

Spring 2010 National Survey of Hospital Compliance Executives

Slow Hospital Compliance with New Regulations Causing Increased Data Breaches & Medical Identity Theft

- Compliance continues to lag as nearly 85% of hospitals are NOT in compliance with the HITECH Act
- Breaches up over 120% -- 41% of hospitals now have 10 or MORE data breaches annually
- Potential patient ID fraud and misuse going un-investigated as 34% of hospitals keep inadequate photo ID records and 70% investigate less than 1 case per week
- 56% of hospitals expect new Healthcare Reform Law to either make no difference or to actually increase medical identity theft

Identity Force.™

National Survey of Hospital Compliance Executives

Conducted by Identity Force

March 30 to April 13, 2010

Report Issued April 20, 2010

2010 HITECH Act Hospital Compliance Report

Preface

The survey referenced in this report was conducted between March 30 and April 13, 2010 with compliance executives from 220 hospitals in 43 states across the United States. Participation in the survey was secured via e-mail outreach by the American Hospital Association.

Executive Summary

A national survey conducted by Identity Force found that the pandemic of data breaches and medical identity theft remains at critical levels throughout hospitals in the United States despite new regulations, including the HITECH Act, meant to protect the security of patients' personal information.

The survey revealed a number of significant issues that raise questions on whether the regulations are or will be effective:

- **PROBLEMS ARE WORSENING DESPITE MAJOR REGULATORY EFFORTS:**
41.5% of hospitals have TEN OR MORE Data breaches each year – a 120.7% increase over last year's survey. Currently, over 20% percent of hospitals have TWENTY OR MORE breaches annually.
- **EVEN NATIONAL HEALTHCARE REFORM NOT EXPECTED TO HELP:**
56.3% of hospital compliance officers believe that the new health care reform law will either have no change or will increase medical identity theft at their institutions.
- **INVESTIGATION OF FRAUD IS SURPRISINGLY LOW:**
Despite the fact that medical identity theft is the fastest growing form of identity fraud, 71.4% of hospitals on average investigate fewer than 50 cases of possible misuse of identity annually, and over 34% still do not keep good patient ID records.
- **TIMELINESS OF COMPLIANCE IS POOR:**
To date, only 15.7% of hospitals feel they are in compliance with the HITECH Act, which went into effect in February 2010. This lack of compliance mirrors last year's slow compliance efforts regarding the FTC's Red Flags Rule.
- **SECURITY OF 3RD PARTIES IS AN UNKNOWN:**
48.3% of hospitals do not know if their vendors and business associates are in compliance with the HITECH Act.

Introduction and Purpose

The electronic survey was conducted with hospital executives from March 30 to April 13, 2010 approximately six weeks after the enforcement deadline for the Health Information Technology for Economic and Clinical Health (HITECH) Act, and over a year after hospitals began preparing for the FACT Act Red Flags Rule.

Two hundred and twenty hospital executives from 43 states participated in the study. Respondents included Chief Privacy Officers, Chief Financial Officers, Chief Information Security Officers, Chief Information Officers, Compliance Officers, HIPPA Officers and their director-level equivalents.

The purpose of the study was to evaluate whether hospitals are in compliance with the HITECH Act, and to evaluate whether state and federal data breach and security laws and regulations have had an impact on identity theft-related matters.

Studies conducted by other reliable organizations have also raised concerns regarding the security of personally identifiable information (PII) and electronic health records (EHR) in the health care marketplace, and its impact on hospitals and patients.

- Fraud resulting from exposure of health data has risen from 3% in 2008 to 7% in 2009, a 112% increase. (Javelin Strategy and Research)
- Nearly 1.5 million Americans have been victims of medical identity theft with an estimated total cost of \$28.6 billion. (Ponemon Institute)
- It takes more than twice the time to detect medical information fraud and the average cost is \$12,100, more than twice the cost for other types of identity theft. (Javelin Strategy and Research)
- Victims of medical identity theft may receive the wrong medical treatment, find their health insurance exhausted, and could become uninsurable for both life and health insurance coverage. (World Privacy Forum)
- Data breaches not only put people at risk of becoming victims, they are costly to the organizations that suffer breaches. A 2009 study revealed that the average cost of a data breach – per record breached -- has risen to \$202 from 2008's \$197. At that rate a breach of 5,000 records will cost over \$1 million. (Ponemon Institute)
- Despite requirements that data be encrypted, the U.S. Department of Health and Human Services has announced that between January 1 and March 9, 2010 at least 74,962 unencrypted health records had already been breached. (HHS)

The following pages outline our findings in detail, and offer conclusions on what to expect in the months ahead.

