INTRODUCTION

The 2012 HIMSS Analytics Report: Security of Patient Data is the third installment of a bi-annual survey of healthcare provider facilities in the United States regarding patient data safety. The survey was commissioned by the information security practice of Kroll Advisory Solutions (previously Kroll Fraud Solutions), a leading risk consulting firm 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.

According to the Department of Health and Human Services (HHS) Annual Report to Congress on Breaches of Unsecured Protected Health Information\(^1\), theft was once again the most commonly reported cause of large breaches in healthcare organizations in 2010. Among the 207 breaches that affected 500 or more individuals:

- 99 incidents involved theft of paper records or electronic media, together affecting approximately 2,979,121 individuals.
- Loss of electronic media or paper records affected approximately 1,156,847 individuals.
- Unauthorized access to, or uses or disclosures of, protected health information affected approximately 1,006,393 individuals.
- Human or technological errors, or other failures to take adequate care of protected health information, affected approximately 78,663 individuals.
- Improper disposal of paper affected approximately 70,279 individuals.

With data theft and compromise on the rise within the industry, the objectives of the HIMSS Analytics Report are: 1) to identify issues and progress relating to patient data security in U.S. hospitals and 2) to monitor and analyze significant trends in the industry and its environment (regulatory, operational). The end goal is to provide the industry with a more accurate view of the current state of patient data security in the U.S. and to use the analysis to inform current security measures and establish those that may be more effective in addressing the constantly evolving threats.

A variety of issues addressed within the study point to the fact that the U.S. healthcare industry is still one of the most at risk for significant data breaches, as well as one of the most likely to be targeted for its well of protected data. And, unfortunately, the changing landscape is only complicating the security challenges further. Since the 2010 report:

- Use of electronic health records (EHR) is on the rise, meaning patient data is more mobile and accessible.

\(^1\)  http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachrept.pdf
• Use of new technologies, in particular mobile devices in the workplace, have skyrocketed, creating new operational efficiencies and security vulnerabilities.
• Particularly with the rise of EHRs, more healthcare providers are entrusting their patient data to third parties, meaning that the scope of patient data security extends far beyond the walls of their own hospital.
• New regulatory requirements make achieving compliance even more challenging.

The latest installment of the HIMSS Analytics report reassesses the state of patient data security in the wake of these most recent developments and the impact they have on the industry’s ability to address and respond to the rising threats.
# Table of Contents

1. Executive Summary.............................................................................................................. 5
2. Methodology ........................................................................................................................ 10
3. Profile of Survey Respondents.......................................................................................... 10
4. Electronic Medical Records and Meaningful Use............................................................ 11
5. Compliance with Security Regulations and the Associated Risks.................................... 12
6. Risk Factors for Breach....................................................................................................... 15
7. Risk Analysis....................................................................................................................... 16
8. Third-Party Vendors........................................................................................................... 18
9. Preparation for Office of Civil Rights HIPAA Audits......................................................... 19
10. Ultimate Responsibility for Patient Data Security........................................................... 20
15. Conclusion......................................................................................................................... 35
16. Survey Sponsors ............................................................................................................... 35
   
   **HIMSS Analytics** ............................................................................................................. 35
   **Kroll Advisory Solutions** ............................................................................................... 35
17. How to Cite this Study ....................................................................................................... 36
18. For More Information ....................................................................................................... 36
1. Executive Summary

The healthcare industry’s approach to protecting patient data has evolved significantly since the bi-annual HIMSS Analytics Report: Security of Patient Data was first commissioned by Kroll Advisory Solutions in 2008. At the time, protecting patient privacy was the primary goal for most hospitals as they strived for compliance under the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II). But as the industry has moved toward more digital frontiers with an aggressive transition to electronic health records (EHR) and mobile-based devices, the increase in cyber threats and system vulnerabilities necessitates that privacy and security no longer be treated as separate issues.

Data breaches not only risk revealing patient health information, they also open up those whose information is compromised to identity theft, fraud and other violations. While hospitals are stepping up to regularly audit their monitoring and response procedures, reports of data breaches are on the rise.

