2010 HIMSS Analytics Report: Security of Patient Data

Commissioned by Kroll Fraud Solutions

April 2010

HIMSS analytics™
Innovative Research | Informed Decisions

KROLL
Fraud Solutions

INTRODUCTION

The following study is based on the results of a bi-annual survey of healthcare provider facilities in the U.S. regarding patient data safety. The survey was commissioned by Kroll Fraud Solutions, a leader in healthcare data security that has helped some of the largest healthcare providers in the country respond to data security breaches, in partnership with HIMSS Analytics, the leading organization representing health information management systems and services.

The purpose of conducting follow-up research to the 2008 study is two-fold: 1) set benchmarks to effectively monitor the changing state of patient data security in U.S. healthcare facilities so that problems can be identified and corrected; and 2) track trends in the industry and its environment (regulatory, operational) that are helping or, in some cases, preventing more effective patient data security and management measures from taking root.

The healthcare provider industry continues to be a data breach risk as well as a primary target for data fraud and identity theft for a number of reasons:

- Both Personal Identifying Information (PII) and Protected Health Information (PHI) are collected and stored in hospitals and healthcare facilities. This patient data is the most valuable and content-rich for fraudulent use and profitability, with more data in one record than those of any other source such as banks, schools or human resources (HR) departments, often including name, date of birth, Social Security number, insurance policy information and, in some cases, credit card information.

- 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.

- The healthcare provider infrastructure is built for fast, reactive patient care and supports environments that are hyperactive. PHI is stored, accessed and used by multiple personnel in a variety of settings making it extremely difficult to create systems that provide for data security in all situations over an extended period of time.

- The patient data environment is in transition, with regulatory and healthcare reform legislation calling for widespread digitization and exchange of information (PHI and personally identifiable information or PII – not necessarily health-related, but sufficient for identity theft) within a networked environment where healthcare provider facilities are working with an ever-increasing pool of third parties, including Health Information Exchanges (HIEs), business associates, vendors, payors, etc. Even the best-planned migration scenarios create security gaps that represent opportunity for incidents such as breach and fraud. Based on the scope and complexity of the coming changes in the way patient data is accessed and shared, it is almost certain the industry will see an increase in breaches of PHI and PII, raising the importance of effective, security controls, monitoring, and response planning.

Since January 2008, over 110 healthcare organizations have reported the loss of sensitive PHI and/or PII affecting over 5,306,000 individuals.[1] Over 40 percent of these reported data loss incidents were caused by theft (stolen laptops, computers, or media/tapes). Another 27 percent were the result of loss or negligence by staff or third parties. Malicious insiders caused 20 percent, nine percent were caused by system hacks, web exposure, virus attacks with the remaining two percent "unknown."

Because of the increased frequency and extended harm that results from patient data breaches, studies such as the 2010 HIMSS Analytics Report: Security of Patient Data, commissioned by Kroll are valuable tools to help monitor the situation and offer third-party insight and expertise into the effect of regulatory changes and the effectiveness of the resulting compliance efforts taking place as well as the evolving state of patient data security and best practice protection methods.

Contents

[1] www.datalossdb.org, accessed 3/05/2010

1. Executive Summary

Patient Data Security in the U.S.: 2008 vs. 2010

Much has changed in the last two years with regard to the laws and regulations that govern institutions handling patient data, and the methods in place to keep that information secure and properly managed. When the 2008 HIMSS Analytics Report, Security of Patient Data, commissioned by Kroll Fraud Solutions was conducted, the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II) was the primary statute that dominated the healthcare landscape, specifying privacy and security regulations that must be met by Covered Entities with the goal of assuring the confidentiality of protected health information[2].

As the 2008 study revealed, the healthcare provider industry's focus on medical *privacy* resulting from HIPAA created a form of tunnel vision – while privacy and compliance were very much a concern, the 2008 study found, there was a disturbing lack of awareness around patient identity theft for fraudulent purposes which resulted in a lack of attention paid to security practices that would help prevent such crimes, leaving gaps in hospital security policies that put patient data at risk. In short, the 2008 study showed that PHI privacy sometimes stole focus from protection against PHI theft.

Two years later**,** the regulatory landscape has changed significantly, with the addition of the Red Flags Rule and HITECH[3], which are meant to close loopholes which exist in the vague language found in almost every previous law regulating patient data management. A lack of definition around what constitutes a data breach and a lack of reporting requirements, combined with ambiguous data security requirement terms such as "reasonable efforts," and "acceptable measures" have not provided an environment that was conducive to reporting breaches. This prevents an accurate reporting of frequency.

The development of both state and federal breach notification laws and the advent of HITECH means that covered entities will generally be required to report to patients any security breach that exposes their PHI to unauthorized persons. Furthermore, notification must be made no later than 60 days after "discovery" of the breach, or whenever the breach is known by either a third party vendor or the covered organization itself. Finally, it is also required that these breaches be reported to HHS and made public when the breach affects more than 500 individuals.

This creates an entirely new reality for healthcare facilities, which are now under much more strict government regulation than in 2008. The positive impact of these changes is that there is **a growing level of awareness around the state of patient data security** in the U.S. healthcare industry related to the increased regulation and the policies put in place to comply with those rules. There is cause for concern, however, as our new study shows that the security practices in place continue to **overemphasize "checklist" mentality for compliance without implementing more**

---

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

[3] "The Health Information Technology for Economic and Clinical Health Act (HITECH) is new federal privacy and security mandates regarding patient information, including mandatory notification of individuals whose information is breached, that was included in the Health Information Technology for Economic and Clinical Health Act (HITECH) as part of the American Recovery and Reinvestment Act of 2009 (ARRA), signed into law by President Obama February 17, 2009. A major change is that the new legislation generally requires covered entities and business associates to disclose to their patients any breach involving a patient's protected health information (PHI)."

comprehensive and sustainable changes needed for meaningful improvements in the day-to-day handling of patient PHI and PII.

Following are some of the top level findings from the 2010 study:

- Increased activity around security practices adopted to achieve compliance with new laws and regulations related to patient data security has not changed the fact that data in the industry continues to be at risk and may be targeted by individuals for fraudulent gain. Healthcare organizations are actively taking steps to ensure that patient data is secure. However, hospitals appear to be focusing on how to handle a breach after it has taken place, rather than focusing on risk assessments.

