



## 3 steps for improving 'red flag' compliance

The new rules on identity theft “red flags” and address discrepancies from the Federal Trade Commission (FTC) require financial institutions and creditors—including hospitals—to implement programs for detecting, preventing, and mitigating identity theft.

According to the FTC, identity theft results in billions of dollars in losses to individuals and businesses each year. Under FTC rules, each financial institution or creditor that holds a consumer account must develop “reasonable policies and procedures for detecting, preventing, and mitigating identity theft” (“Agencies Issue Final Rules on Identity Theft Red Flags and Notices of Address Discrepancy,” FTC, Oct. 31, 2008). Additionally, these organizations are required to develop procedures for verifying consumer addresses and dealing with address discrepancies (such as when a hospital attempts to verify patient demographic information and discovers a discrepancy between the address reported by a consumer and the address listed by credit reporting agencies).

The FTC assures the healthcare community that the red flag rules should not prevent any organization from providing medical services to a patient. Instead, the agency is asking providers to become active participants in curbing identity theft. Many hospitals are going beyond the FTC requirements of detection, identification, and action on possible identity theft incidences. They are taking proactive steps to prevent identity theft before it occurs.

Until the red flag rules were established, most hospitals discovered identity theft cases after medical services were rendered and the patient released—often resulting in unrecoverable expenses. Now, instances of identity theft could result not only in a loss of revenue, but also in potential government fines if processes to prevent identity theft are not in place and used consistently.

There are three actions hospitals can take to mitigate their risk and improve their compliance with the recent FTC regulations.

### Step One: Be Proactive

The FTC has mandated providers to become both proactive and reactive in their approaches to preventing identity theft. Establish controls that dramatically limit access to Social Security numbers (SSNs) and other patient identification information internally and to third parties (e.g., collection agencies) to prevent internally generated cases. Patient folders should be stripped of all mentions and photocopies of government IDs. Minimizing the internal theft of patient identification will have the most significant impact on reducing both red-flag instances and losses from identity theft.

### Step Two: Involve Other Departments

Securing patient information cannot be achieved by finance and administration alone. Other departments, such as human resources and healthcare information management (HIM)/medical records, also need to become actively involved in the process.

For example, human resources staff have access to identification, such as SSNs and driver's license numbers, that is attractive to identity thieves. Hospitals should be sure this information is secure and accessed only by those who need it.

As new hires are made, human resources managers should pay attention to any background checks that include identity theft citations or convictions. These individuals should have very strict controls placed on their access to patient information—or be given no access at all—and their activities should be monitored frequently.

Human resources managers also should teach new hires about the red flag rules and, if appropriate, the new hires' role in compliance. This will specifically

impact registration and billing staff; however, all hospital staff should be made aware of the need for strict controls regarding access to patient identification information.

The HIM/medical records department also is critical in reducing opportunities for in identity theft and ensuring compliance with the red flag rules. Its staff should work with finance and administration to identify new user permissions and controls to protect the electronic storage of government IDs in patient folders (until removed) and the secure database where this information will reside. The department should also review its current procedures for detecting misuse of passwords that provide access to identification information.

Paper copies of patient folders containing personal identification information should be removed. Medical records staff are critical to performing this task, as they know where this information is kept. Members of this department will be instrumental in developing a plan that will govern the information kept in patient folders going forward as well as how to “clean” existing and former patient documentation.

**Step Three: Develop Industry Best Practices**

Providers should team together to share their programs and aid one another in developing best practices for protecting patient identification data and dealing with address discrepancies.

The following are examples of industry best practices that hospitals are considering and/or including in their red flag rules programs.

**Red flag policy triggers.** Managers will be immediately notified when:

- > Personal information provided by the patient is inconsistent with current patient information residing in its systems
- > A patient’s identification documents appear to have been altered
- > The hospital is advised of unauthorized charges applied to bank or credit/debit card accounts from their organization

When a fraud alert is associated with a patient account, the information should be verified with the guarantor or disregarded if unable to validate.

**Proactive protection of patient accounts.** The following steps should be taken to protect patient identity:

- > All patient web sites or portals containing patient information should be password protected.
- > Date of birth or SSN of the account guarantor should be verified on all inbound phone calls requesting account information.> Requests for medical documents and/or patient statements should only be sent to the address on record for the guarantor.
- > Physician/health provider offices should be provided with an identification code that would be required when requesting account information.
- > A photo ID (for in-person requests) or the patient’s date of birth and/or SSN (for phone requests) should be required to change the name and/or address on a patient’s account.

**Payment/refund controls.** All credit card payments given via phone should require the submission of the identification number located on the back of the card. And all patient refunds should be mailed to the address of the guarantor or refunded to the original credit/debit card used for payment.

**Policy changes.** The organization should periodically update its red flag rules program based on its experience with identity theft and the availability of new solutions to detect, prevent, and mitigate identity theft.

**Taking a Proactive Stance**

Virtually all hospitals must comply with the FTC’s rules regarding identity theft red flags and notices of address discrepancy. Each hospital’s red flag rules compliance program will be unique. Your organization’s red flag policy should reflect a strong due diligence process with a goal of decreasing premature filings, or false positives.

For more information on the FTC’s red flag rules, visit [www.ftc.gov](http://www.ftc.gov). ●

---

Bruce Nelson is vice president sales and marketing, Search America, Inc., Maple Grove, Minn. ([bruce.nelson@searchamerica.com](mailto:bruce.nelson@searchamerica.com)).

Tina Eller is vice president revenue cycle services, Search America, Maple Grove, Minn. ([tina.eller@searchamerica.com](mailto:tina.eller@searchamerica.com)).