In 2012, 27 percent of all respondents to this survey indicated their organization has had a security breach in the past 12 months (up from 19 percent in 2010 and 13 percent in 2008); of those who reported a breach, 69 percent experienced more than one.

The increase is likely due to a more accurate picture of security and privacy than had previously existed within the industry, thanks to more stringent auditing and reporting guidelines under regulations such as the Red Flags Rule\(^2\) and The American Recovery and Reinvestment Act of 2009’s Health Information Technology for Economic and Clinical Health Act’s (ARRA HITECH) Breach Reporting\(^3\) requirement.

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 increased regulation and the policies put in place to comply with those rules. However, there is cause for concern, as our new study shows that the security practices in place continue to overemphasize a “checklist” mentality for compliance without implementing more comprehensive and sustainable changes needed for meaningful improvements in the day-to-day handling of patient Personal Health Information (PHI) and Patient Identity Integrity (PII).

\(^2\) [http://www.ftc.gov/bcp/edu/microsites/redflagsrule/index.shtml](http://www.ftc.gov/bcp/edu/microsites/redflagsrule/index.shtml)

\(^3\) [http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/breachnotificationifr.html](http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/breachnotificationifr.html)
KEY FINDINGS IN 2012

Healthcare providers prioritize compliance over security

While increased regulation and better-articulated guidance have led to increases in privacy and security measures within hospitals, they have also contributed to a false sense of security within organizations that comply with these mandates.

Despite the increase in the number of breach incidents reported, most hospitals continue to believe that if they are more prepared, they are more secure.

On the whole, individuals responding to the 2012 survey reported they were more prepared than two years ago, giving themselves a 6.40 on a scale of one to seven in 2012, compared to 6.06 in 2010 and 5.88 in 2008. None of the 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”).

While organizations are actively taking steps to ensure that patient data is secure, they are so focused on meeting compliance requirements that they have little awareness of the efficacy of their security programs.

While 96 percent of respondents reported conducting a formal risk analysis at their organization, 27 percent reported they had experienced a breach and 18 percent were not aware of whether or not their organization had actually experienced a data breach in the past 12 months.

Of those who experienced a security breach, only one quarter said it triggered an update to their organization’s security action plan. Instead, 73 percent said changes in external policies and regulations such as HIPAA and ARRA HITECH drove updates to their action plan for securing patient information.

The majority of breaches result from internal sources

Similar to the studies in 2008 and 2010, respondents were most likely to indicate that breaches at their organizations were caused by an individual employed by the organization at the time of the breach.

In 2012, 79 percent of respondents reported that a breach was reported by an employee.
In another study question, respondents attributed 16 percent of breaches to actions taken by an outsourced or contract employee.

While organizations are strengthening policies and training in response to reported incidents, employees continue to be both accidental and deliberate actors within breaches. Forty-five (45) percent of respondents indicated that lack of staff attention to policy puts data at risk—an increase of 14 percent from 2010.

Fifty-six (56) percent of respondents 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. Respondents were much less likely to report that patient data at their organization was compromised in other ways.

Increases in outsourcing lead to vulnerabilities in security

As the outsourcing of patient data rises, the provider focus on compliance over security is creating more opportunities for third-party breaches.

Ninety-eight (98) percent of respondents require third parties to sign a Business Associate (BA) agreement and 82 percent require third parties to notify them of a breach, demonstrating very high levels of compliance with HIPAA regulations.

Meanwhile, other data security best practices not specified in current regulations show low levels of implementation.

Only half (56 percent) of respondents indicated they ensure that their third-party vendors conduct a periodic risk analysis to identify security risks and vulnerabilities.

The rate of providers requiring proof of employee background checks form partners was nearly static (56 percent in 2012 vs. 51 percent in 2010) and those requiring vendors to show proof of employee training actually dropped 10 percent (50 percent in 2012 compared to 60 percent in 2010).

It is likely that these security vulnerabilities have contributed to the rise in third-party breaches seen in 2012.
Eighteen (18) percent of respondents that experienced a breach in the past 12 months cited third parties as the source and 28 percent indicated that sharing information with external parties is the top item that put patient data at risk (up from 18 percent in 2010 and 6 percent in 2008).