  Our survey indicates that the number of healthcare facilities that reported a breach that requires notification increased six percent this year, from 13 percent in 2008 to 19 percent in 2010. Among those respondents who reported a breach, nearly three-quarters reported their organization had one (43 percent) or two (28 percent) breaches in the past 12 months. Another 15 percent reported 10 or more breaches during this time. The remaining 15 percent had three to nine breaches during this time. This echoes the phenomenon described in the 2008 HIMSS Analytics Report; Security of Patient Data, commissioned by Kroll Fraud Solutions, where having identified an initial data breach, healthcare organizations experience the "snowball effect", as subsequent events that would have otherwise gone unnoticed are recognized and addressed more effectively.

  Similar to the study in 2008, malicious intent is still "less likely" to be the cause of most breaches that occurred. Nearly two-thirds of respondents (66 percent) in the 2010 study indicated that the source of the breach was unauthorized access to information by an individual employed by the organization at the time of the breach. This was most closely followed by the wrongful access of paper-based patient information (32 percent). Respondents were much less likely to report that patient data at their organization was maliciously compromised in other ways. Eleven percent of respondents noted that data was compromised when a laptop, handheld device or computer hard drive was lost or stolen.

  Organizations also widely use tools to monitor the flow of patient information. For instance, 98 percent have a policy in place to report a breach of patient information and 87 percent reported that they have a policy in place that requires monitoring of patient information access and sharing. Analysis of audit logs to identify inappropriate access to data is also widely used. Active steps to change security tools and resources, while widely used, are used less frequently than policies. For instance, in the past six months, most respondents reported making changes to security-related items at their organization, from technical IT security measures to physical security measures to updating policies, procedures and enhancing their hiring practices. However, the most frequently identified step, revising technical IT security measures, was identified by three-quarters of respondents.

  Despite the increase in the number of breach incidents reported, and the more stringent data security controls and the notification standards mandated by HITECH, **most healthcare facilities continue to believe that if they are more prepared, then they are more secure**. Only two percent of respondents indicated that their readiness at the time of the security breach at their organization

was a one or two (on a scale of 1-7 with 1 being "not at all prepared" and seven being "extremely prepared"). On the whole, individuals responding to this survey were slightly more likely to report they were more prepared than two years ago, giving themselves a 6.06 on a scale of 1-7, compared to 5.88 in 2008.

- There continues to **be a lack of awareness of the extremely high costs associated with a healthcare breach.** This is surprising, given the fact that breaches in the healthcare industry ultimately come at a higher overall price than the cost realized in the financial and retail sectors. Full enforcement of HITECH – including sanctions – which took effect Feb. 22, 2010, will make the costs associated with a breach even more burdensome[4].

  When asked to identify the perceived impact that the security breach had at their organization, 38 percent of respondents selected patient satisfaction as the primary impact, (down from 41 percent in 2008). Just 15 percent were concerned about a financial impact of a breach, down from 18 percent in 2008.

- While there is expanding awareness around the importance of data security, it continues to be an issue addressed through cyber security in siloed departments (IT, Security Policy), adhoc training, or policy approval events. **Awareness has yet to translate into organization-wide responsibility that is addressed through a holistic solution that covers all data (cyber and offline) across the entire organization's continuum of care (including third party vendors).**

  Security and monitoring of electronic data was well-represented in survey responses with 87 percent reporting that "they have a specific policy in place to monitor electronic patient health information access and sharing" and 86 percent noting that "regular audits are conducted of systems that generate, collect and transmit patient information."

  Organizations are also taking an active role in managing their security environment. In the past six months, respondents reported making changes to a wide variety of security-related items at their organization. For instance, nearly three-quarters of respondents noted that they had made changes in their technical IT security measures. A similar percent noted that changes were made in the area of physical security measures.

  As with the 2008 data, a wide range of individuals were identified to be responsible for patient data security. In the 2010 data, only one-third of respondents reported that the individual who is responsible for patient data security is a Chief Security Officer, Chief Privacy Officer or Chief Compliance Officer. The remaining respondents reported that they responsibility fell to an individual with a title such as Chief Information Officer or HIM Director.

[4] Section 13410(d) of the HITECH Act established a tiered ranges of increasing minimum penalty amounts. Penalties can range from $100 to $1.5 million and will apply even if a person did not know (and by exercising reasonable due diligence would not have known).

Where policies and security practices fell short, however, was in **the lack of auditing third party security systems/methods where patient information is shared with other external organizations**. Only 60 percent of respondents noted that they required their third party vendors to provide proof of employee training and half indicated that they required their third party vendors to provide proof of employee background checks.

- When reviewing differences in the survey responses by hospital type – general medical/surgical, academic medical center, and critical access – **critical access facilities lagged behind the others in terms of electronic patient health information security policy implementation and ongoing review/auditing**.

  All respondents working for an academic medical center reported that they have a specific policy in place to monitor electronic patient health information access and sharing; 95 percent of respondents in general medical/surgical hospitals also have this type of policy in place. This type of policy is used much less frequently in critical access hospitals – only 74 percent of respondents reported such a policy was in place.

  With regard to IT tools, all respondents working for an academic medical center have IT applications with audit functions, compared to 89 percent of respondents at critical access hospitals. A similar trend exists with the use of IT audit logs that are created and analyzed for inappropriate access to patient data. Ninety percent of respondents from academic and general medical/surgical hospitals report that this is the case, compared to 72 percent of respondents working at critical access hospitals.

  This trend also exists for physical security measures, such as locks, guards or badge access tools. All respondents working at academic medical centers report these are in place, compared to 88 percent of respondents working for a critical access hospital.

  Given the increased attention on the roles and responsibilities of third-parties in patient data security, the trend regarding due diligence related to vendor hiring practices is of particular concern. Where 80 percent of academic medical centers report that they require proof of a vendor's employee training, only 48 percent of critical access hospital respondents report such due diligence.

  The final trend that exists by hospital type is where regular audits are conducted for processes where patient information is shared with external organizations. This practice is widespread among academic medical centers (90 percent) and general medical/surgical hospitals (80 percent), but much less frequently used by respondents working for critical access hospitals (61 percent).

2. Methodology

HIMSS Analytics extended invitations to participate in this telephone-based survey to a variety of individuals within healthcare organizations that have experience with their organization's privacy and security environment. Respondents included senior information technology (IT) executives, Chief Security Officers and Health Information Management (HIM) Directors/Managers, Compliance Officers and Privacy Officers. Only one respondent per organization was invited to participate in this survey. A total of 250 respondents participated in this research, which was conducted in December 2009. Funding and industry expertise for this research was provided by Kroll Fraud Solutions.

3. Profile of Survey Respondents

All respondents who participated in this research were required to be 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.

