2008 HIMSS Analytics Report: Security of Patient Data

Commissioned by Kroll Fraud Solutions

April 2008

HIMSS analytics™
Innovative Research | Informed Decisions

KROLL
Fraud Solutions

INTRODUCTION

The Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II) required the Department of Health and Human Services (HHS) to establish national standards for the security of electronic healthcare information.

On February 20, 2003, the final rule adopting HIPAA standards for security was published in the Federal Register. This final rule identifies a series of security procedures to assure the confidentiality of electronic protected health information. These procedures include administrative, technical and physical measures.[1] The security rules went into effect in April 2005.

In addition to these security rules, other legislation followed. The Gramm-Leach-Bliley Act, originally passed in 1999 was amended in 2003 to provide for enhanced protection of non-public information, including healthcare information. The Sarbanes-Oxley Act of 2002 includes regulations that impact information at public hospitals[2].

Numerous states have also passed legislation that has impacted the security of personal health information. For instance, Washington State has included the following safeguards in the Revised Code of Washington (RCW), Title 70, Chapter 70.02 , Section 70.02.150. "A healthcare provider shall affect reasonable safeguards for the security of all healthcare information it maintains. Reasonable safeguards shall include affirmative action to delete outdated and incorrect facsimile transmission or other telephone transmittal numbers from computer, facsimile, or other databases. When healthcare information is transmitted electronically to a recipient who is not regularly transmitted healthcare information from the healthcare provider, the healthcare provider shall verify that the number is accurate prior to transmission". [3]

Recognizing that California regulations have inspired other states to introduce similar notification laws, the enactment of AB1298 effective January 2, 2008 may reasonably be viewed as a harbinger of changes to come across the country. AB1298 expands California's data-breach notification law to include: unencrypted medical histories, information on mental or physical conditions, medical treatments and diagnoses, unencrypted insurance policy or subscriber numbers, any applications for insurance, claims histories, and appeals. Virtually ANY loss or compromise of patient data will require patient notification.

In addition to the political and legislative context outlined above, there are a number of other issues that keep the security of patient information at the forefront for healthcare organizations. While none of these was specifically addressed in the survey, we believe that these provide additional context:

- Patient data collected and stored in hospitals and healthcare facilities is the most valuable and content-rich for fraudulent use and profitability. In addition to name, Social Security number and date of birth (the golden combination), records in these facilities also contain mailing address, insurance policy information, medical history, and, in some cases, credit card and financial

[1] Centers for Medicare & Medicaid Services (CMS); security standard overview; http://www.cms.hhs.gov/SecurityStandard/

[2] Sarbanes-Oxley, financial and accounting disclosure information; http://www.sarbanes-oxley.com/

[3] Washington State Legislature, http://apps.leg.wa.gov/RCW/default.aspx?cite=70.02.150

information to expedite billing and payment – more data in one record than those of any other source such as banks, schools or HR departments.

- Hospitals are aggregators of birth and death records which are often used for synthetic identity theft where the identity is fabricated from multiple sources. These are valuable resources for this type of crime because they are harder to detect and restore and include victims who are not likely to have any prevention measures in place – minors and the deceased – extending the life of the identity theft cycle.

- Patient data breaches are the most difficult to clean-up and cause problems beyond financial damage. Patients whose data is used for medical fraud (i.e. the perpetrators use stolen information to receive treatment), suffer from insurance eligibility/application issues as well as misdiagnosis due to data on their records that does not apply to them.

In the period from 2006-2007, over 1.5 million names were exposed during data breaches that occurred in hospitals alone.[4] This doesn't include the other categories of healthcare facilities and services such as home healthcare providers, physician offices and pharmaceutical companies who also suffered breaches of similar content-rich records.

HIMSS Analytics joined with Kroll Fraud Solutions, a leader in data security, privacy and data breach response, to examine how healthcare organizations are dealing with an environment in which the need to secure patient data is ever becoming a priority. This report summarizes our findings from a survey of senior executives from healthcare organizations across the United States. Funding and industry expertise for this research was provided by Kroll Fraud Solutions.

Contents

[4] www.attrition.org, 03/01/2008.

1. Executive Summary

The broad objective of this research was to gain a clear understanding of the status of patient data security at hospitals across the U.S. Respondents were asked to provide information on the following areas:

- Their awareness and understanding of security risks associated with patient data
- Their awareness and understanding of laws and regulations in place and compliance issues
- Patient data security practices in place and perceived effectiveness
- Resources allocated to patient data safety, and
- Costs associated with patient data breaches

Following are some of the top level findings:

- There is a lack of awareness within the healthcare industry around the frequency and seriousness of identity theft that negatively impacts efforts to contain the problem and reduce the risk. There are a number of factors contributing to this phenomenon.

  - *Regulatory Loopholes*

    There are loopholes ("reasonable efforts," "acceptable measures" and similarly vague language) in almost every law regulating patient data management, including HIPAA, the Sarbanes-Oxley Act of 2002 (SOX), and Payment Card Industry Data Security Standards (PCI DSS) that have enabled breach cases to go unreported, preventing an accurate report on frequency.

    Only 56 percent of respondents who experienced a security breach notified the patients involved, indicating that compliant organizations do not always recognize the need to report breaches or notify patients with exposed records depending on the circumstance.

  - *A Focus on Compliance Over Risk Mitigation*

    On a scale of one to seven, where seven is a high level of awareness of HIPAA, respondents had an average score of 6.53. More tellingly, nearly three-quarters of respondents (74 percent) answered this question with a rating of seven (7). HIPAA awareness is higher among respondents working for larger organizations. Among respondents working for an organization with fewer than 100 beds, the average awareness of HIPAA is 6.43; this average is 6.67 among respondents who work for an organization with 300 or more beds.

    Such high scores are not a surprise given the HIPAA audits underway and the penalties and funding at risk for facilities found non-compliant. While HIPAA requires organizations to have a risk management process in place, it does not specifically identify how organizations should implement security controls. It allows them latitude to make these determinations based on risk analysis. By and large, healthcare organizations have not been dealing with the area of accessing data with malicious intent.

- *The Snowball Effect*

  The size and scope of breach cases are difficult to accurately assess. Data forensics conducted after a breach has been detected usually reveals the scope and severity is beyond initial expectations. Upon recognizing the loss or exposure of certain data via a given leak, facilities may realize the link: a series of events that would have otherwise gone unnoticed have been identified and addressed more effectively.

  The healthcare industry is not the only one experiencing this phenomenon. Approximately 47 percent of Kroll Fraud Solutions clients have experienced subsequent breaches.