REGULATORY OVERVIEW

Hospitals are Required to Address the Security of Patient Data and the Possibility of Identity Misuse and Fraud

- **The Health Information Technology for Economic and Clinical Health (HITECH) Act**, which became effective February 17, 2010, sets rules for disclosure reporting, privacy monitoring, limited use of personal medical data for marketing, and patients' electronic access to their health information. The HITECH Act is enforced by the U.S Department of Human Services.



These new privacy and security requirements, which impact hospitals and their vendors, include new and strengthened enforcement provisions and penalties related to the Health Insurance Portability and Accountability Act.

- **The FACT Act Red Flags Rule**, which went into effect on January 1, 2008, with an enforcement deadline of June 1, 2010, requires that certain businesses and organizations — including hospitals, and other health care providers — are required to have formal, written policies and procedures (and training programs) in place to spot and heed the red flags that often can be the telltale signs of identity theft.



The Red Flags Rule is enforced by the Federal Trade Commission, which has extended the enforcement deadline several times to give ample opportunity for organizations to be in compliance.

- **46 States have data breach notification laws in effect** that hospitals are required to adhere to, including Massachusetts' tough new law that impacts any facility that has a breach that involves 1 or more Massachusetts residents.



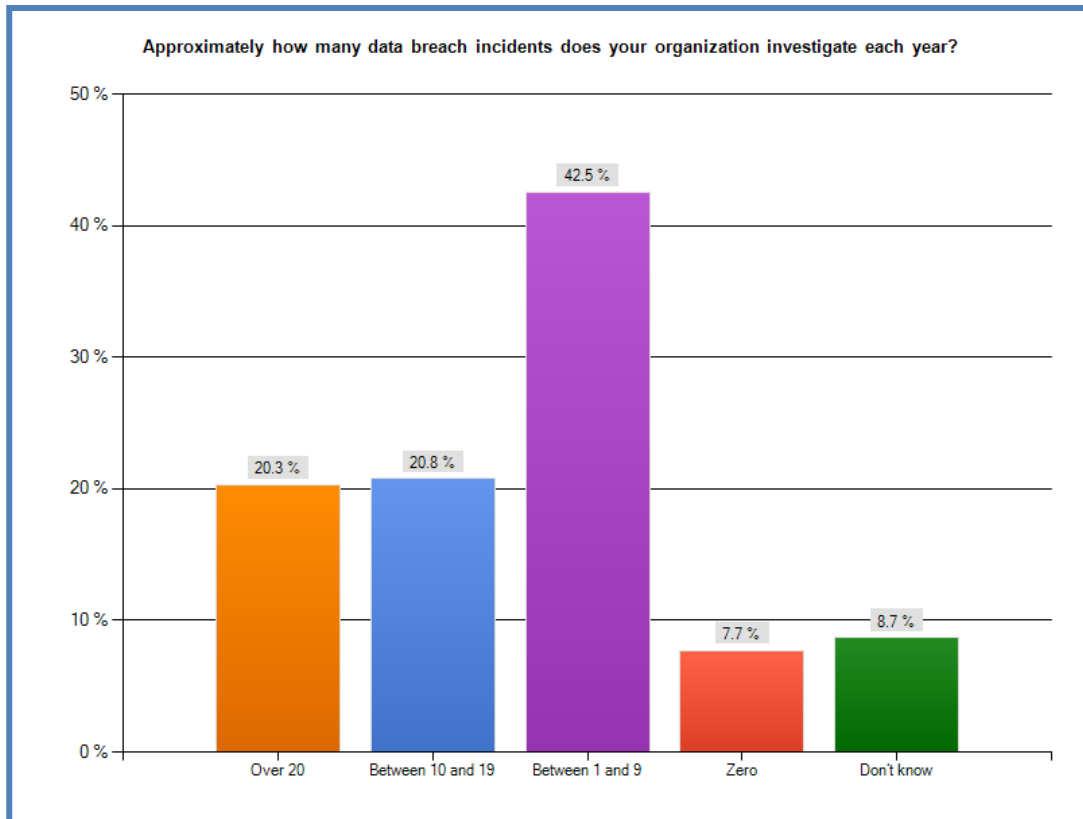
Our survey asked questions related to compliance and compliance efforts; procedures involving patient identification and the investigation of possible fraud; the frequency of data breaches; and the status of HITECH Act compliance by hospitals' vendors and business associates. You may request a copy of the survey and the results for each question by contacting Identity Force (see page 11 for contact information).