Approximately half of the respondents who participated in this research identified their title as an HIM Director or Manager (45 percent). Another quarter reported their title to be an IT executive. A similar percent reported their title to be either Compliance Officer or Privacy Officer. Another four percent of respondents hold the title of Chief Security Officer. The remaining four percent of respondents hold "other" titles, including Risk Manager, Chief Executive Officer, HIPAA Director and Quality Manager. All respondents who participated in this research were **required** to be familiar with the security of patient data at their organization.

Half of survey respondents work for hospitals with fewer than 100 beds. Another 37 percent of respondents work for organizations with between 100 and 299 beds. The final 13 percent of respondents work for a hospital with 300 or more beds. The average number of beds per hospital is 185 and the median is 99 beds. For this report, we will classify all hospitals with fewer than 100 beds as "small", those with 100 to 299 beds as "medium" and those with 300 or more beds as "large".

The survey data will also be examined by type of hospital. Slightly more than half of respondents (56 percent) reported that they work for a general medical/surgical hospital, with another third working for a critical access hospital. Four percent work for an academic medical center. The remaining seven percent of respondents work for a hospital classified as "other", which includes pediatric or other specialty hospital.

4. Managing Data Flow

In general, respondents reported a highly coordinated approach to managing patient information. In addition, all use at least one method to monitor the flow of patient information.

Healthcare organizations manage multiple types of patient data, including clinical, financial and demographic information. On a scale of one to seven, where one is no coordination and seven is a high level of coordination, respondents reported an average score of 5.98, suggesting that healthcare organizations take a highly coordinated

approach for managing patient data to ensure a secure environment. In fact, 71 percent of respondents gave this item a score of six or seven on the seven-point scale.

More specifically, all organizations reported that they have at least one method in place for monitoring patient information flow. Nearly all respondents (98 percent) reported that their organization has a process in place for reporting breaches in patient information (see Figure One). Approximately 87 percent reported that "they have a specific policy in place to monitor electronic patient health information access and sharing" and 86 percent noted that "regular audits are conducted of systems that generate, collect and transmit patient information".

Least frequently selected was "conducting regular audits for processes where patient information is shared with other external organizations, entities or agencies" (74 percent)

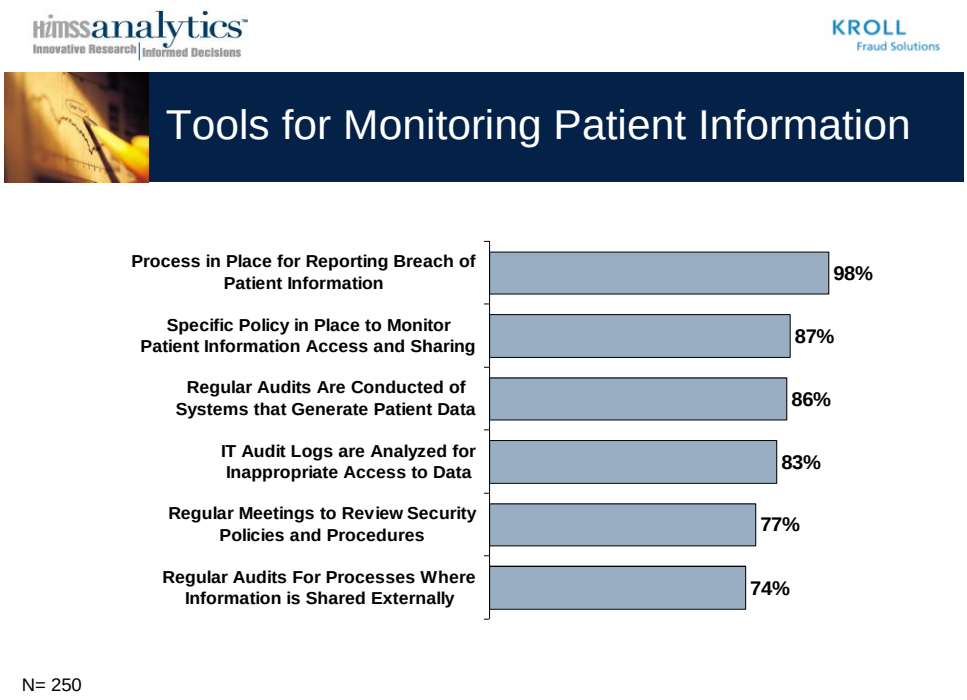

Figure One. Tools for Monitoring Patient Information

There are some differences in the responses to this question when bed size or type of organization are taken into consideration. All respondents working for an academic medical center reported that they have a specific policy in place to monitor electronic patient health information access and sharing; 95 percent of respondents in medical/surgical hospitals also have this type of policy in place. This type of policy is used much less frequently in critical access hospitals – only 74 percent of respondents reported such a policy was in place.

A similar trend exists with the use of IT audit logs that are created and analyzed for inappropriate access to patient data. Ninety percent of respondents from academic and general medical/surgical hospitals report that this is the case, compared to 72 percent of respondents working at critical access hospitals.

The final trend that exists by hospital type is where regular audits are conducted for processes where patient information is shared with external organizations. This practice is widespread among academic medical centers (90 percent) and general medical/surgical hospitals (80 percent), but much less frequently used by respondents working for critical access hospitals (61 percent).

By hospital bed size, respondents working for large hospitals (100 percent) were more likely to report that they have a specific policy in place for monitoring electronic patient health information access and sharing than were those working for small hospitals (77 percent). This is also true for instances where IT audit logs are created and analyzed for inappropriate access to patient data. Nearly all respondents at large hospitals (94 percent) reported this type of tool was in place, compared to three-quarters of respondents at small hospitals.

A similar trend exists for situations in which regular audits are conducted for processes where patient information is shared with external organizations. Respondents working for medium size hospitals (84 percent) and large hospitals (78 percent) were more likely to report these types of audits were conducted than were respondents who worked for small hospitals (66 percent).

5. Compliance with Security Regulations and the Associated Risks

Respondents report a high level of compliance with the security regulations that govern personal health information. There is no dominant factor that respondents overwhelmingly believe puts patient data at risk – no item was selected by more than one-third of respondents.

Respondents were asked to identify whether or not their organization was compliant with several industry regulations that govern personal health information. Each of these regulations was tested using a one to seven scale, where one is "not at all compliant" and seven is "compliant with all applicable standards". As Figure Two suggests, respondents were most likely to indicate that they were compliant with HIPAA (average score of 6.60). This figure also suggests that respondents believe they are compliant with all of the rules tested, with the lowest average score being received for HITECH/ARRA, with an average score of 5.75.