- *Focus on Inappropriate Access and Privacy vs. Fraud and Malicious Intent*

  Because of the complexity of information sharing and access at healthcare facilities, security policies must address a number of patient data abuses, including regulated access and appropriate use among approved personnel in addition to the prevention of theft. In fact, 62 percent of the respondents who indicated that they had a breach at their organization identified the source as unauthorized use of information while 32 percent identified wrongful access of paper records. There was very little mention or indication of data theft for fraudulent purposes. The data most frequently breached was patient name or high-level patient information, such as a diagnosis.

  Noticeably absent were breach sources associated with malicious intent, such as stolen laptops/computers, deliberate acts by unscrupulous employees, etc., supporting the lack of industry focus on fraudulent data breaches that masks the frequency and severity of the problem.

  Since 2000, 23 percent of all breaches[5] that required notification were caused by an employee of the breached organization. Such incidents are often more difficult to detect, which can extend the duration of the breach.

  Examples of insider breach with malicious intent in a healthcare setting include:

  - Philadelphia, PA - September 2007. A temporary clerk, employed for two years before the crimes surfaced, was convicted of stealing the identities of elderly patients and using the details for personal gain.

  - Slidell, LA - March, 2007. An emergency room clerk employed for 12 years was found sending text messages to her son when patients arrived in life-threatening condition. The text messages included the patients' names, dates of birth and Social Security numbers.

  As stated above, these types of malicious activity are noticeably absent from respondents' attribution of breach source.

[5] www.attrition.org, 03/01/2008.

    - *Lack of Awareness Around Cost and Impact*

      Only 18 percent of those respondents who experienced a fraud-related breach believed there was a negative financial impact, which is consistent with other findings that indicate while patient data security is a priority, awareness in the healthcare industry around the impact and implications of a data breach, even when one has occurred at their organization, is low. As reference, some studies place the average cost of a breach as high as $197 per record or $6.3 million per incident (Ponemon Institute's 2007 Cost of Data Breach Study), which would make a patient data breach a debilitating event for any healthcare facility regardless of size.

      Approximately one-quarter of respondents (21 percent) changed their breach response action plan as a result of a change in organizational leadership at their organization, yet, as was noted above, in the instance of a security breach only 56 percent of respondents informed the patient(s) whose data had been compromised. This points to a largely reactive orientation towards security enforcement and breach planning with a troubling tendency to deal with situations as they arise.

- The healthcare industry has to manage and maintain complex information security systems that address a hierarchy of needs surrounding successful healthcare delivery. In this environment, competing needs more directly related to patient treatment overshadow resources devoted to patient data security.

    - *The Larger the Facility, the Greater the Risk of Breach*

      According to the survey, identity theft is three times as likely to happen at a larger facility (over 100 beds) than a smaller facility (under 100 beds).

- Employee education is only one part of an effective security policy and healthcare organizations need to ensure that they are addressing their security policy with an eye on the larger picture.

    - *Employee behavior needs to be compliant with security policy*

      Dismissing an employee does not solve the problem, it only removes the offender. Organizations need to continue to be vigilant about ensuring that their security policies and procedures are enforced and that educating employees remains a top priority. Healthcare organizations also need to monitor that employee behavior is compliant with the security policies that have been put in place.

        - 62 percent of the respondents who indicated that they had a breach at their organization identified the source as unauthorized use of information while 32 percent identified wrongful access of paper records

- *Ensure that security technologies fit into clinical workflow*

  Password sharing among clinicians to facilitate more efficient care (i.e. physicians sharing passwords with nurses to enter order sets) has been a commonly cited problem. This practice opens the door for security risks.

  - 12 percent of respondents note that improper IT security practices in place at the organization, such as sharing or improper protection of system password and ID log-ins to systems that have patient data are of concern

2. Methodology

HIMSS Analytics extended invitations to participate in this telephone-based survey to senior information technology (IT) executives, Chief Security Officers and Health Information Managers. Only respondents who indicated that they were familiar with the security of patient data at their organizations were included in the final dataset. Only one respondent per organization was invited to participate in this survey. A total of 263 respondents participated in this research, which was conducted in January 2008.

3. Profile of Survey Respondents

This survey focuses on the responses of individuals who are familiar with the security of patient data at their organization. Particular attention was paid to hospital bed size, so that a cross-section of organizational sizes is reflected in this report.

Over half of the respondents who participated in this research identified their title as an IT professional. More specifically, 29 percent of respondents indicated their title as senior IT executives and another 30 percent of respondents indicated that they were an “other IT executive”. Twenty-one (21) percent of respondents indicated their title was Health Information Management (HIM) Manager and another 12 percent of individuals indicated that they were the Chief Security Officer. The remaining respondents identified their title was “other”, which includes titles such as Chief Executive Officer, Chief Financial Officer, HIPAA Security Officer or Chief Safety Officer. All respondents who participated in this research were **required** to be familiar with the security of patient data at their organization.

Over half of survey respondents (55 percent) work for organizations with fewer than 100 beds. Another 30 percent of respondents work for organizations with between 100 and 299 beds. The final 15 percent of respondents work for a hospital with 300 or more beds. The average number of beds per hospital is 167 and the median is 84 beds.

By type of organization, 46 percent of respondents indicated that they worked for a general medical/surgical facility. Another 44 percent of respondents reported that they worked at a critical access hospital. The remaining ten percent of respondents reported a primary work site that will be classified as “other” for the purposes of this report. This category includes academic medical centers, pediatric facilities and long term acute care facilities.

4. Primary Concerns with Regard to Data Security

When asked to describe their primary concerns with regard to data security at their organization, two primary themes emerged. The first was a general concern that patient data was secure. The second was a very real concern that employees represent a key factor for data breaches.

In an open-ended format, respondents were asked to identify the primary concerns they have with regard to data security at their organization. The responses to this question can be divided into two broad categories. First, respondents expressed a general level of concern about the security of patient data; simply put, **they wanted their information to remain confidential and secure**. In the respondents' own words, this concern can be summarized with the following statements "**maintaining security of protective health information in a shared database is the primary concern" or "our primary concern is to maintain complete security of our data**".