KEY SURVEY FINDINGS

New Regulations on Hospitals Are Not Curing the Pandemic of Data Breaches and Medical Identity Theft

1. Data Breaches are Rampant

- **83.6 percent** of hospitals have **data breaches** every year.
- **41.5 percent** of hospitals have **TEN OR MORE data breaches** each year.
- **20.3 percent** of hospitals have **TWENTY OR MORE breaches** annually.



Diagnosis: Data Breach Laws Are Not Working. The frequency of data breaches at hospitals far exceeds what is publicly reported. This under-reporting is likely no different than other sectors of our economy, however it raises great concern that patients’ personally identifiable information is extremely vulnerable and falls in line with other studies that reveal medical identity theft as the fastest growing form of identity fraud in the nation. *(more...)*

Last year, in our 2009 report on Red Flags Rule compliance, we found that over 63% of hospitals had at least one breach annually, and nearly 20 percent reported having 10 or more (a leap of over 120%). BOTH of those statistics have increased substantially in this year's study. This does not bode well, especially as hospitals move more heavily to the use of Electronic Health Records.

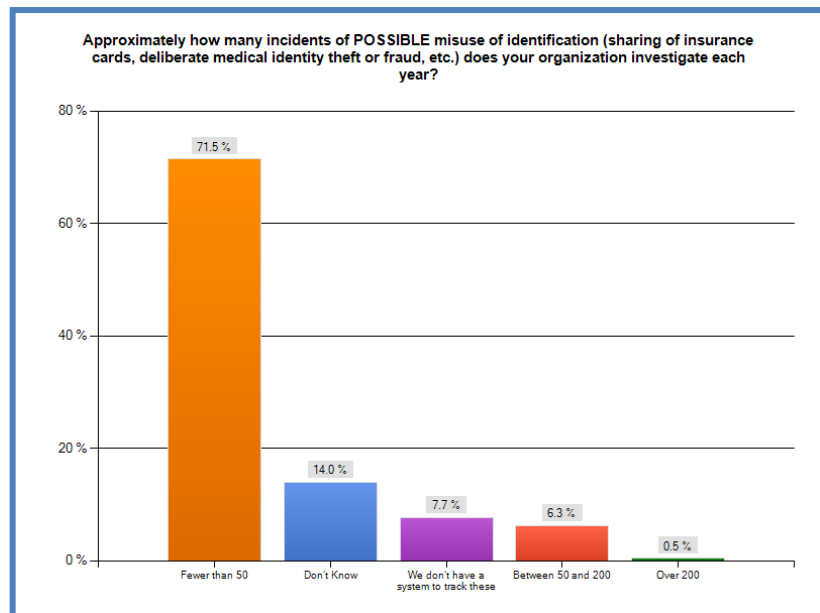
In addition to patient vulnerability, hospitals are at high risk for exposure to significant costs related to regulatory action, fines, litigation and loss of revenue.

While many compliance officers are working to ensure that organizations are prepared to comply with data breach notification requirements, that will actually not address the overriding issue of how to actually eliminate breaches.