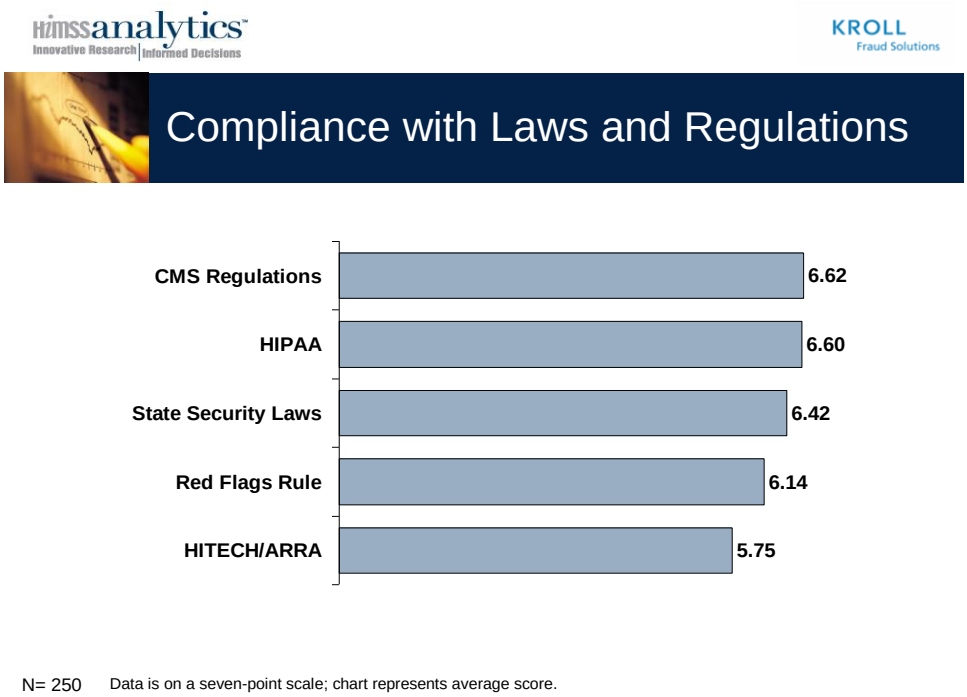

Figure Two. Compliance with Laws and Regulations

There are also some differences in compliance by bed size and type of organization. In general, respondents working at larger hospitals have a greater level of awareness than do those working at smaller organizations.

- Hospitals with under 100 beds – 6.52
- Hospitals with 100 to 299 beds – 6.73
- Hospitals with 300 beds or more – 6.75

By organization type, those working for academic centers reported higher levels of compliance with both state security laws and Centers for Medicare & Medicaid Services (CMS) regulations. See below for detail.

State Security Laws

- Academic Medical Centers – 6.90
- Other Hospitals – 6.71
- General Medical/Surgical Hospitals – 6.65
- Critical Access Hospitals – 6.20

CMS Regulations

- Academic Medical Centers – .6.80
- Other Hospitals – 6.71
- General Medical/Surgical Hospitals – 6.74
- Critical Access Hospitals – 6.39

Respondents were also asked to identify the items that were most likely to put patient information at risk at their organization. This data suggests that there is no single overwhelming item that is perceived to put data at risk (see Figure Three). Most frequently selected was lack of attention to the organizational security policy by staff; this was selected by 31 percent of respondents; this was also the top item of concern in the 2008 research[5]. Also of concern was the fact that organizations have improper IT security practices in place (26 percent). Respondents were least likely to suggest that information was at risk due to the lack of a security policy (eight percent) or because electronic information is unsecured (six percent).

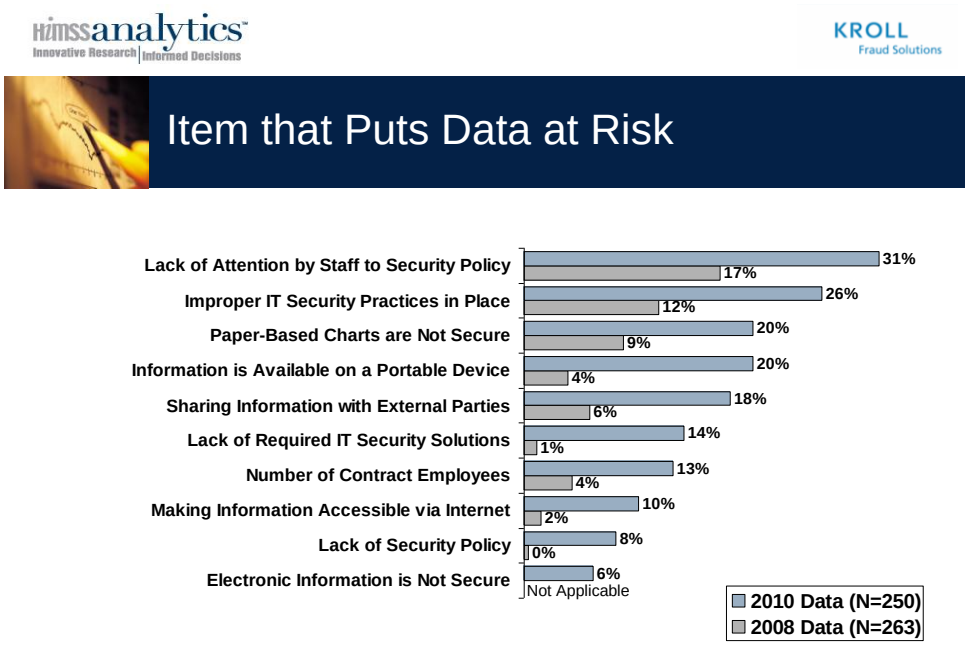

Figure Three. Item that Puts Data at Risk

By bed size, respondents working for small hospitals were more likely (17 percent) to indicate that the number of contact/temporary employees who can access information is a common problem that puts patient information at risk, compared to three percent of respondents who work for large hospitals. There are also differences with regard to the security of paper-based charges. The percent of respondents identifying this as an issue is shown below.

- Under 100 beds – 25 percent;
- 100 to 299 beds – 13 percent;
- 300 or more beds – 22 percent.

[5] In the 2008 data, respondents could select only one response. In the 2010 data, respondents could select all that apply.

6. Changes in Data Security Tools and Resources

Ensuring that data is protected is a dynamic process. In the past six months, respondents reported making changes to a wide variety of security-related items at their organization, from technical IT security measures to physical security measures to updating policies, procedures and enhancing their hiring practices.