**An increasingly mobile healthcare industry**

As mobile devices proliferate in exam rooms and administrative areas, so do the associated vectors of potential attack. Added to this are the risks from employee negligence and organizational policies that have not kept pace with ever-changing technology. In fact, 31 percent of respondents indicated that information available on a portable device was among the factors most likely to contribute to the risk of a breach (up from 20 percent in 2010 and four percent in 2008).

With more activities taking place on devices not tethered to a workstation, the risk of data loss and/or compromise is an issue many organizations are not properly prepared to address.

**Twenty-two (22) percent of respondents reporting a breach noted that data was compromised when a laptop, handheld device or computer hard drive was lost or stolen, which is twice the amount (11 percent) reported in 2010.**

**The debate continues: Who’s in charge of patient data safety?**

As securing patient data becomes an increasingly complex issue crossing nearly every department within health organizations, the question of who ultimately is responsible for championing the issue beyond mere compliance has become a game of hot potato.

As organizations struggle to address data and privacy breaches, a lack of ownership for the issue across the industry remains. Various titles hold responsibility for pieces of the compliance puzzle, ensuring that their organizations meet the mandates and regulations set forth, but the overall security picture continues to elude most.

When asked in the 2012 survey which individual in their organization was responsible for the security of patient data, the answers were fairly varied. Answers included:

- HIM Director – 21 percent
- Chief Information Officer – 19 percent
- Chief Privacy Officer, Chief Compliance Officer, Chief Executive Officer – each reported at 12 percent
• Chief Security Officer – 10 percent

Those naming Chief Security Officers dropped from 2010 (14 percent) and 2008 (22 percent) - a trend illustrating how the responsibilities of this role continue to be spread across other titles in organizations.
2. Methodology

HIMSS Analytics invited a variety of individuals with experience in their healthcare organization’s privacy and security environment to participate in this telephone-based survey. The 250 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. Data was collected in December 2011. Kroll Advisory Solutions provided funding and industry expertise for this research.

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 to encompass a cross-section of organizational sizes in this report.

One-third of the respondents who participated in this research identified their title as an HIM Director or Manager. Another quarter reported their title to be Compliance Officer (24 percent). Nearly one-quarter of respondents (21 percent) reported their title to be a senior IT executive, such as Chief Information Officer or Director of IT. Five percent (5 percent) of respondents were Chief Privacy Officers and 2 percent were Chief Security Officers. The remaining 10 percent of respondents hold “other” titles, including Risk Manager, Chief Executive Officer or Administrator, Director of Quality or HIPAA Security Officer.

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.”

- Small (under 100 beds) – 51 percent
- Medium (100 to 299 beds) – 30 percent
- Large (300 or more beds) – 18 percent

The average number of beds per hospital is 181 and the median is 88 beds.

The survey data will also be examined by type of hospital. A list of hospital types is below:

- General Medical/Surgical Hospitals – 56 percent
- Critical Access Hospitals – 34 percent
- Other Hospitals – 6 percent
- Academic Medical Centers – 3 percent
The “other” category includes pediatric, cardiac, long-term acute care and other types of specialty hospitals.

4. Electronic Medical Records and Meaningful Use

Respondents were asked how much of their organizations’ patient data was captured in an electronic record. The majority of respondents reported that their organization captures at least some patient data in an electronic format (94 percent). All responses are outlined in Figure One below.

![Percentage of Patient Data Captured in an Electronic Record](image)

**Figure One. Percentage of Patient Data Captured in an Electronic Record**

Half of the survey respondents (52 percent) reported that, at the time of data collection, their organizations had plans to attest for Stage One Meaningful Use, but had not yet done so. Another third (37 percent) had already attested. Five percent had no immediate plans to attest. The remaining 5 percent were unsure of their organization’s status. All of the data for this is recorded in Figure Two below.
By organization type, academic medical centers (43 percent) and general medical/surgical hospitals (41 percent) were most likely to report that they had already attested for Stage One. All academic hospitals in this sample had either attested at the time of data collection or indicated plans to do so in the future. Five percent of critical access hospitals and four percent of general medical/surgical hospitals had no plans to attest to Meaningful Use. There is no statistically significant relationship by bed size.

