Red Flags Rules: Hospital Compliance Report

As Data Breaches Increase, Identity Theft Prevention Programs Continue to Challenge Hospitals

National Survey of Hospitals
Conducted by Identity Force
March 24 – 30, 2009

Report Issued April 22, 2009

© Copyright 2009 Identity Force

Identity Force.™

Red Flags Rules: Hospital Compliance Report

Preface

The survey referenced in this report was conducted with executives from 74 hospitals in 34 states across the United States. Identity Force believes this sample size identifies notable trends, and that the survey establishes a reliable snapshot of Red Flags Rules compliance efforts being undertaken by hospitals. The results may reflect the characteristics of executives who have a heightened awareness of Red Flag Rules. Additionally, self-reports of compliance do not necessarily indicate true compliance (which can only be determined by an enforcement agency).

Identity Force's extensive interaction with hospitals and health care facilities has consistently found leadership teams committed to the highest level of compliance, and working diligently to meet their obligations and responsibilities.

Executive Summary

A national survey conducted by Identity Force found that hospitals in the United States are struggling to comply with the Federal Trade Commission's Red Flags Rules. Further, the study discovered that data breaches occur with regularity at these facilities.

Introduction and Purpose

The online survey was conducted with hospital executives from March 24 to 30, 2009, just four weeks before the Red Flags Rules enforcement deadline of May 1. Seventy-four hospitals from 34 states participated in the study. Respondents included Chief Privacy Officers, Chief Financial Officers, Chief Information Security Officers, Chief information Officers, Compliance Officers and their director-level equivalents.

The purpose of the study was to evaluate whether organizations are in compliance with Red Flags Rules, the new identity theft regulations that went into effect on November 1, 2008. The Federal Trade Commission extended its enforcement deadline of the law until May 1, 2009. Additionally, the study examined the number of data breaches hospitals experience, who is leading compliance efforts, and the program components that are included in Red Flags Rules programs.

Federal Trade Commission Position on Hospital Compliance

The FTC has specifically addressed the need for hospitals to comply with Red Flags Rules:[i]

- "Under the Red Flags Rule, which went into effect on January 1, 2008 *, certain businesses and organizations — including many doctor's offices, hospitals, and other health care providers — are required to spot and heed the red flags that often can be the telltale signs of identity theft."

- "Although every business or organization with an ongoing relationship with consumers should keep an eye out for the possibility of identity theft, health care providers should pay particular attention to the requirements that the Red Flags Rule applies to "creditors."

- "Health care providers are creditors if they bill consumers after their services are completed. Health care providers that accept insurance are considered creditors if the consumer ultimately is responsible for the medical fees."

** On October 22, 2008, the Federal Trade Commission issued an Enforcement Policy statement that delayed enforcement of the Red Flags Rule until May 1, 2009*

KEY SURVEY FINDINGS

Some progress, but many "red flags"

I. Compliance with Red Flags Rules

- Only 17.5 percent of hospitals reported that they were in compliance with Red Flags Rules.

- Of the 82.5 percent not yet in compliance, 52.7 percent indicated that they were working towards compliance, and 24.3 percent said that they were still evaluating options.

- Questions remain about the completeness of Red Flags Rules programs (either in place or planned), even at facilities that are either in compliance or "in the final stages" (see section III).

II. Frequency of Data Breaches

- 63.3 percent of hospitals reported that they experience at least one data breach annually.
- Nearly 20 percent reported that they experience 10 or more data breaches annually.
- These findings indicate that data breaches may be under-reported by hospitals and that compliance with data breach notification laws that are in place in 44 states is in question.

III. Completeness of Compliance Efforts

- 51.1 percent of facilities reported that they will not have their employees trained in Red Flags Rules compliance by May 1, 2009 (*Note: this is a requirement of the new law*).
- 44.5 percent reported that they will not have an incident tracking program in place that includes features like risk analysis, investigation and reporting (*Note: this is a requirement of the new law*).

- Only 48.6 percent of hospitals said that their Red Flags Rules program has or will introduce significant changes in policies and procedures (e.g. identity theft training, incident tracking, incident risk assessment, state by state legal compliance, etc.).
- 50% of hospitals report that their Boards of Directors have not approved their Red Flags Rules programs (*Note: this is a requirement of the new law*).