Respondents were given a broad list of items and asked which for which items a change, enhancement or addition had been made in the past six months. Three-quarters of respondents noted that their technical IT security measures (such as firewalls or use of encrypted e-mails) had been changed in the past six months (see Figure Four). Also selected by at least 70 percent of respondents were changes in physical security measures such as locks or badge access (72 percent) and updating their HIM security policies/procedures.

Two-thirds of respondents (65 percent) noted that they had made a change in their organizations' active monitoring of information technology (IT) application audit reports. The same percent noted that they had made change in ensuring that the patient is who they say they are by initiating an ID check at the time service is initiated.

The item for which respondents were least likely to report a change, enhancement or addition in the past six months was in the area of changing hiring practices such as conducting background checks. However, even this area was identified by 49 percent of respondents.

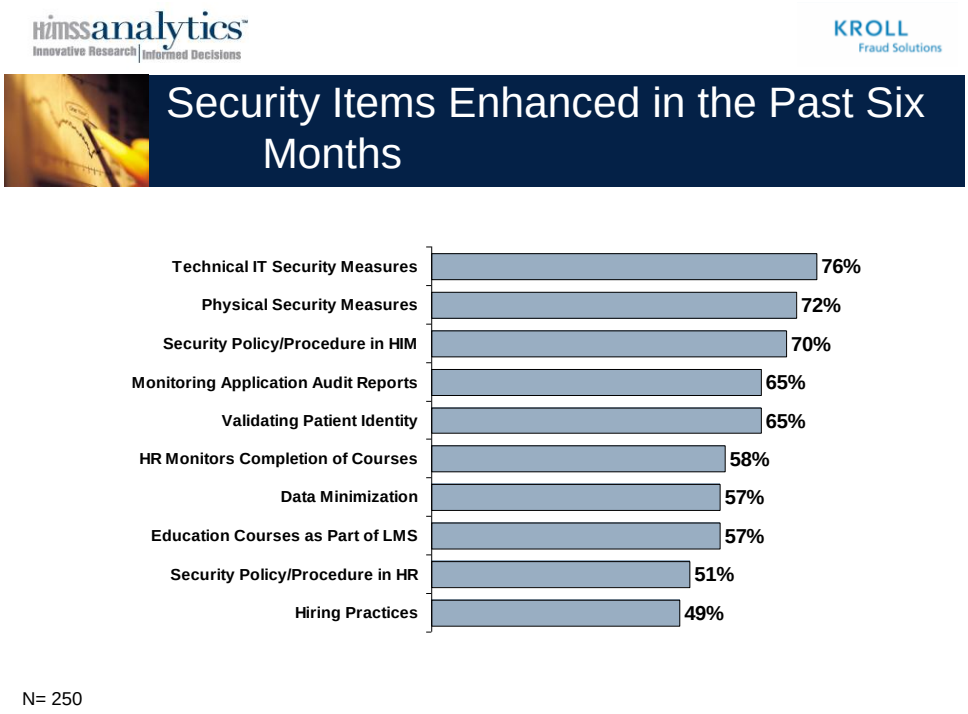

Figure Four. Security Items Enhanced in Past Six Months

By organization type, all respondents working for an academic medical center noted that their organization had changed their policies/procedures in the HIM department in the past six months, compared to 76 percent of those working for a critical access hospital and 67 percent of those working for a general medical/surgical facility. A similar trend emerges when the data for making a change to HR policies/procedures is examined. Eighty (80) percent of respondents working for an academic medical center reported a change in the past six months, compared to 55 percent of respondents at a critical access hospital and 51 percent of respondents at general medical/surgical facilities.

In addition, respondents were asked to identify what due diligence they performed to ensure that third party vendors are compliant with organizational policies and procedures to keep patient information private and secure. Nearly all respondents (97 percent) reported that they require their third party vendors to sign a business associate agreement for accessing patient identifiable information for HIPAA compliance. Also widely used are practices pertaining to the utilization of tools to secure patient information (81 percent), ensuring that the third party had a plan in place to notify covered entities of a breach (79 percent) and ensuring that the third party has a plan in place to identify potential breaches (74 percent).

The utilization of tools to secure patient information is most likely to be seen in general medical/surgical hospitals, where 87 percent of respondents reported this to be the case. This can be compared to 80 percent of respondents working for academic medical centers and 71 percent of those working for a critical access hospital.

Respondents were less likely to perform due diligence in areas of employment practices. Only 60 percent of respondents noted that they required their third party vendors to provide proof of employee training and half indicated that they required their third party vendors to provide proof of employee background checks. This trend is clarified slightly when organization type is taken into consideration. Nearly all respondents working for an academic medical center (80 percent) reported that they require proof of employee training, compared to 64 percent of respondents working for a general medical/surgical facility and 48 percent of respondents working for a critical access hospital.

7. Ultimate Responsibility for Patient Data Security

There continues to be a lack of consensus in the industry with regard to who should be the individual responsible for data security. While one-quarter of respondents indicated this position as HIMS Director, Chief Information Officers, Chief Security Officers and Chief Privacy Officers were also identified by 15 to 18 percent of respondents. Regardless of who is responsible for data security, respondents were overwhelmingly likely to report that this individual has support from the top management team.

The 2008 study suggested that the responsibility for patient data security is spread throughout a wide variety of title types. This trend continues in the 2010 data. One-quarter of respondents indicated that the HIM Director has primary responsibility for the security of patient information. Another 17 percent of respondents note that the Chief Information Officer has this responsibility. Identified by 14 percent each were the Chief Security Officer and Chief Privacy Officer. Also identified by at least 10 percent of the respondents were the organizations Chief Executive Officer (12 percent) and Chief Compliance Officer (10 percent). Fewer respondents indicated that the Chief Financial

Officer (five percent) and General Counsel (two percent). None of the respondents reported that the Chief Operating Officer had responsibility. A comparison of this year's results to the previous results can be seen in Figure Five.