Course of Treatment: Hospitals must expand their activities from tactical triage (“what’s the minimum we need to do right now?”) to strategic action. Successful organizations will implement organization-wide training programs designed to create a “Breach-Free Culture.” These programs usually pay for themselves by lowering risk and making breaches must less frequent. Avoiding one substantial breach, according to the statistics cited earlier from the Ponemon Institute, can save millions of dollars in costs.

2. Investigation of Possible Fraud Surprisingly Low

- 71.4 percent of hospitals on average **investigate fewer than 50 cases** of possible misuse of identity annually.
- **34.3 percent of hospitals do not keep** government-issued picture identification records on the majority of their patients
- While most organizations have an employee training program in place regarding misuse of identification (a Red Flags Rule best practice), **37.9 percent of hospitals report that they either do not have a training program, or that very few employees have been trained.**



Diagnosis: Medical identity theft is not being stopped at the hospital door. Beyond working to eliminate data breaches, the single most effective way to combat medical identity theft is for providers to diligently and universally corroborate the identity of their patients.

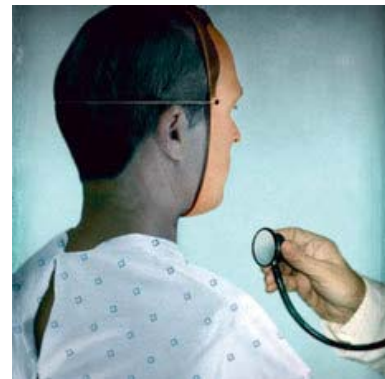
Nearly 40 percent of hospitals have not fully trained their employees regarding the misuse of identification (sharing of insurance cards, deliberate medical identity theft or fraud, etc.). That, coupled with the fact that a surprising number of hospitals do not keep records on patients' identification, sets the stage for fraud to continue unabated at many institutions.

The most interesting data retrieved through this survey on this topic, though, is that the overwhelming majority of hospitals (71.4%) investigate less than 1 possible case of identity misuse per week.

Course of Treatment: Hospitals can be more proactive when it comes to patient identification – which is at the forefront of medical identity theft. It is not necessary to wait for a patient to discover that his or her identity has been stolen, or for an insurance claim to be denied before taking straightforward action to effectively identify and track patient ID issues, and train employees.

3. Healthcare Reform Not Expected to Help

- **56.3 percent of hospitals believe that the new health care reform law will either have no change or will increase medical identity theft** at their institutions.
- Only 17 percent indicated that they thought the new law recently passed by Congress and signed by the President would reduce the number of incidents of ID misuse and medical identity theft at their institutions.



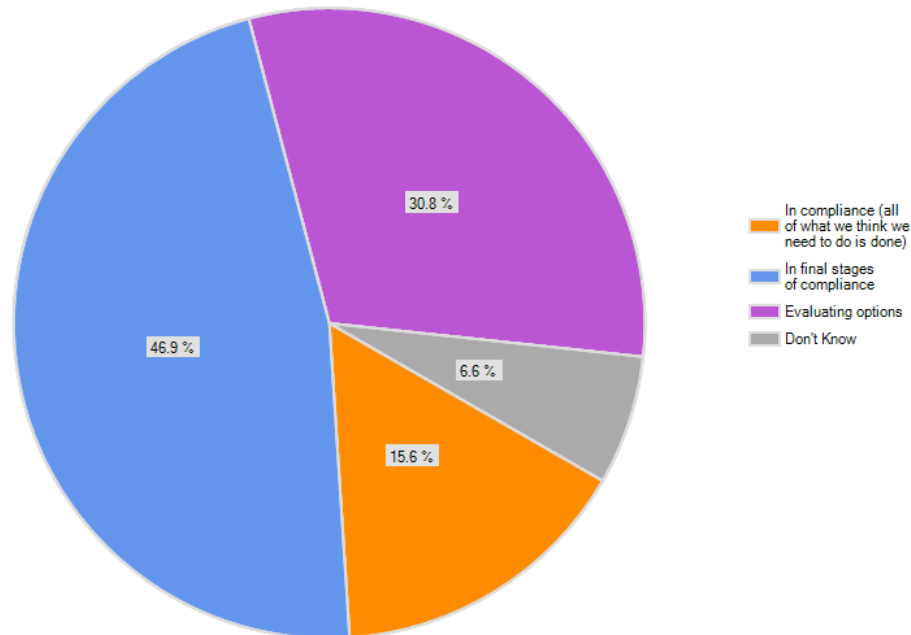
Diagnosis: Existing regulations and the new health care reform law will not solve medical identity theft. Data breaches are up, medical identity theft continues to surge, and even the most sweeping reform of the health care system we have seen in the past 40 years is not expected to come to the rescue.