IV. Who is Coordinating Compliance Efforts?

- 56.7 percent of facilities reported that privacy or compliance officers are leading operational implementation of Red Flags Rules.
- In facilities where Red Flags Rules compliance is being led by departments other than privacy or compliance, the survey found that efforts are divided among a wide set of other departments. (Revenue Cycle (12.1%), Chief Information Officer/IT (8.1%), Health Information Management (4.0%), Legal and Chief Financial Officer (2.4% each).)

© Copyright 2009 Identity Force

Identity Force.™

ANALYSIS OF FINDINGS

Delaying the Red Flags Rules deadline hasn't helped hospitals. Compliance decreases while data breaches increase.

The Good News

- Hospitals are aware of Red Flags Rules.

- Many hospitals are working to comply with Red Flags Rules.

The Bad News

- Identity Force expects the **majority of hospitals will not be in compliance** of Red Flags Rules by the May 1, 2009 enforcement deadline. Non-compliance will put most facilities at risk for regulatory action, including fines of up to $11,000 per day. The facilities with the highest risk will include those that suffer data breaches.

- Identity Force sees a **disconnect between compliance efforts underway and actual compliance requirements**. Compliance is more than just a written policy, it also requires training, risk analysis, incident tracking, reporting and Board of Director approval.

    - The inadequacy of compliance efforts is apparent not only in the responses to questions relating to program components, but also in the fact that **less than half of hospitals** surveyed said that their Red Flags Rules program has or will introduce significant changes in policies and procedures.

- The number of **data breaches at hospitals is alarmingly high** – more than 60 percent of hospitals have at least 1 breach annually, and nearly 20 percent have more than 10 each year.

- It is evident to Identity Force that **compliance with current breach notification laws is a question that deserves further study**. The survey uncovered a frequency of data breaches that is not in synch with the number of publicly disclosed breaches reported in the media or by sites such as The Open Security Foundation (http://datalossdb.org/). If these findings hold true, it may be a forewarning of potential compliance issues with future regulations and audit requirements outlined in the recently enacted stimulus legislation.

Identity Force.™

CONCLUSION

Overall, the delaying of the Red Flags Rules enforcement deadline has not helped hospitals. Medical Identity Theft and data breaches are increasing, yet compliance efforts are woefully behind schedule.

The state of non-compliance is due either to the fact that compliance with meeting the standards set forth by Red Flags Rules to protect patients from identity theft is either a low priority for hospitals, or it is too complex a task for mid- to large-sized hospitals to satisfy internally.

Additionally, it is clear that data breaches are occurring regularly at hospitals. The question is not *if* a facility will have a breach, but *when* and how often they take place. Breaches put organizations at significant risk. Their financial implications are onerous; in fact The Ponemon Institute reports that a significant breach can cost an organization more than $6 million. Breaches also damage an organization's reputation and relationships with patients, staff, regulators, the media and the public.

Recommendation

Identity Force recommends that hospitals explore the option of implementing an outsourced program that can eliminate data breaches and bring organizations into immediate compliance with all state and federal identity theft-related laws, including Red Flags Rules.

For more information contact Derek Beckwith (**derek@beckwithpr.com** or 617-331-3567), visit **www.identityforce.com**, or call 1-877-IDFORCE.

Identity Force's Identity Protection, Compliance and Data Breach Solutions have the exclusive endorsement of the American Hospital Association (AHA).

American Hospital Association Comments

Lawrence Hughes, Assistant General Counsel for Advocacy and Public Policy for the American Hospital Association, offered his thoughts on the survey: *"Identity Force's survey suggests that hospitals' awareness of the Red Flags Rule is high and that many have made significant strides in their compliance efforts. But, with the FTC ending its 6-month enforcement delay on May 1, it is important that all hospitals step up their compliance efforts to ensure that they are fully prepared to recognize and respond appropriately to warning signs and other suspicious activities that might suggest identify theft."*

Additional Resources

Identity Force: For more information and to download a copy of the Identity Force National Survey of Hospitals, visit Identity Force: **www.identityforce.com**

American Hospital Association: AHA News article on **Red Flags Rules**

AHA Solutions: **Endorsed solutions** available to hospitals

Federal Trade Commission Red Flags Rules Web site: **http://www.ftc.gov/redflagsrule**

[i] Excerpts from: Federal Trade Commission. *"The "Red Flags" Rule: What Health Care Providers Need to Know About Complying with New Requirements for Fighting Identity Theft."* September, 2008. Article accessed on April 16, 2009 from http://www.ftc.gov/bcp/edu/pubs/articles/art11.shtm.