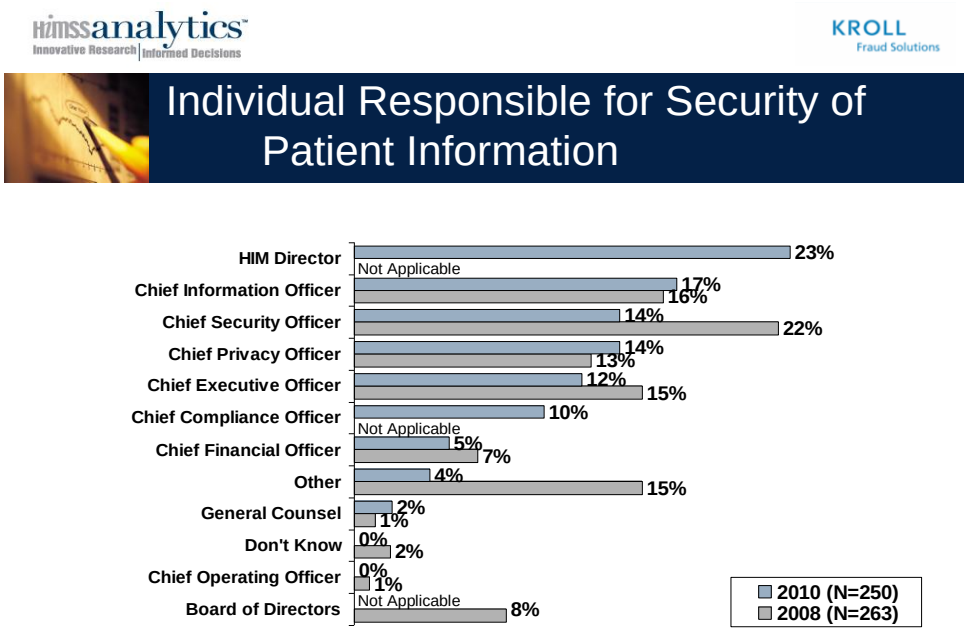

Figure Five. Individual Responsible for Security of Patient Information

There are also differences in who has ultimate responsibility by type of organization – half of the respondents working for an organization classified as an academic medical center suggested that a Chief Security Officer has ultimate responsibility for the security of patient information. In comparison, one-quarter (27 percent) of respondents working for a critical access hospital report that the HIM Director holds this responsibility. And, while one-quarter (22 percent) of respondents at general medical/surgical hospitals indicated that the security of patient information is the responsibility of the HIM Director, a similar percent noted that this responsibility is held by the Chief Information Officer.

In addition, respondents were asked to what extent the person who is ultimately responsible for the security of patient data had top level support. On a one to seven scale, where one is no support and seven is highly supported by top management, respondents provided an average score of 6.47. Indeed, nearly two-thirds of respondents selected a score of seven on this scale.

8. Measures for Securing Patient Information

Security policies/procedures continue to be used almost universally to help ensure that patient data is secure. Technical IT security measures (such as firewalls) and hiring practices that include background checks are also widely used.

As with the 2008 data, respondents reported using a wide variety of tools to secure patient information. Nearly all respondents noted that they have formal security policies/procedures (99 percent). Also used universally are hiring practices that include background checks (97 percent) and technical IT security measures such as firewalls and encrypted e-mails). A full list of all measures for which this research tested, as well as a comparison to 2008 results is included in Figure Six.

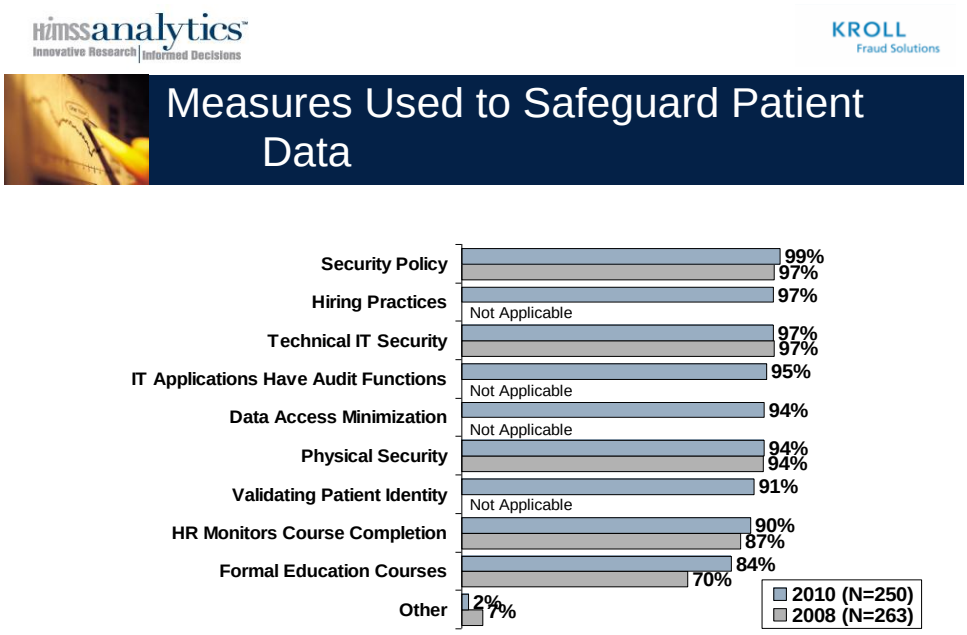

Figure Six. Measures Used to Safeguard Patient Data

There were some reported differences in the tools that were in place by the number of licensed beds in an organization. In general, a higher percent of respondents working for larger hospitals (300 or more beds) had the following tools, when compared to their counterparts at smaller organizations.

- IT Applications have Audit Functions
- Technical IT Security Measures

In comparison, hiring practices (including background checks) were more likely to be reported by respondents working for small hospitals (98 percent) and large hospitals (100 percent) than at mid-size hospitals (92 percent). Physical security measures, such as locks, guards or badge access tools were most likely to be identified by respondents at mid-size hospitals (99 percent) than at small hospitals (91 percent) or large hospitals (94 percent).

By hospital type, all respondents working for academic medical centers reported that their organization has IT applications with audit functions; this technology is also in use at 98 percent of general medical/surgical hospitals. In comparison, 89 percent of respondents at critical access hospitals reported that IT applications with audit functions were in use. A similar analysis can be made for physical security measures – all respondents working for an academic medical center have these in place, as do 98 percent of respondents working for a general medical/surgical hospital. This percent drops to 88 percent among respondents working for a critical access hospital.

9. Action Plan for Securing Patient Information

Healthcare organizations regularly monitor their action plans to ensure that the action plan is effective and appropriate. Nearly 40 percent of respondents reported making changes as a result of a security breach at their organization or at another organization.

Respondents were asked to identify what triggered their most recent update to their organizations' action plan. Approximately 12 percent of respondents reported that a key trigger was that they did not have an action plan in place previously.

Most respondents, however, reported that updating their organizations' action plan was routinely reviewed to ensure that the action plan was effective and appropriate (89 percent). Three quarters of respondents also reported that they changed their action plan in response to changes in external policies, such as ARRA/HITECH (77 percent).

A number of respondents reported that their organization reviewed its action plan due to either another security breach at their organization (24 percent) or hearing about inadvertent access to data at another healthcare organization (29 percent).