Identified nearly as often was a concern that employees could compromise the security of patient information. Simply stated, "employee awareness would be our primary concern" or "the employees are always the worry". Other respondents were somewhat more descriptive. For some, it was ensuring that employees were aware of company policy—"It is just keeping in front of the employees whether it is a breach of confidentiality. I am not concerned about the system of our security; I am just concerned that an employee understands what is a violation of our policy". Others were concerned about deliberate action that an employee might take—"Our primary concern is employees leaking out information". Several other people in this category also specifically identified password sharing as a concern. **As one respondent noted, "Our primary concern is the people who are accessing data. It is a matter of password security and log-off. We will continue to train our staff to know the policy".**

Other themes mentioned were concerns about a breach of security from an external source such as a hacker or that sharing data with outside organizations and/or third parties would compromise the data. For instance, "when we have to share information externally, our concerns are that outside sources could be giving out the information" or "the primary concerns are an inadvertent or an intentional breach from the outside". Some respondents were concerned that their organization was in compliance with regulations, such as HIPAA. As one respondent noted, "our main concern is making sure we are following HIPAA. We verify all employee training on HIPAA, and send e-mails and letters to have the employees trained every year".

Two final concerns that were raised by multiple individuals included security of data included on a mobile device, such as a laptop that was subject to loss or theft or the fact that records were still paper-based. **With regard to the mobile devices, one respondent commented, "There is an increased focus on the encryption of emails and security of laptops because of the things that happened in other corporations".** As one respondent noted "we have an old manual system and it's not very easy to do checks and balances". **Another respondent commented, "The primary concerns here are dealing with paper records leaving the hospital…"**

Only a handful of respondents reported that their organization did not have any concerns regarding the security of patient data at this time.

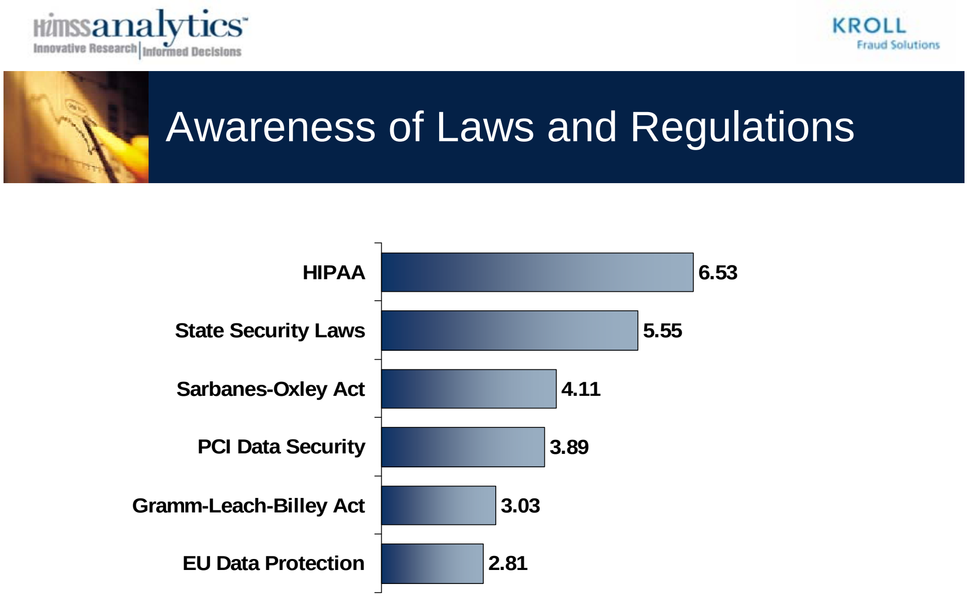
5. Compliance with Security Regulations and the Associated Risks

With regard to policies and procedures that impact the security of patient information, respondents were most likely to be familiar with the HIPAA regulations and those regulations put forward by their individual states. HIPAA requires organizations to have a risk management process in place but does not specifically identify how organizations should implement security controls, opening the door for interpretation.

Respondents were asked to identify their familiarity with several laws and requirements that impact the security of patient information. On average, respondents were most familiar with HIPAA. On a scale of one to seven, where seven is a high level of awareness, respondents had an average score of 6.53. More tellingly, nearly three-quarters of respondents (74 percent) answered this question with a rating of seven (7). HIPAA awareness is higher among respondents working for larger organizations. Among respondents working for an organization with fewer than 100 beds, the average awareness of HIPAA is 6.43; this average is 6.67 among respondents who work for an organization with 300 or more beds.

Respondents also indicated a fairly high level of awareness of the state security laws that impact their organizations—the average score of awareness was 5.55.

Familiarity is lower with other laws/requirements that regulate the security of patient data. The average score of each law/requirement included in this survey is listed below.



N= 263 Data is on a seven-point scale.

Figure One. Awareness of Laws and Regulations

Background on Sarbanes-Oxley and HIPAA

Sarbanes-Oxley and HIPAA share a common theme for storage: data must be controlled and protected.

Both focus on the following points:

- Access to local data;
- Access to backup data, and
- Ensuring that backups of critical data are maintained.

Sarbanes-Oxley Act

Sarbanes-Oxley is ultimately an act that mandates financial accountability rather than a records storage implementation guideline. It does not call for the retention of specific record types, require specific media, or specify recovery time objectives for archived records.

From a risk perspective, the issue is that companies do not know where the dividing line is between what they need to keep and what they can dispose of. This creates a data storage problem as many companies are keeping everything that may have a bearing on financial reporting, significantly increasing the risk of a breach year over year as the amount of records stored grows.

HIPAA

For HIPAA, documents relating to uses and disclosures, authorization forms, business partner contracts, notices of a healthcare facility's information practice, responses to a patient who wants to amend or correct their information, the patient's statement of disagreement, and a complaint record must be maintained for six years. (See 64 Fed. Reg. 59994). It is the amendment why hospitals and other healthcare providers maintain medical records as well as billing records on Medicare (Title XVIII), Medicaid (Title XIX), and Maternal and Child Health (Title V) for at least six years. Records must also be retained for two years after a patient's death under HIPAA. The Medicare Conditions of Participation, section 42 CFR 482.24 (b), states that all hospitals must retain medical records in their original or legally produced form for a period of five years.

It is often recommended that healthcare facilities give consideration to the statute of limitation, or time period for suing, in determining their retention policy. Many facilities will retain the medical records of minors for longer periods of time, sometimes until they are at least 21 years of age. The medical records should be retained for a patient who institutes a malpractice or wrongful suit against a facility. Generally, facilities select longer retention periods because of the concern of having the medical records available for defense purposes for litigation.

Similar to Sarbanes-Oxley, this significantly increases the risk of a breach year over year as the amount of records stored grows and complications arise around effective use, access and protection.

6. Educating Employees about Securing Patient Data

Respondents reported that their organizations take educating their employees about the importance of security patient data very seriously. The data also suggests that most of the breaches reported surround inadvertent access rather than malicious intent. Because it was not addressed in the survey, there is no way of knowing what the focus of the employee training programs is.

