer reports, may be affected by this rule, but this portion of the rule is not the topic of this article.
- Financial institutions and creditors holding consumer or other "covered accounts" must develop and implement a written identity theft prevention program that covers both new and existing accounts. This rule is likely to be the primary source of hospitals' new obligations.

How Hospitals Are Affected

Hospitals likely meet the rule's broad definition of "creditor" and have patient accounts that would fall within the broad scope of "covered accounts." The definition of creditor is drawn from the Equal Credit Opportunity Act and includes anyone who defers payment for services rendered. Most hospitals bill for services previously rendered on either a continuing or *ad hoc* basis, and many aspects of hospital billing therefore may meet the rule's definition of creditor, even if the hospital does not request and/or use a consumer report.

Covered accounts are used mostly for personal, family or household purposes and involve multiple payments or transactions. However, accounts for business purposes that the creditor determines have a high risk of use in identity theft, such as small business or sole proprietorship accounts, also may meet the definition.

The rule and the FTC's guidance specifically identify certain types of relationships – such as automobile dealers, government or non-profit entities or telecommunications providers – where an individual establishes a *continuing relationship* (emphasis added) with the enterprise, including billing for previous services rendered, as covered accounts. There may be certain hospital services, such as emergency department or clinic visits, that as a regular practice are billed and paid for in one lump sum. These services, therefore, may not meet the continuing relationship standard in the covered account definition. But any type of patient account or payment plan that involves multiple transactions or multiple payments likely falls within the definition of covered account in the rule.

The FTC does not have jurisdiction over not-for-profit entities when the entities are engaging in their not-for-profit capacity, and the rule does not expressly address whether it applies to not-for-profit entities. However, the FTC has consistently taken the position that not-for-profit organizations are subject to its jurisdiction when they are engaging in activities that a for-profit entity also would engage in.

In fact, in its July Guidance, "New 'Red Flag' Requirements for Financial Institutions and Creditors Will Help Fight Identity Theft," the FTC states, "[w]here nonprofit and government entities defer payment for goods or services, they, too, are to be considered creditors." Therefore, the FTC likely would claim that a not-for-profit hospital that collects payment information from patients in order to bill them for services rendered falls within the definition of creditor and they would need to comply with the rule.

What's Required for Compliance

Under the rule, hospitals, as creditors holding covered accounts, must develop an identity theft prevention program that includes reasonable policies and procedures for detecting or mitigating identity theft. The program should enable the hospital to:

- Identify relevant "red flags" (patterns, practices and specific activities) that signal possible identity theft and incorporate those red flags into its identity theft program;
- Detect the red flags that have been incorporated into the program;
- Respond appropriately to detected red flags to prevent and mitigate identity theft; and
- Ensure the program is updated periodically to reflect changes in risks.

Hospitals will need their governing boards (or an appropriate committee thereof) or senior management to approve the initial written program. And they will need to obtain board approval quickly to meet the rule's Nov. 1 compliance deadline.

The FTC and federal banking regulators identified examples of the 26 "red flags" that are useful to incorporate into any identity theft prevention program, including address discrepancy; name discrepancy on identification and insurance information; presentation of suspicious documents; personal information inconsistent with information already on file; unusual use or suspicious activity related to a covered account; and/or notice from customers, law enforcement or others of unusual activity related to that covered account. These examples are in supplemental guidance issued as an appendix to the final rule.

The rule allows flexibility for structuring the identity theft prevention program, depending on the types of activities the creditor conducts and the "complexity" of its covered accounts. Because most hospitals would likely only have covered accounts for their patients, some of whom may not have continuing relationships with the hospital, an appropriate identity theft prevention program may not need to be particularly detailed or complex. The program, however, should be written, approved by the board and implemented by all relevant departments throughout all parts of the hospital. Although that requirement to obtain board approval may appear daunting, it is necessary to obtain the approval only for the first written program.

CALLAHAN

MEADE

Many hospitals may have certain procedures in place to flag some address discrepancies. The Red Flags Rule requires that hospitals systematize their procedures and obtain governing board (or equivalent) approval of their programs. Even if this rule does not squarely apply to hospitals, they should consider it and establish a reasonable security program consistent with the rule.

The definitions of "creditor" and "covered accounts" are broad and likely encompass hospitals and their patient accounts. In addition, inadvertent noncompliance may trigger liability with the FTC. Furthermore, having these types of standards in place is an industry best practice. Therefore, establishing written procedures to identify major identity theft risks would benefit hospitals and their billing systems, allowing them to catch deficiencies previously not identified until it was too late.

Mary Ellen Callahan is a partner and Daniel Meade is an associate at Hogan & Hartson, LLP, where they practice in the firm's Privacy group. Hogan & Hartson is the AHA's outside counsel on privacy-related issues.