Meeting the FTC's Red Flag Requirements: How One Organization Developed Its Compliance Plan

by **Nancy Davis** , MS, RHIA

Like many other privacy and security officers, I was vaguely aware of the Fair and Accurate Credit Transactions Act. I knew that the act, passed by Congress in 2003, was intended to provide consumers with protection from identity theft. I knew the Federal Trade Commission (FTC) was in charge of its enforcement. I was just not aware the law affected healthcare providers. I didn't know what I didn't know.

In August of last year I received a health law advisory bulletin titled "Health Care Providers: Don't Miss the Red Flags."[1] I was astounded to find that the act's "red flag" rules applied to healthcare providers. As I began to network with colleagues and review more e-newsletters, I became aware that I was not the only person in healthcare who had been in the dark. Fueling my concern was the quickly approaching compliance date of November 1. (The FTC would later extend that deadline to May 1, 2009.)

As I dug deeper into the requirements I discovered good news: healthcare organizations can meet red flag requirements by building on their established privacy and security practices. Here is what we have developed at Ministry Health Care in Wisconsin to assist us in meeting the compliance requirements of the red flag rules.

Building on Established Policies

While I began working with our legal counsel to establish a compliance process, others within our system were becoming aware of the need through their own professional networks. We soon realized that we had the advantage of established policies and procedures to prevent identity theft. These included a recently updated position statement titled "Patient Identity Theft—Management of an Occurrence."

Using a basic framework for developing a compliance plan and the guidance provided by the FTC, we established a document titled "Identity Theft Prevention Program—In Compliance with the Red Flag Rules." We chose to embed the plan in a privacy policy, which is consistent with how our organization distributes administrative guidance.

Program Composition

Ministry's plan took the following outline:

1. Policy Statement: The policy's intent to establish an identity theft prevention program to detect, prevent, and mitigate identity theft.
2. Program Requirements/Composition.

    a. Administration and Accountability: Addresses oversight and responsibilities for senior leaders, corporate integrity staff, privacy and security officers.
    b. Reporting Structure and Reports: Addresses how relevant identity theft information/incident documentation will be maintained and shared within the organization.
    c. Identification of Red Flags: What the actual red flags may include.
    d. Identification of Red Flag Covered Accounts: For the system, covered accounts included individual payment accounts set up for patients, credit agency accounts for payment and debt collection, and occupational health services accounts for employee-sponsored wellness activities.
    e. Verification of Identity of Patients/Others: The policies and procedures in place for identity verification (e.g., in person, by phone, etc.).

f. Responding to Identity Theft Incidents: Policies and position statements that provide guidance that include "Patient Identity Theft—Management of an Occurrence"; "Security Incident Response and Reporting"; and "Responding to Privacy Complaints."
g. Other Related Administrative Guidance: All supporting policies and position statements along with a brief summary of each. (See sidebar for summaries.)

- Business associate agreements as required by HIPAA
- Disclosure of protected health information
- Management of a patient identity theft occurrence
- Response to a privacy complaint
- Security incidence response and reporting
- Management, use, and disclosure of Social Security numbers
- Identity verification of individuals requesting access to patient protected health information
- Verification of patient identity

3. Ongoing Program Evaluation: Responsibilities of the program manager.
4. Business Associates/Service Providers: Addresses third-party relationships and the need for established safeguards and compliance (accomplished through a HIPAA-compliant business associate agreement).
5. Regulatory Enforcement: The FTC's role in compliance.
6. Approval of the Program: Approval required at the board of directors level.
7. Other: Attachments, related policies and position statements, applicable regulations, applicable Joint Commission standards, sources, etc.

The FTC and other organizations offer online resources to assist healthcare providers in complying with the rules (see the resource list below).

While these and other valuable resources are available, an identity theft prevention program should be designed to address the needs of the organization. Adopting a pre-existing template from another source will work if the time is taken to customize the template to the organization's needs and established practices. Ministry's legal counsel assisted in developing the plan. Also key was representation on the work group from risk management, IT, compliance, HIM, patient accounting, and patient registration.