Least likely to be identified as a trigger was a change in organizational leadership, identified by about one-quarter of respondents.

10. Security Breach

Nineteen percent of respondents reported that their organization has had a security breach in the past 12 months, up from the reported 13 percent in the 2008 research. Most frequently compromised were patient name and high level patient information, such as a diagnosis.

Approximately 19 percent of respondents reported that their organization had experienced at least one breach that required notification in the past 12 months. This can be compared to the 13 percent of respondents reported this to be the case in the 2008 research. Among those respondents who reported a breach, nearly three-quarters reported their organization had one (43 percent) or two (28 percent) breaches in the past 12 months. Another 15 percent reported 10 or more breaches during this time. The remaining 15 percent had three to nine breaches during this time.

By organization type, respondents working for academic medical centers were most likely to report a security breach (30 percent). In comparison, 22 percent of respondents

working for a general medical/surgical facility reported a breach and 12 percent of respondents working for a critical access hospital reported a breach.

Among those respondents that reported a security breach at their organization, approximately one-third of the breaches took place in organizations that have fewer than 100 beds. However, a higher proportion of larger hospitals reported a security breach. Approximately 14 percent of respondents working for hospitals with fewer than 100 beds reported a breach, compared to 26 percent of respondents working for hospitals with 100 to 299 beds and 19 percent of respondents working for hospitals with 300 or more beds. Although the gap is closing, the fact that larger hospitals were more likely to report a breach than smaller hospitals is consistent with the 2008 research, when only 10 percent of the respondents working at a small hospital reported a breach of security, compared to 28 percent of the hospitals with 300 or more beds.

Respondents were asked to identify the type of data that was compromised in a security breach. Almost 90 percent of respondents noted that a patient's name was compromised in the security breach(es) at their organization. Another two-thirds (66 percent) reported that high level patient information, such as diagnosis was breached. These were also the items that were most frequently identified as being compromised in the 2008 research.

Nearly half (47 percent) reported that a patient's date of birth was compromised and 45 percent reported that other patient demographic information, such as gender or employer was compromised. The 2008 survey did not test for either of these items. A full list of items that were compromised in a data breach is listed in Figure Seven below.

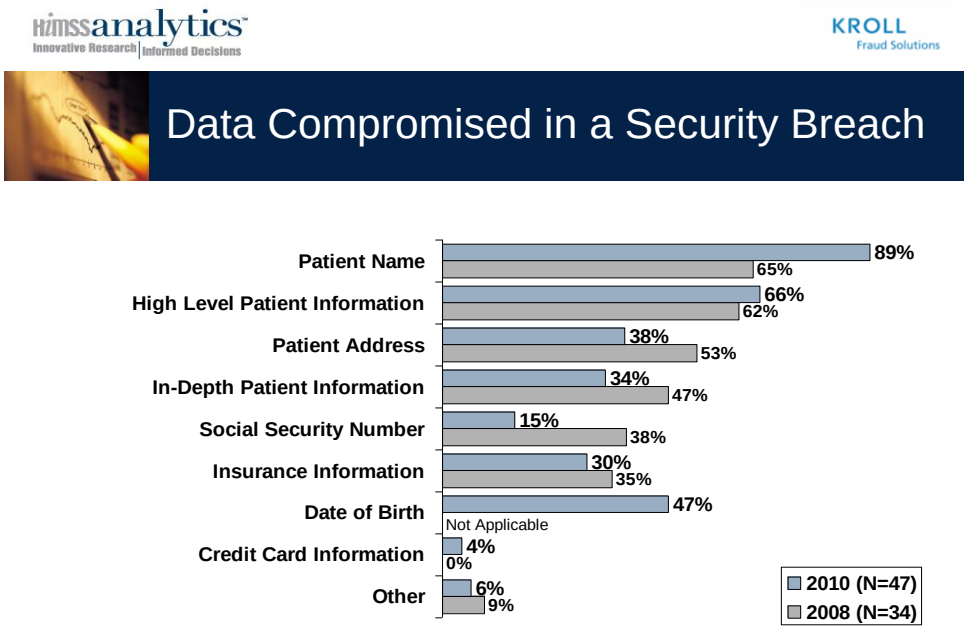

Figure Seven. Data Comprised in a Security Breach.

As in the 2008 research, respondents were asked to identify what was the source of the breach. Nearly two-thirds of respondents (66 percent) in the 2010 study indicated that

the source of the breach was unauthorized access to information by an individual employed by the organization at the time of the breach. This was most closely followed by the wrongful access of paper-based patient information (32 percent). These respondents were nearly identical to those reported in 2008, when 62 percent of respondents identified that the breach stemmed from the unauthorized use of information by an employee and 32 percent of respondents indicated the breach was the result of wrongful access of paper-based information.

Respondents were much less likely to report that patient data at their organization was maliciously compromised in other ways. Eleven percent of respondents noted that data was compromised when a laptop, handheld device or computer hard drive was lost or stolen. Other sources of breach included data housed by third-party vendor was breached (six percent), data was breached due to improper destruction of paper-based records (four percent), data was accessed on a second hand computer from which data wasn't removed (two percent) and data was accessed when the organizational network was breached by an individual outside the organization (two percent).

Nearly all respondents (94 percent) 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. Thirteen (13) percent of respondents noted that breach was the result of an individual who was employed by the organization at the time of the breach and 11 percent noted that the breach was perpetrated by a former employee. Only four percent of respondents noted that the breach was the result of an individual working at a third party organization such as an insurance company. The information generated from the question—"who was the perpetrator of the security breach"—validates the information identified above and is very similar to the data provided in 2008.

A full list is included in Figure Eight.