5. Compliance with Security Regulations and the Associated Risks

Respondents reported a high level of compliance with the security regulations that govern personal health information. Respondents were most concerned that a lack of attention to security policy would put patient data at risk.

Using a scale of one to seven (1-7), where one (1) is “not at all compliant” and seven (7) is “compliant with all applicable standards,” respondents were asked to rate their level of compliance with the regulations that govern personal health information (PHI). As Figure Three suggests, respondents indicated their organizations are most compliant with CMS regulations (average score of 6.64) and least compliant with ARRA HITECH, though compliance with this set of regulations is still very high (5.97). In general, as the figure below suggests, respondents continue to report having the highest level of compliance with CMS regulations.
Figure Three. Compliance with Industry Regulations

There were some differences in compliance by bed size and type of organization.

By bed size, those working for academic centers reported higher average levels of compliance with both ARRA HITECH and the Red Flags Rule. See below for average levels of compliance with both rules/regulations.

ARRA HITECH

- Academic Medical Centers – 6.50
- Other Hospitals – 6.38
- General Medical/Surgical Hospitals – 6.13
- Critical Access Hospitals – 5.57

Red Flags Rule

- Academic Medical Centers – 7.00
- Other Hospitals – 6.50
- General Medical/Surgical Hospitals – 6.21
- Critical Access Hospitals – 5.86
Large hospitals recorded higher than average scores for CMS regulations, the Red Flags Rule and ARRA HITECH. See below for the average compliance scores for each rule/regulation by bed size.

**CMS Regulations**

- Small (under 100 beds) – 6.54
- Medium (100 to 299 beds) – 6.70
- Large (300 or more beds) – 6.82

**Red Flags Rule**

- Small (under 100 beds) – 5.94
- Medium (100 to 299 beds) – 6.12
- Large (300 or more beds) – 6.67

**ARRA HITECH**

- Small (under 100 beds) – 5.68
- Medium (100 to 299 beds) – 6.22
- Large (300 or more beds) – 6.30

Looking at the average compliance across all regulations, respondents recorded an average score of 6.37. There are statistically significant relationships by type and bed size. These are noted below.

**Overall compliance average**

- Small (under 100 beds) – 5.84
- Medium (100 to 299 beds) – 6.16
- Large (300 or more beds) – 6.30

- Academic Medical Centers – 6.57
- Other Hospitals – 6.25
- General Medical/Surgical Hospitals – 6.11
- Critical Access Hospitals – 5.80
6. Risk Factors for Breach

Respondents were asked to identify what puts patient information most at risk at their organization. Nearly half of respondents reported that a lack of attention by staff to their organization’s security policy puts patient information at risk; this was also most frequently identified in the 2010 study.

Respondents were least likely to report that the lack of a security policy will put patient information at risk.

Overall, 12 percent of respondents noted that lack of a data incidence response plan puts patient data at risk and those working at small to medium hospitals were more likely to report the lack of an actionable data breach incident response plan.

- Medium (100 to 299 beds) – 15 percent
- Small (under 100 beds) – 14 percent
- Large (300 or more beds) – 2 percent

Sixteen (16) percent of respondents indicated that none of the items addressed in the study put patient information at risk.

In 2012, 16 percent of respondents noted that none of the items on this list put data at risk.

**ITEM THAT MOST PUTS DATA AT RISK**

![Graph showing item that most puts data at risk]

Figure Four. Item that Most Puts Data at Risk
7. Risk Analysis

Most hospitals are conducting a formal risk analysis, with two-thirds relying on internal resources to lead the initiative. Respondents are also likely to rely on NIST and Meaningful Use guidelines when conducting a risk analysis.

Respondents were asked to identify the type of resource their organization uses to lead a formal risk analysis. Nearly all of the respondents in this study conduct a formal risk analysis at their organization (96 percent).

Among those conducting a formal risk analysis, 65 percent rely on internal resources to lead the initiative; approximately one-quarter (27 percent) reported that the initiative is led by an external resource, such as a consultant.

