

Medical News, Inc.

YOUR PRIMARY SOURCE FOR PROFESSIONAL HEALTHCARE NEWS

[Home](#)[About Us](#)[Publications](#)[Advertising](#)[Contact Us](#)[Subscriptions](#)[Member Options](#)

Addressing the Medical ID Theft Crisis

By: LYNNE JETER

[Printer-friendly format](#)



Medical identification (ID) theft is among the fastest-growing concerns facing the healthcare sector. Nine of 10 hospitals remain noncompliant with the federal FAST Act Identity Theft Red Flags Rule, with many unaware of the consequences.

What's at risk? Patients' health, lawsuit liability for doctors and hospitals, and mounting debts as a result of improper billing are among the most important issues. Also, medical ID theft is more difficult to trace than financial ID theft, because the labyrinth paper trail challenges the medical community to unravel the origination of errors.

Compliance Coach, the nation's leading provider of automated regulatory compliance solutions, released the Red Flags Compliance Survey Results & Best Practices report on Oct. 31, 2008, the day before compliance was mandated. The survey, distributed to 100 hospitals across the United States to assess the level of preparedness and compliance with the rule, revealed that 91 percent were not yet in compliance; 73 percent were surprised to learn the rule applied to them; and nearly 60 percent indicated it would cost \$10,000 or more to comply.

Of those surveyed, 55 percent represented large hospitals, with gross receipts of more than \$6.5 million; 41 percent reflected medium hospitals, with gross revenues between \$1 million and \$6.5 million; and 5 percent were small hospitals, with gross receipts of less than \$1 million. One in three respondents said their organization had experienced medical ID theft within the last 12 months.

"It's critical for healthcare professionals to receive more education about good privacy practices and appropriate interpretation of HIPAA and other regulations," said American Health Information Management Association (AHIMA) president Wendy Mangin, director of medical records and privacy officer at Good Samaritan Hospital in Vincennes, Ind.

The Red Flags Rule applies to financial institutions, such as banks and credit unions, and creditors. Hospitals fall under the heading of creditor, which is broadly defined as an entity that regularly extends or arranges for credit or defers payment for goods or services.

The deadline for compliance with the rule, mandating the development and implementation of a written identity theft prevention program, was Nov. 1. The Federal Trade Commission (FTC), which has jurisdiction over creditors under the rule, has said it would not enforce compliance until May 1, 2009.

Mangin said that AHIMA has prioritized educating healthcare professionals on privacy and security issues within the health information industry.

Recently, she pointed out, AHIMA's House of Delegates voted to approve a resolution that asked AHIMA members to call on healthcare organizations to educate users of health information about the need for improved and consistent patient privacy and security; that health information management professionals be on the forefront of educating about auditing and monitoring access to health information; and that AHIMA endorse consistent healthcare policies and standards when a breach does occur.

In early 2008, San Diego, Calif.-based Compliance Coach launched a user-friendly, Web-based software that employs a five-step system to enable quick and efficient compliance with the Red Flags Rule. The software represents one of few solutions available for hospitals to use for compliance with the rule.

"Hundreds of financial institutions and creditors of all sizes and types throughout the United States have already used CompliancePal to attain compliance," said Compliance Coach CEO Sai Huda. "CompliancePal is an extremely timely and cost effective solution for the medical community ... saving hundreds of hours and thousands of dollars in compliance costs."

CompliancePal walks the user through a series of questions and produces the required risk assessment, the mapping of red flags to appropriate detection-and-response procedures, the written program, the training materials, and the compliance status report—all that is required to pass an audit. The software contains 65 red flags, including those related to medical ID theft and the government's 26 red flags. Updated routinely to address new ID theft schemes and red flags, it enables a hospital to easily update its ID Theft Program and maintain compliance.

Huda's compliance best practices for hospitals to follow to comply with the Red Flags Rule:

- Formulate a compliance committee to implement compliance with the Red Flags Rule.
- Perform an inventory to identify all patient accounts and service providers. Use a worksheet to document an audit trail.
- Use the risk factors in the rule to perform a risk assessment to identify covered accounts. Aggregate similar accounts into an overall category, and identify the level of risk as high, medium or low. Use a worksheet for the risk assessment, again to document an audit trail.
- Consider the 26 red flags in Appendix J to the rule, but also red flags from historical incidents of ID theft cases. Document the analysis.
- Map applicable red flags to one or more detection-and-response procedures for each covered account.
- Develop a risk-based written Identity Theft Prevention Program, making sure it includes service provider oversight procedures. Obtain and document board approval, and educate board members on the non-compliance risks. Implement a change management process to periodically update the program as needed or mandated under the rule.
- Train staff on how to implement the program; document that training.

[American Health Information Management Association](#), [CompliancePal](#), [federal FAST Act Identity Theft Red Flags Rule](#), [medical identification](#), [Red Flags Rule](#)

[Login and voice your opinion!](#)

Do you know someone else who would like to see this?

Your Email:

Their Email:

Comment:

(Will be included with e-mail)

[Send to a friend](#)

Copyright © and Trademark ™ 2008 All Rights Reserved
[Copyright Statement](#) | [Privacy Statement](#) | [Terms of Service](#)

Expect More from Bondware's Website Design Tools
Email Marketing & Web Design | eCommerce, HOA, Publishing, Non-Profit, Intranet, Real Estate & Association Websites