Respondents were asked to identify the training that they have in place to educate employees about the security of patient data. All survey respondents indicated that some level of education regarding the security of patient data is provided to employees at their organization. Additionally, only 11 percent of respondents indicated that their organization did not have a formal policy in place for educating employees. This was most likely to be the case at smaller hospitals, as 15 percent of respondents working for a hospital with fewer than 100 beds reported their organization did not have a formal policy. This can be compared to six percent of respondents working for a hospital with 100 to 299 beds and eight percent of respondents working for a hospital with 300 or more beds.

According to survey results, providing this type of training as a part of new hire training is nearly universal, as 95 percent of employees suggest that this is in place at their organization. There is little variation reported in this area by organization type or size.

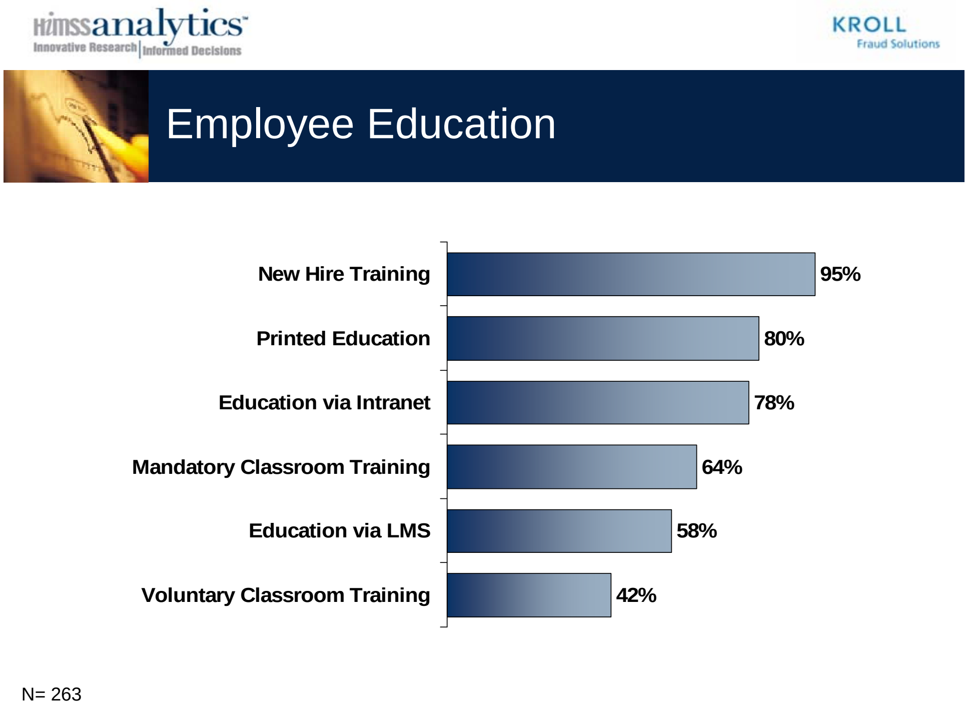


Figure Two. Employee Education

Organizations often supplement new hire training with additional training provided over the course of an employee's tenure. Two-thirds of respondents (64 percent) indicated that employees at their organization are required to participate in mandatory training classes. Nearly 90 percent of respondents that offer mandatory training indicated that this training is offered on an annual basis. Another 42 percent of respondents indicated that their organization offers voluntary classroom based training above and beyond new-hire training.

Educational materials the employees are able to review at their convenience are also widely used. Eighty percent of respondents indicated that employees at their organization are provided with print educational materials, such as brochures or pamphlets.

Another three-quarters of respondents (78 percent) indicated that their organization provides educational information to their employees on the organization's Intranet. A higher percentage of individuals working at general medical/surgical hospitals indicated that this was the case when compared to the response of those individuals working for a critical access hospital. Eighty-four (84) percent of respondents working at a general medical/surgical hospital reported that this type of content was available on their Intranet compared to 71 percent of respondents working for a critical access hospital. A higher percent of individuals working at larger organizations reported that their Intranet was used for this purpose (under 100 beds—72 percent; 100 to 299 beds—86 percent; 300 or more beds—82 percent).

Finally, 58 percent of respondents make courses regarding the security of patient data available through their organization's learning management systems (LMS). As with content provided via Intranet, a higher percent of respondents working for a general medical/surgical facility (66 percent) reported that they provide data via an LMS than do individuals that work for a critical access hospital (47 percent). Respondents working at larger hospitals were also more likely to provide educational material via an LMS. Less than half of respondents (48 percent) working for a hospital with under 100 beds reported that their organization provided education about securing patient data via an LMS, compared to 65 percent of respondents working for an organization with 100 to 299 beds and 80 percent of respondents working for an organization with 300 or more beds.

Kroll Fraud Solutions firmly believes that education alone is not enough. Learning, comprehension and actual practice must drive institutional behavior. When it comes to protecting the safety of patient data, caretakers must demonstrate the same diligence they apply to ensuring patient health. The goal of every healthcare organization should be to elevate sensitivity to patient data to this superior level -- from the most senior administrator to every doctor, nurse and staff member. Key elements to ensure increased employee understanding and compliance include: 1) sound security and privacy procedures, 2) a solid educational foundation, 3) periodic refresher training and 4) frequent reminders of the established policies and procedures.

7. Ultimate Responsibility for Patient Data Security

There is a lack of consensus in the industry around experience profiles and organizational placement of senior staff responsible for implementing hospital patient data security. While Chief Security Officers were most frequently identified at 22 percent, three additional titles were nearly equally likely to be responsible.

While nearly one quarter of respondents (22 percent) identified the Chief Security Officers as the person who is responsible for patient data security, the broader picture of responsibility for this data is spread throughout a wide variety of title types. Sixteen (16) percent of respondents indicated that the Chief Information Officer (CIO) has this responsibility and 15 percent indicated that this is the responsibility of the Chief Executive Officer (CEO). The Chief Privacy Officer holds this responsibility at 13 percent of respondents' organizations. The individuals least likely to be held accountable are the Chief Operating Officer (COO) and the General Council. Each of these titles was identified by only one percent of respondents.

Several interesting trends are shown when organizational bed size is taken into consideration. One-quarter of the respondents (26 percent) working for small organizations—under 100 beds—reported that the Chief Security Officer at their organization was ultimately responsible for patient data security. Another 20 percent of respondents working at small organizations reported that the CEO holds this responsibility. The pictures shifts somewhat at organizations with between 100 and 299 beds, where 23 percent of respondents reported that the CIO holds this responsibility and 20 percent reported that the Chief Security Officer is responsible. At larger organizations (300 beds or more), the responsibility is mixed fairly evenly across title types. Most frequently selected as holding this responsibility were CIOs (21 percent). Another 18 percent of respondents indicated that the security of patient data is the responsibility of the Chief Privacy Officer. The Chief Security Officer, CEO and Board of Directors were each selected by 15 percent of respondents.