The majority of respondents (63 percent) use a combination of internal and external resources to complete their risk analysis. Another third (31 percent) reported that they rely solely on internal resources to conduct their risk analysis, with five percent using only external resources.

By organization type, none of the academic medical centers in this study rely solely on internal resources to conduct their risk analysis. On the other hand, more than one-third of critical access hospitals (37 percent) and 31 percent of general medical/surgical hospitals conduct their risk analysis using only internal resources.

Respondents were also asked to identify the role that two specific initiatives play in their risk analysis: CMS Meaningful Use requirements and NIST guidance. Eighty-eight percent (88) of respondents take CMS Meaningful Use requirements into consideration. General medical/surgical facilities (91 percent) and critical access hospitals (89 percent) were more likely to take these regulations into consideration than academic medical centers (71 percent). Another three-quarters (71 percent) of respondents take NIST standards into consideration. There were no statistically significant relationships by bed size or organization type.
Respondents were most likely to report their risk analysis had uncovered a deficiency in their security policies and/or procedures. More than 40 percent of respondents also indicated their risk assessment indicated gaps in use of physical or technical IT security measures.
Respondents that identified gaps were most likely to report that their risk assessment led them to establish a data breach incident response plan for the first time (19 percent). They were much less likely to report that their risk analysis led to the establishment of new HR practices.

8. Third-Party Vendors

Nearly all respondents require their third-party vendors to sign business associate agreements as required under current regulations, yet fail to hold third parties to other best practice security standards.

Respondents were asked to identify what due diligence they performed to ensure that third-party vendors comply with organizational privacy and security policies and procedures. In general, the responses recorded in 2012 are similar to those recorded in 2010. As in 2010, respondents were most likely to require their third-party vendors to sign a Business Associate (BA) agreement for accessing patients’ personally identifiable information for HIPAA compliance. While respondents were least likely to require third parties to show proof of employee training, it was still selected by half of survey respondents. More than half (56 percent) of respondents ensure their third-party vendors conduct a periodic risk analysis to identify security risks and vulnerabilities.

Figure Seven. Due Diligence Performed to Ensure that Third Parties are Compliant
9. Preparation for Office of Civil Rights HIPAA Audits

Nearly all respondents indicated their organization had taken steps to prepare for a potential Office of Civil Rights (OCR) HIPAA audit. Because of these actions, respondents recorded an average level of preparation of 5.50, based on a one to seven scale.

Respondents were asked to identify steps taken to prepare for a potential Office of Civil Rights (OCR) HIPAA audit. Nearly all respondents reported that their organization had taken some type of action (98 percent). The full list of each specific action is identified in Figure Eight below.

**Figure Eight. Actions Taken in Preparation for an OCR HIPAA Audit**

In general, more than half (58 percent) reported using only internal resources to prepare for this type of audit. Another 35 percent reported using a combination of internal and external resources. Only one percent of respondents indicated that they relied only on external resources.

Only four percent of respondents indicated that their organization has had an OCR HIPAA Audit. Using a one-to-seven scale, where one is “not at all prepared” and seven is “extremely prepared,” respondents recorded an average level of preparation of 5.50. In fact, only one respondent indicated a score of one, suggesting that they were not at all prepared for this type of audit.
Despite the fact that the majority of respondents reported taking multiple steps to prepare for an OCR HIPAA audit, 90 percent of respondents reporting they had experienced an audit indicated that they would take a variety of actions to better prepare for an audit in the future. Respondents were most likely to indicate they would conduct a risk analysis more frequently.

**Figure Nine. Additional Steps that Would Have Enhanced Preparation for a HIPAA Audit**

- Conduct a More Frequent Risk Analysis: 60%
- Contract with HIPAA Consultant for a Practice Audit: 60%
- Better Organizational Understanding of Audit Parameters: 50%
- Hire Appropriate Staff Versed in Security Requirements: 50%
- Other: 10%
- Don't Know: 10%

Only two percent of all respondents reported that their organization had been fined as a result of a HIPAA violation.