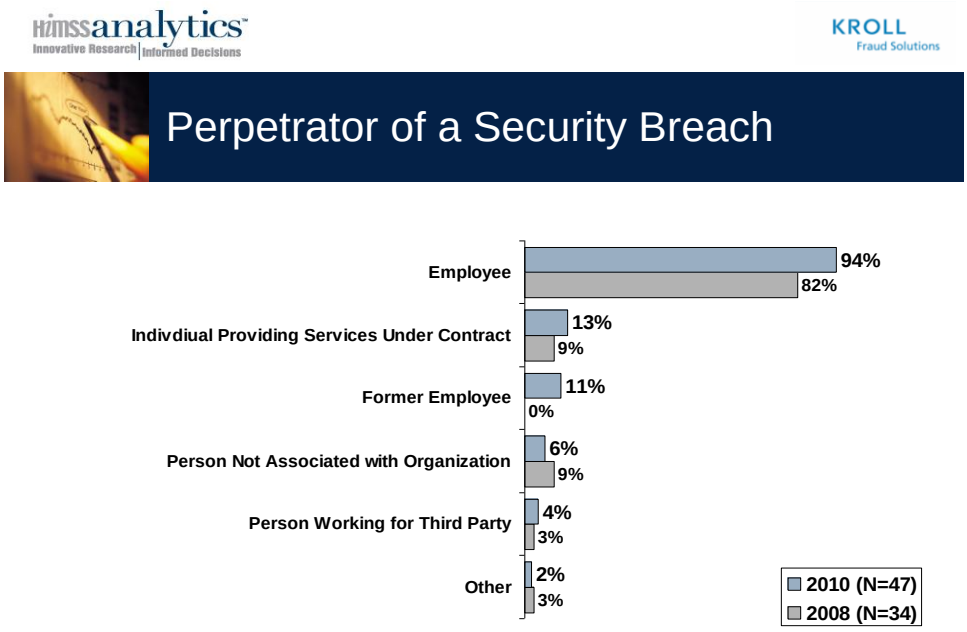

Figure Eight. Perpetrator of a Security Breach

When asked to rate their level of "preparedness" with security breach, respondents who work for organizations at which a breach was reported in this study reported an average level of preparedness of 6.06, on a one to seven scale—where one is not at all prepared and seven is extremely prepared. In fact, 43 percent of respondents indicated rated their readiness as a seven. Only two percent of respondents indicated that their readiness at the time of the security breach at their organization was a one or two. On the whole, individuals responding to this survey were slightly more likely to report they were prepared compared to those in the 2008 study (5.88).

Compared to respondents in the 2008 study, this year's respondents were more likely to make a change to their organizations' security practices as a result of a breach. In 2008, 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; this percent declined to 17 percent in 2010.

The most frequent response to a security breach was the provision of increased training for employees; this option was selected by 79 percent of respondents. This is twice the number of respondents that identified that their organization made changes to the security policies and procedures at their organization (34 percent). These were also the top responses to the 2008 survey, selected by 38 and 34 percent respectively.

Also selected by at least 10 percent of respondents were the following:

- Purchase of Additional Security Tools – 19 percent;
- Increased Funding to Pay for Remediation/Other Costs – 17 percent;
- Revising Contracts with Third Parties – 11 percent.

Respondents were least likely to identify that their organization terminated contracts with their third parties (four percent).

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 38 percent of respondents. Another 15 percent were concerned about a financial impact, such as additional costs associated with credit monitoring. This is nearly identical to the 2008 data, when 41 percent and 18 percent of respondents selected these items respectively.

Bad press related to the breach and impact to business continuity (being able to run business as usual) were each identified by 13 percent of respondents. Only two respondents noted that their organization had been faced with a lawsuit as a result of the security breach. None of the respondents indicated that they needed to switch third party vendors as a result of a security breach.

In 2008, 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; in the 2010 research, only 26 percent of respondents reported this to be the case. In both studies, notifying the patient of the breach was the most frequently selected type of remediation offered to patients (66 percent in 2010 compared to 56 percent in 2008). One-quarter of respondents also noted that they offered customer

service lines for patients whose data had been breached. This item was not tested for in the 2008 research. Credit monitoring was offered by 15 percent of respondents and identity theft consultation/restoration services were offered by 13 percent of respondents.

11. Preparation for Future Security Breaches

Most respondents are open to the idea of using an outside service provider in the event of a future data breach, particularly to get legal advice or conduct data forensics/investigation.

All respondents were asked to identify the areas in which they would consider using an outside service provider in the event of a future data breach. Nearly all respondents (80 percent) were likely to consider using an outside service provider in the event of a future data breach. The areas in which they were most likely to consider using an outside service provider were litigation (54 percent) and data forensics/investigation (52 percent). Nearly half were also likely to report that they would consider using an outside firm to assist in extending remediation to individual victims. Notification of the individuals whose records were breached was considered by 44 percent of respondents, as was communication. Forty percent reported that they would consider using an outside vendor for public notification.

There are several points of clarification that can be made by type of organization. Respondents working for critical access hospitals were most likely indicate that they would bring in external resources for both data forensics and litigation. Nearly two-thirds of respondents (61 percent) noted that they would bring in a resource for data forensics, compared to half of respondents working for a general medical/surgical facility and 40 percent working for an academic medical center. In the area of litigation, 65 percent of respondents working for a critical access hospitals reported they would use outside resources, compared to half of respondents working for either an academic medical center or a general medical/surgical facility.

Finally, respondents were asked to identify those areas in which organizations could take additional steps to ensure that they were more effective in responding to future breaches. Nearly all respondents (88 percent) noted that it would be of value to debrief after a security breach to identify areas of improvement. Three-quarters also noted that it would be of value to have employees practice the steps outlined in the response plan on a regular basis. Respondents were least likely (49 percent) to report that they would engage or re-engage a security consultant to evaluate the nature of the breach and the organization's response to the breach. Only six percent of respondents stated that no additional steps were required at their organization.

12. Conclusion

The year 2010 and those that follow will surely turn a focused eye and heightened expectations on healthcare providers, payors and suppliers as the methods by which patient data is created, shared, and stored move into the digital landscape. There is no question that challenges lie along the path: multi-access systems that support quick, reactive patient care are not built for data breach prevention; many healthcare professionals perform their daily duties in highly-mobile, non-traditional workspaces; improved hiring and training practices are taking root, but they must produce serious behavioral change that is nurtured and sustained in the new electronic environment.

When considering the true cost of a data breach, organizations must recognize the direct costs (mailing expense, call center services) as well as indirect costs (fines and penalties due to missed regulatory deadlines or mandates).

Concern over patient satisfaction must extend to the manner by which the facility safeguards ALL patient data and inappropriate access to it – for those at the vulnerable point of injury or illness would be doubly wounded if their very identity were to be put at risk or compromised.

Reliance on third-party suppliers and vendors – such as contract caregivers, linen services and cafeteria food and beverage suppliers – must be balanced with due diligence about that third party's background screening methods, hiring practices, and training initiatives aimed at a heightened level of data security for all sensitive personal information, be that PHI or PII.

13. Survey Sponsors

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.

14. 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 2010 HIMSS Analytics Report: Security of Patient Data commissioned by Kroll's Fraud Solutions.

15. For more information, contact:

HIMSS Analytics

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

Kroll's Fraud Solutions

Donna Allen
Director of Marketing & Business Development
615-320-9800 x1389
donna.allen@kroll.com