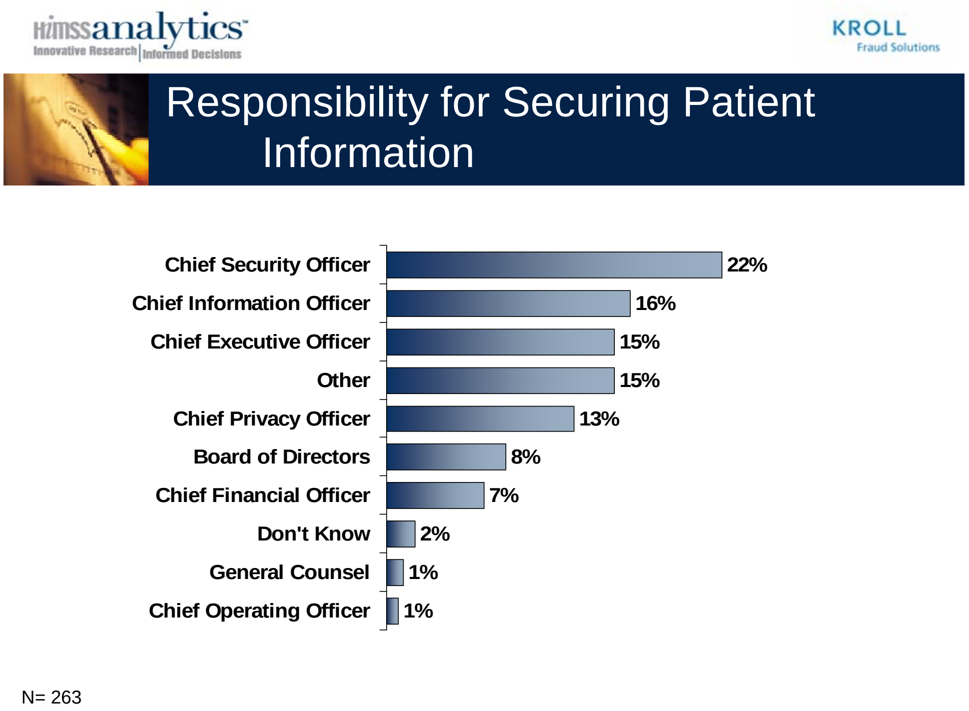
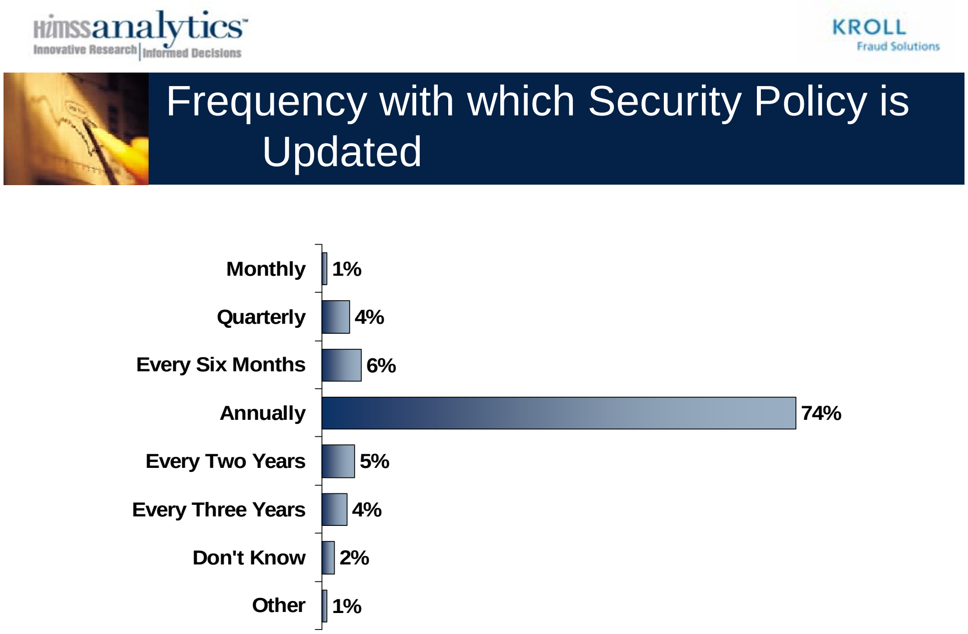


Figure Three. Responsibility for Securing Patient Information

8. Measures for Securing Patient Data

Security policies/procedures are almost universally used to help ensure that patient data is secure. Technical IT security measures (such as firewalls) and physical security measures (such as locks or badge access) are also widely used.

Respondents were asked to identify what measures were in place at their organization to secure patient data. Nearly all respondents (97 percent) indicated that their organization has implemented a security policy. In order to keep this policy relevant and current, 85 percent of respondents indicated that this policy was updated on at least an annual basis. The most frequently identified timeframe for updating this information was annually, which was identified by 74 percent of respondents.

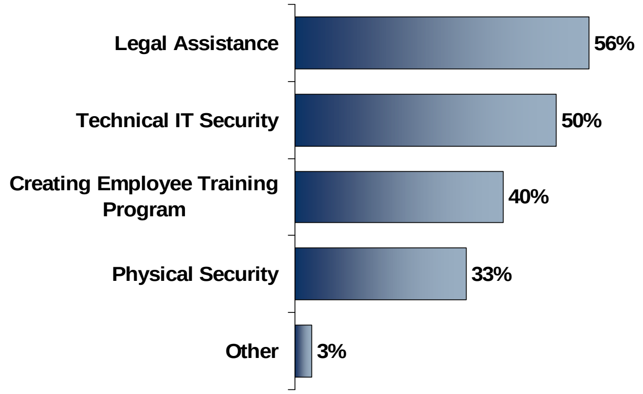


N= 256

Figure Four. Frequency with which Security Policy is Updated

Approximately 40 percent of respondents reported that they did not use an outside firm to create their organization's security policy. Among those respondents that did report using an outside firm for assistance, legal assistance was the area in which outside council was most likely sought—56 percent of respondents indicated that their organization used assistance in this area. Another half of respondents indicated that their organization used assistance with respect to how their organization's security policy impacted technical IT security. Respondents were least likely to report that they used an outside firm to create the portions of their security policy that applied to physical security measures. This response was selected by only 33 percent of respondents.