Course of Treatment: Hospital executives are right to be skeptical of the new law's ability to stem identity theft and data breaches. Hospitals need to build an approach founded in industry Best Practices that brings departments together to implement solutions aimed at both prevention and compliance.

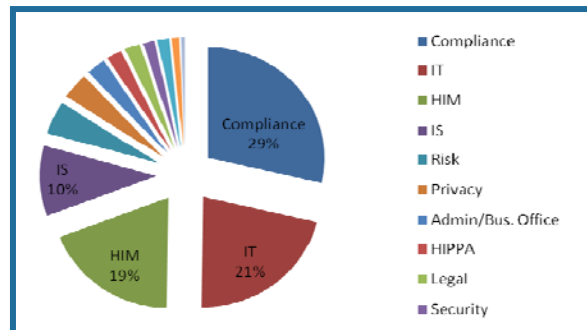
4. Timeliness of Compliance with HITECH Act is Poor

- Only 15.7 percent of hospitals feel they are in compliance with the HITECH Act, which went into effect in February 2010.
- 30.5 percent of are only at the “evaluating options” stage.
- The good news is that almost half of hospitals say they are in the final stages of compliance; however, they are nearly 2 months behind the enforcement deadline.

How far along is your hospital in the process to comply with the HITECH Act? (Compliance meaning that all the key things you believe you need to do are completed.)



- A wide variety of departments are leading or sharing the lead for HITECH Act Compliance, but the most common are Compliance (29%), IT (21%), HIM (19%) and IS (10%).
- Compliance leaders identified a wide range of activities they see as related to meeting the requirements of the HITECH Act, but by far the two most frequently listed are having “new written data breach processes and procedures” and “Amended Business Associate Agreements.”



Diagnosis: Lack of compliance is likely due to a lack of resources, and the difficulty of building homegrown solutions. The fact that so many different compliance models exist is a

reflection of a lack of knowledge of Best Practice approaches to dealing with these relatively new laws, as well as a lack of understanding on how to eliminate data breaches and thwart medical identity theft.

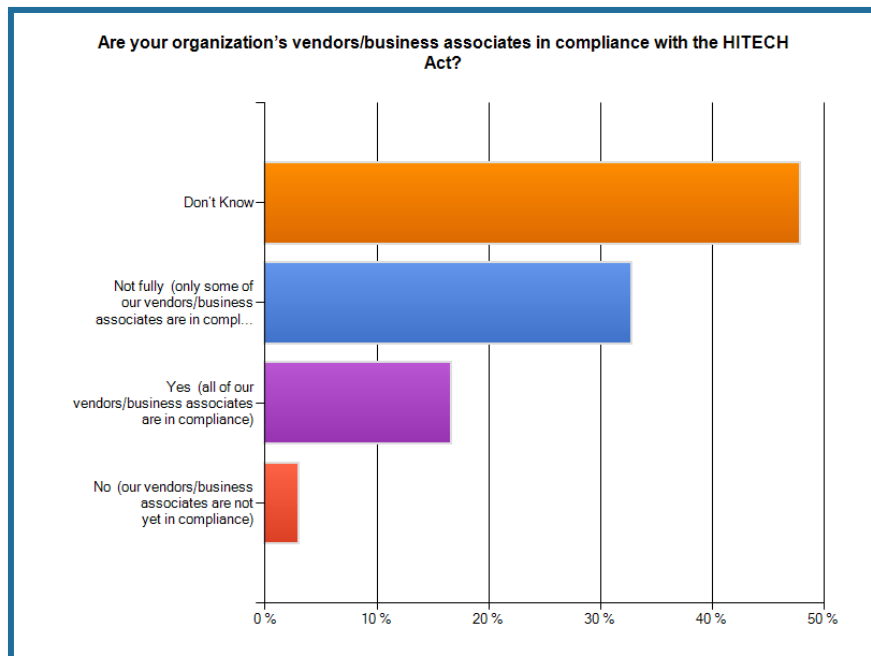
Last year's survey on compliance with the Red Flags Rule identified that on the eve of the deadline to comply (then set for May 1, 2009, but subsequently delayed until June 1 of this year) the lion's share of facilities were not able to comply. This recurring pattern of not being able to comply is troubling.