Once the plan was completed, the organization's focus turned to implementation and staff education and awareness. These activities will be carried out through presentations to privacy and security officials first and then additional staff through presentations, newsletter articles, and other reference tools as needed.

Supporting Administrative Policies and Position Statements

Ministry Health's red flag plan builds upon its privacy and security policies already in place. The plan cites the organization's following resources:

Business associate agreements as required by HIPAA. Policy addressing the HIPAA requirement to obtain business associate agreements with those vendors and business associates who provide services on behalf of Ministry Health Care that involve the use of patient protected health information.

"Disclosure of Protected Health Information." Comprehensive policy addressing release of patient information and requirements prior to disclosure of patient information in response to external requests.

"Patient Identity Theft—Management of an Occurrence." Position statement initially created as a proactive response to identity theft in 2004; revised in 2008. Includes current guidance, FTC recommendations, and most importantly a checklist of steps to carry out when investigating identity theft.

"Responding to Privacy Complaints." Policy providing guidance to privacy officers and others in responding to patient privacy complaints. The policy also includes the following tools for enterprise and local use: privacy-

related complaints log (sample); privacy-related complaint investigation record (sample); recommended involvement in privacy complaint investigation matrix; and quick tips for privacy investigations.

"Security Incidence Response and Reporting." Policy establishing guidelines for the identification, response, reporting, assessment, analysis, and follow-up to information security incidents. An information security incident is a violation or imminent threat of violation of information security policies, acceptable use policies, or standard security practices that includes identity theft.

"Social Security Numbers—Confidential Management, Use, and Disclosure." Policy providing guidance on how Ministry Health Care collects, manages, and shares the confidential Social Security numbers of patients, providers, and work force members.

"Verification of Identity for Individuals Requesting Access to Patient Protected Health Information." Position statement establishing practices for verifying identity of individuals inquiring about patient information after the encounter phase (e.g., telephone inquiries regarding account information).

"Verification of Patient Identity." Position statement addressing patient verification at the time of the encounter, specifically during the registration process. Provides guidance to acceptable forms of identity verification when deemed appropriate. Patient identity verification may be established by review of the following documents produced by the patient (a photocopy of the documents may be obtained for reference): driver's license or other governmental identification that includes picture verification; Social Security card; student ID card; passport; insurance card; other photo ID or substantiating document (e.g., correspondence from governmental, utility, or other established entity).

Note

1. Davis Wright Tremaine, LLP. "Health Care Providers: Don't Miss the Red Flags." *Health Law Advisory Bulletin,* August 2008. Available online at www.dwt.com/practc/healthcr/bulletins/08-08_RedFlagRules(print).htm

Resources

American Hospital Association. "Red Flag Rules Resources." October 2008. Available online at www.aha.org/aha/advocacy/compliance/redflags.html.

Federal Trade Commission. "New 'Red Flag' Requirements for Financial Institutions and Creditors Will Help Fight Identity Theft." June 2008. Available online at www.ftc.gov/bcp/edu/pubs/business/alerts/alt050.shtm.

Gellman, Robert, and Pam Dixon. "Red Flag and Address Discrepancy Requirements: Suggestions for Health Care Providers." World Privacy Forum. September 24, 2008. Available online at www.worldprivacyforum.org/pdf/WPF_RedFlagReport_09242008fs.pdf.

Nancy Davis (nancy.davis@ministryhealth.org) is director of privacy/security officer at Ministry Health in Sturgeon Bay, WI, and cochair of the AHIMA 2008 Privacy and Security Practice Council.

Article citation:
Davis, Nancy. "Meeting the FTC's Red Flag Requirements: How One Organization Developed Its Compliance Plan" *Journal of AHIMA* 80, no.2 (February 2009): 48-49.