Areas in Which an Outside Firm was Used to Create Security Policy

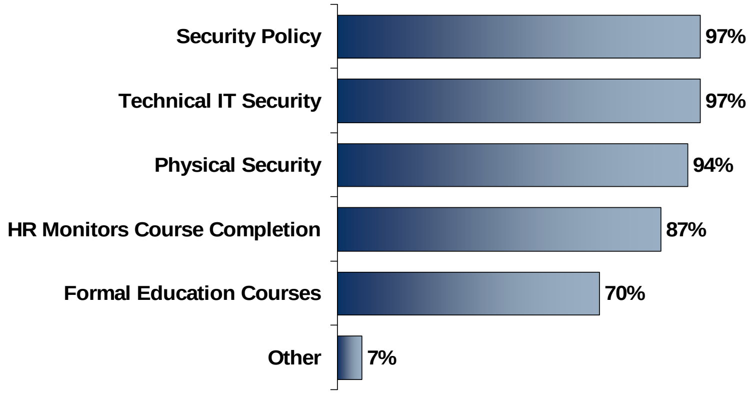


N= 158

Figure Five. Areas in Which an Outside Firm was Used to Create Security Policy

In addition to the security policy, this survey also tested for the utilization of a number of other types of means used to secure patient information. Nearly all of the respondents (97 percent) also indicated that technical IT security measures, such as firewalls, encrypted e-mails and network monitoring, were in place at their organization. Over 90 percent of respondents also indicated that physical IT security measures, such as locks, guards and badge access, were in place at their organization. By hospital type, a higher percent of respondents working at general medical/surgical hospitals (97 percent) were likely to report that physical security measures were in place, compared to critical access hospitals (90 percent).

Measures Used to Secure Patient Data



N= 263

Figure Six. Measures Used to Secure Patient Data

Monitoring the courses that employees take regarding the security of confidential patient data was less likely to be identified as a means of securing patient data. Eighty-seven percent of respondents indicated that the human resources team at their organization monitors the completion of courses on confidential patient data for hiring and continuing education tasks. Seventy (70) percent of respondents indicated that their organization offers formal education courses for employees as part of an LMS that tracks and monitors the successful completion of these courses.

9. Monitoring the Security of Patient Information

The most frequently identified security breach action plan response was to reprimand/terminate the employee responsible for the breach. In addition, breach action plans were lacking in their focus on proactive risk mitigation rather than reactive updates related to regulatory changes or organizational changes.

Respondents were asked to identify the plan of action that their organization follows in the event that data is inappropriately accessed. Most frequently cited was to reprimand the employee responsible for the inadvertent access of data, which could include termination. This option was selected by nearly half of the respondents (48 percent). Simply stated, “normally, termination is the result”. Respondents were much less likely (11 percent) to indicate that their organization provided education to employees who were responsible for a security breach. As one respondent noted, “We have a policy on that...The employees are suspended if they normally give out information for personal gain or malicious content. If they accidentally or inadvertently did it, they will be educated properly”. Or as stated by another respondent “We do conduct investigation and identifying individuals who commit such violation. So, we take appropriate measures such as counseling, putting on probation, then termination depending on the severity of the violation".

A quarter of the respondents specifically indicated that they investigated the terms of the security breach at their organization. One respondent noted "We do an investigation, and then we deal with the issue. We also do our best to fix the breach". By organization type, respondents at general medical/surgical hospitals had a higher likelihood of conducting an investigation (32 percent) that did those respondents at a critical access hospital (21 percent).

Slightly more than 20 percent of respondents indicated that their course of action was driven by corporate policy. As one respondent noted, "We follow policies and external regulations. We follow up on how we investigate, remediate and follow reporting for those instances required by the law".

In the instance of a security breach, only ten percent of respondents indicated that their organization would inform the patient(s) whose data had been compromised. In one respondent's words, "we have to notify the person whose information it is that has been accessed and then we have to discipline the person who was responsible for the event".

Respondents were also asked to identify what triggered their most recent update to their organization's action plan. Ten percent of respondents reported that their organization did not previously have an action plan and this triggered the creation of such a plan. This is particularly true among critical access hospitals—15 percent of respondents working for critical access hospitals suggested this was a reason why they established an action plan, compared to six percent of respondents working for general medical/surgical hospitals.

Respondents were much more likely (70 percent) to suggest that revising their action plan is part of a regular process at their organization. Another third of respondents (30 percent) indicated that the most recent update to their action plan was done in response to changes in external policies and/or regulations.

Approximately one-quarter of respondents (21 percent) changed their action plan as a result in a change in organizational leadership at their organization. A higher percent of respondents working for a small organization (under 100 beds) reported that their organization changed their action plan as a result of a change in organizational leadership. Twenty-six (26) percent of respondents working at a small hospital identified this as a reason for changing their action plan, compared to 15 percent of respondents working for a hospital with 100 to 299 beds and 13 percent of respondents working for a hospital with 300 or more beds. Similarly, a higher percent of respondents working for a critical access hospital (28 percent) reported that a change in organizational leadership triggered a response in their action plan. This was the case among only 15 percent of respondents working for a general medical/surgical hospital.

Action plan changes were least likely to be triggered by a security breach. Only ten percent of respondents indicated that they made a change in their action plan as a result of a security breach at another organization, while eight percent indicated that they made a change in their action plan as a result of a security breach at their own organization. Larger organizations were more likely to indicate that a security breach at their own organization would result in a change to their action plan. Eighteen (18) percent of respondents who work for an organization with 300 or more beds reported that this was a trigger for revising their action plan, in comparison to six percent of respondents working smaller hospitals (under 100 beds).

The responses suggest a largely reactive orientation to security and breach response planning and a troubling tendency to deal with situations as they arise rather than proactive and ongoing review and revision to security and breach response plans based on constantly changing environments.

10. Biggest Risk to Patient Data

Consistent with the focus on employee training and dismissal as effective prevention tactics, respondents were most likely to identify that they are concerned about inadvertent access of patient information by employees.

Noticeably absent were concerns around breach sources associated with malicious intent, such as stolen laptops, stolen computers, deliberate acts by unscrupulous employees, cyber attacks through the Internet, etc., supporting the lack of industry focus on fraudulent data breaches.