Hospitals face the dual challenges of not being versed in Best Practice solutions to identity theft-related issues, and not having the internal resources to meet compliance deadlines.

Course of Treatment: Hospitals that cannot easily add the myriad of new laws to their organization's compliance efforts should examine finding a partner to help. Sharing experiences and approaches with colleagues throughout the industry will also be helpful. Building and adhering to Best Practices should begin without delay.

5. Security of Hospital Business Associates and Vendors is Unknown

- **61.0 percent of hospitals report that they do not have a formal process to verify that vendors or business associates are in compliance with the HITECH Act.**
- **48.3 percent of hospitals do not know** if their vendors and business associates are in compliance with the HITECH Act.
- **36.0 percent report that they have business associates that are NOT in compliance with the HITECH Act** (combination of "no" and "not fully" responses).



Diagnosis: Even as hospitals slowly move towards compliance with federal and state laws, exposure to their organizations and to their patients will continue to be high. While a majority of organizations report having amended business associate agreements (BAAs), most do not have a formal process in place to verify compliance with the HITECH Act. This partial approach is definitely a red flag.

Course of Treatment: Business Associates and Vendors need to be fully trained on Best Practices and Procedures to prevent data breaches and medical identity theft. Further, hospitals should be proactive for their own protection and for their patients'.

CONCLUSION

The pandemic of data breaches and medical identity theft is getting worse in hospitals across the United States – and the new laws and regulations instituted over the past 3 years have done little, if anything, to cure the problem.

Hospitals should evaluate a variety of approaches to protect themselves and their patients, including:

- ❖ Hospitals must expand their activities and efforts to eliminate data breaches from tactical triage to strategic action, with the goal of building a Breach-free Culture.
- ❖ Hospitals need be more proactive when it comes to patient identification issues.
- ❖ Hospital executives should not rely on the new health care reform law to stem identity theft and data breaches.
- ❖ Hospitals that cannot easily add the myriad of new laws to their organization's compliance efforts should examine finding a partner to help and implement Best Practice policies and procedures.
- ❖ Business Associates and Vendors need to be fully trained on Best Practices and Procedures to prevent data breaches and medical identity theft.

About Identity Force

Identity Force is a leading provider of complete, 360° proactive identity theft protection for hospitals, individuals, businesses and government agencies. Identity Force was launched in 2005 as a response to the dramatic increase in identity theft crimes in the United States. A division of Bearak Reports, Inc. which was founded in 1992, Identity Force draws on broad, deep expertise in information verification services for its complete, proven approach to identity theft protection. For more information about Identity Force, call 1-877-IDFORCE or visit www.identityforce.com.



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

Additional Resources

Identity Force: For more information, visit Identity Force: www.identityforce.com or call us at **1-877-IDFORCE**

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: www.ftc.gov/redflagsrule

U.S. Department of Health and Human Services Web site: www.hhs.gov

Media: For more information contact Derek Beckwith (dbeckwith@identityforce.com or 508.788.9400 x 230), visit www.identityforce.com, or call 1-877-IDFORCE.

Note about this survey:

Identity Force believes this sample size identifies notable trends, and that the survey establishes a reliable overview of compliance efforts being undertaken by hospitals. Survey participants were secured through e-mail outreach by the American Hospital Association to its membership. The results may reflect the characteristics of executives who have a heightened awareness of identity theft, medical identity theft, data breaches and compliance, security, privacy and legal issues. Additionally, self-reports of compliance do not necessarily indicate true compliance (which can only be determined by an enforcement agency).