Respondents were asked to identify the most common item that will put data at risk at their organization. By and large, they are concerned about inadvertent access to data by employees. Half of respondents indicated a response that on some level dealt with employee access to patient information. More specifically, 19 percent of respondents indicated that a lack of attention by staff to the organization's security policy was an issue. Another 12 percent of respondents indicated that their primary concern was a lack of effective employee education relative to data security and the potential liability that causes to the organization. Four percent were most likely to attribute risk to patient data to the sheer volume of contract/temporary employees that had access to organizational systems and/or networks. In addition, 16 percent of respondents who answered this question "other" reported a response that could be directly attributed to employee behavior. A sample of the responses given in this category include "employee error", "employees have access to patient data", "nosy employees", "uneducated employees".

The other area that was most likely to be identified was improper IT security practices in place at organization, such as sharing or improper protection of system password and ID log-ins to systems that have patient data. This area was identified by 12 percent of respondents. Also identified as the most common items that can put patient data at risk are:

- Lack of required IT security solutions—one percent;
- Lack of security policy—zero percent;
- Paper-based charts are not secure—ten percent;
- Information is available on a portable device—four percent;
- Sharing information with an external organization—eight percent;
- Making information accessible via the Internet—two percent;
- Other—11 percent.

Items included in the "other" category included natural disasters, carelessness, complacency and fraud.

11. Security Breach

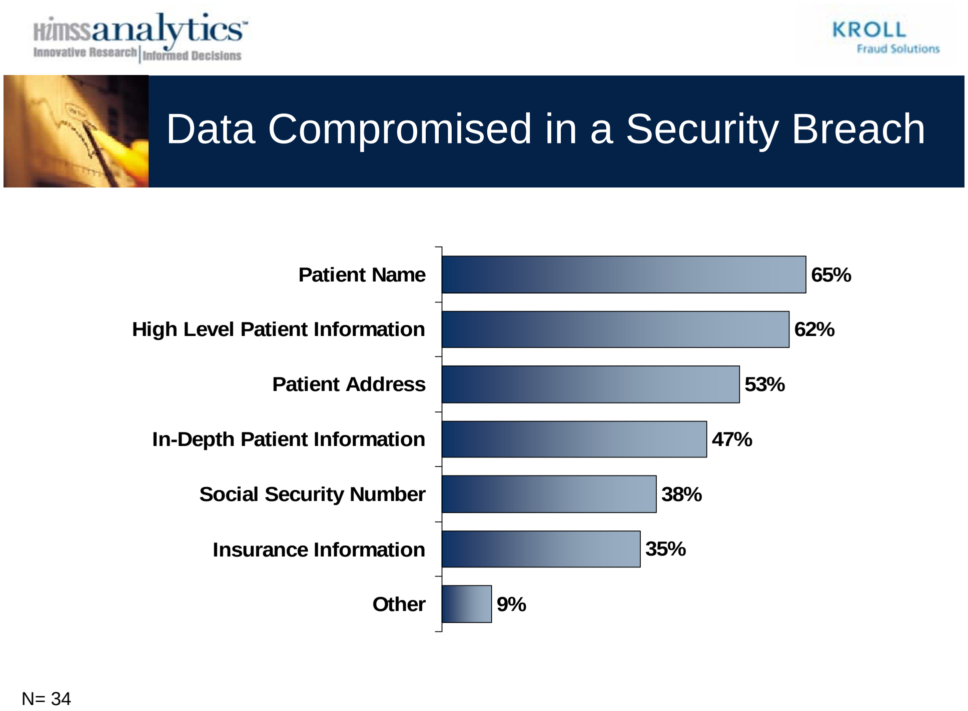
Thirteen percent of respondents reported that their organization has had a security breach in the past 12 months. Most frequently compromised were patient name and high level patient information, such as a diagnosis. Most respondents felt that their organization was prepared to deal with a security breach and very few have sought out assistance from an external organization.

Consistent with other responses in the study, there is a focus on breaches in the "inappropriate access" category rather than breaches with malicious intent and for fraudulent purposes, demonstrated by employees as perpetrators, the type of information accessed and the responses that took place.

Even within organizations where breaches took place, respondents did not focus on changing their security policies, but instead focused on proactively monitoring compliance with those policies. A small percentage believed that there was any financial damage associated with breaches that took place.

Approximately 13 percent of respondents reported that their organization has had a breach of security in the past 12 months. Among those respondents that reported a security breach at their organization over 40 percent worked for a hospital with fewer than 100 beds. However, a higher proportion of larger hospitals reported a security breach. More specifically, only 10 percent of the respondents working at a small hospital reported a breach of security. This can be compared to 28 percent of the hospitals with 300 or more beds. There was no correlation by type of hospital.

Respondents were asked to identify the type of data that was compromised in a security breach. Nearly two-thirds of respondents (65 percent) indicated that the patient's name was compromised in the security breach at their organization. This was closely followed by high-level patient information, such as a diagnosis, which was reported to be compromised in 62 percent of the security breaches in this sample. Approximately half of respondents (53 percent) indicated that a patient's mailing address was compromised. Nearly half (47 percent) also reported that in-depth patient information, such as clinical notes, was compromised. None of the respondents indicated that credit card information was compromised in a security breach.



Data Compromised in a Security Breach

N= 34

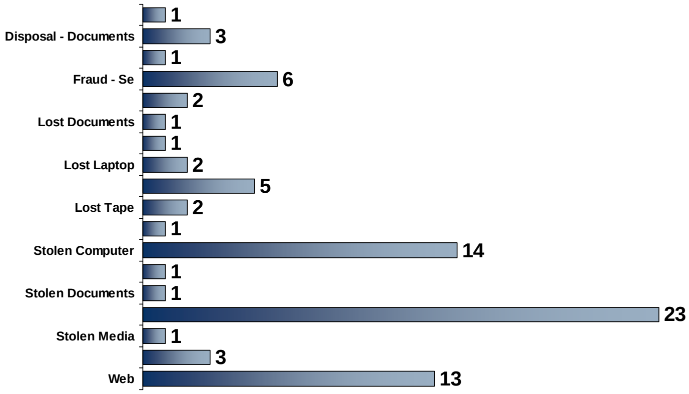
Figure Seven. Data Comprised in a Security Breach.

With respect to the manner in which the breach took place, respondents were most likely (62 percent) to identify that the breach stemmed from the unauthorized use of information by an employee. This was most closely followed by wrongful access of paper-based patient information, which was identified by 32 percent of respondents. Respondents were much less likely to report that patient data at their organization was maliciously compromised through a breach of network by an outsider; only one respondent indicated that this was how patient data at their organization was compromised.

The information generated from the question—"who was the perpetrator of the security breach"—validates the information identified above. Over 80 percent of respondents indicated that the breach was a result of the action taken by an individual employed by the organization at the time of the security breach. This outpaces by nearly ten times any other reason that a security breach has taken place. More specifically, nine percent of respondents indicated that the breach was the result of actions taken by an individual performing outsourced services at the time of the breach. The same percent of respondents indicated that the breach was the result of action taken by an individual not associated with their organization. However, no respondent indicated that the breach was an act of retaliation by a former employee.

For comparison, the following chart represents the types of breach by source that took place at healthcare organizations from 2006 to 2007.

Source of Data Breach



Source: www.attrition.org

Figure Eight. Source of Data Breach[6].

When asked to rate their level of "preparedness" with security breach, respondents reported an average level of preparedness of 5.88, on a one to seven scale—where one is not at all prepared and seven is extremely prepared. In fact, over one-third of respondents (38 percent) indicated rated their readiness as a seven. Only six percent of respondents indicated that their readiness at the time of the security breach at their organization was a one or two.

One-third of respondents (35 percent) indicated that no changes were made to their organizations' security practices as a result of the security breach that took place at their organization. The most frequent response to a security breach was the provision of additional education; this option was selected by 38 percent of respondents. Nearly as many respondents (32 percent) indicated that the security breach at their organization resulted in changes to the organization's security policies. Respondents were least likely to indicate that they increased funding for remediation or purchased additional security tools. Each of these items was selected by nine percent of respondents.

In organizations in which patient data is inadvertently accessed, there are often consequences. Respondents were asked to identify the perceived impact that the security breach had at their organization. Most frequently selected was patient satisfaction, which was identified by 41 percent of respondents. Eighteen (18) percent of respondents indicated that their institution experienced a financial impact, such as additional costs associated with credit monitoring. Six percent of respondents noted that their organization had experienced bad press as a result of the security breach. The same percent of respondents indicated that the security breach did not have an impact on their organization.

[6] www.attrition.org, 03/01/2008.

Despite the repercussions identified above, only one respondent indicated that a lawsuit had been filed by a patient(s) that had been the victim of a security breach. None of the respondents indicated that their organization experienced reduced donations as a result of a security breach.

Slightly more than one-third of respondents (38 percent) indicated that their organization did not offer remediation services available to the patients impacted by the security breach. The remediation most likely made to patients was notification, identified by 56 percent of respondents. Twelve percent of respondents indicated that their organization offered credit monitoring to patients. Only one respondent each indicated that non-credit monitoring services and identity restoration were offered by their organizations.

Three-quarters of respondents indicated that their organization did not use an external firm to manage the impact of the security breach. Among the organizations that did use an external firm to manage the impact of the security breach, there was no leading type of services that was used. Each of the items identified in this survey (notification, data forensics/investigation, litigation, remediation and communications) were each used by only two to three respondents.

12. Use of Outside Firm to Mitigate Fallout from Future Security Breaches

Respondents have considered using outside consultants in the eventuality that patient data at their organization is compromised. The area in which outside assistance is most likely to be sought would be in the area of litigation.

Among those respondents that reported a security breach, use of an outside consultant to mitigate the breach was less than widespread. However, respondents were likely to predict that they may use assistance from an outside firm in the future. Only 11 percent of respondents indicated that they did not anticipate using an outside firm in the case of a future security breach.

The area in which respondents were most likely to report a future need for assistance was in the area of litigation; this was identified by 65 percent of respondents. Half of respondents also indicated that they would consider using an outside firm for data forensics/investigation. Respondents were least likely to identify notification as the area for which they would consider using an outside firm; this option was selected by 24 percent of respondents.

13. Conclusion

There is a combination of factors in the healthcare industry that raises serious concerns about the frequency and severity of patient data breaches and supports the need to modify both regulatory and operational environments to more aggressively address the situation.

- When conducting a risk analysis and putting a plan into place, organizations need to be aware of the full range of areas where security breaches can take place, from inadvertent access by employees to malicious intent.

- There is an over-reliance on employee education and disciplinary action as effective prevention and response techniques that do not address the incidence of malicious intent that is responsible for the industry's largest and most damaging breaches.
- Evidence suggests that the actual number of security breaches that take place in the industry is actually higher than reported in this research. The size and scope of breach cases are difficult to accurately assess. Data forensics conducted after a breach has been detected usually reveals the scope and severity is beyond initial expectations. This prevents accurate measurement of breach incidence.

Progress towards better security and safer patient data environments will start with a paradigm shift in the approach to patient data security, treating it as an ongoing operational and behavioral change that guards against both malicious theft of patient data records for fraudulent purposes as well as inappropriate access during treatment.

14. Survey Sponsors

About HIMSS Analytics

A Trusted, Experienced Resource for Healthcare Provider Organizations

HIMSS Analytics supports improved decision-making for healthcare delivery organizations, as well as healthcare IT companies, state governments, financial companies, pharmaceutical companies and consulting firms, by delivering high quality data and analytical expertise. The company collects and analyzes healthcare data related to IT processes and environments, products, IT department composition and costs, IT department management metrics, healthcare trends and purchasing related decisions. It is a wholly-owned not-for-profit subsidiary of the Healthcare Information and Management Systems Society (HIMSS).

About Kroll Fraud Solutions

Kroll, the world's leading risk consulting company, provides a broad range of investigative, intelligence, financial, security and technology services to help clients reduce risks, solve problems and capitalize on opportunities. Kroll Inc. is a wholly-owned subsidiary of Marsh & McLennan Companies, Inc. (NYSE: MMC), the global professional services firm. Kroll began providing identity theft solutions in 1999 and created its Fraud Solutions practice in 2002 in response to increasing requests from clients for counsel and services associated with the loss of sensitive personal information, and related identity protection and restoration issues facing organizations and individuals.

Since then, Kroll's Fraud Solutions clients have included Fortune 500 companies, non-profit organizations, and government entities dealing with healthcare, financial services, insurance, consumer service, and any activity involving the collection and use of personal information. Kroll's Fraud Solutions team presently serves over 10,000 businesses and millions of individual consumers. For more information, visit: www.krollfraudsolutions.com.

15. How to Cite This Study

Individuals are encouraged to cite this report and any accompanying graphics in printed matter, publications, or any other medium, as long as the information is attributed to the 2008 HIMSS Analytics Report: Security of Patient Data commissioned by Kroll Fraud Solutions.

16. For more information, contact:

HIMSS Analytics

Joyce Lofstrom
Sr. Manager, Corporate Communications
312-915-9237
jlofstrom@himss.org

Kroll Fraud Solutions

Susan Moerschel
Manager of Public Relations
615-320-9800 x964
smoerschel@kroll.com