**10. Ultimate Responsibility for Patient Data Security**

There continues to be a lack of consensus in the industry with regard to who is most often responsible for data security, with HIM Directors and CIOs both being identified by a similar number of respondents. Regardless of where the responsibility lies, respondents were overwhelmingly likely to report that this individual had support from top management.

The two previous studies suggested that the responsibility for patient data security was spread across a wide variety of job titles, a trend that continues in 2012. A full breakdown of titles is included in Figure Ten.
There are also differences in who has ultimate responsibility by type of organization—respondents working for an academic medical center were most likely to report that a Chief Compliance Officer has this responsibility (29 percent); at general medical/surgical facilities, CIOs are most likely to have this responsibility (26 percent). At both critical access hospitals and other hospitals, HIM Directors are most likely to have this responsibility (23 percent and 38 percent respectively).

Respondents working for small and medium-sized hospitals were most likely to report that the HIM Director has this responsibility (24 percent for each hospital segment). One-third of respondents at large hospitals indicated that CIOs have this responsibility.

Respondents were also asked to rate the extent of top-level support that the person responsible for patient data security receives. On a one-to-seven scale, where one is “no support” and seven is “highly supported by top management,” respondents reported an average score of 6.46. This finding closely matches data reported in the 2010 study (6.47). Indeed, approximately two-thirds of respondents (64 percent) selected a score of seven on this scale. There was no relationship by bed size or organization type.
11. Measures for Securing Patient Information

Organizations use a wide variety of tools to secure patient information. Hiring practices, such as background checks, security policies and procedures, and data access minimization are most widely used.

All respondents reported using at least one of the measures outlined in this study to secure patient information at their organization. In fact, half of the respondents use all 11 measures outlined in this research and 26 percent use ten of the 11 measures. Figure Eleven demonstrates the full spectrum of measures employed by respondents in this study.

<table>
<thead>
<tr>
<th>Measures Used to Safeguard Patient Information</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hiring Practices</td>
<td>98%</td>
</tr>
<tr>
<td>Security Policies/Procedures</td>
<td>96%</td>
</tr>
<tr>
<td>Data Access Minimization</td>
<td>96%</td>
</tr>
<tr>
<td>Conducting ID Checks</td>
<td>94%</td>
</tr>
<tr>
<td>Having Data Breach Incidence Response Plan</td>
<td>92%</td>
</tr>
<tr>
<td>Audit Functions In IT Applications</td>
<td>92%</td>
</tr>
<tr>
<td>Physical Security Measures</td>
<td>91%</td>
</tr>
<tr>
<td>Periodic Risk Analysis Conducted</td>
<td>89%</td>
</tr>
<tr>
<td>Technical IT Security Measures</td>
<td>87%</td>
</tr>
<tr>
<td>Formal Education Courses for Employers</td>
<td>86%</td>
</tr>
<tr>
<td>HR Monitors Completion of Courses</td>
<td>85%</td>
</tr>
</tbody>
</table>

Figure Eleven. Measures Used to Safeguard Patient Information

With regard to bed size, a higher percentage of respondents working for large hospitals (300 or more beds) used the following measures to safeguard patient information when compared to their counterparts at smaller organizations.

IT Applications with Audit Functions

- Small (under 100 beds) – 86 percent
- Medium (100 to 299 beds) – 96 percent
- Large (300 or more beds) – 100 percent
Technical IT Security Measures

- Small (under 100 beds) – 80 percent
- Medium (100 to 299 beds) – 92 percent
- Large (300 or more beds) – 100 percent

Periodic Risk Analysis to Identify Security Risks and Vulnerabilities

- Small (under 100 beds) – 85 percent
- Medium (100 to 299 beds) – 90 percent
- Large (300 or more beds) – 98 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 94 percent of general medical/surgical hospitals. In comparison, 91 percent of respondents at critical access hospitals reported using this technology, as did only 75 percent of those from other hospitals. A similar analysis can be made for the use of hiring practices such as background checks—all respondents working for an academic medical center have these in place, as do 99 percent of respondents working for a general medical/surgical hospital or critical access hospital. This percentage drops to 88 percent among respondents working for other hospital types.


Most healthcare organizations make monitoring the effectiveness of their security action plans part of their normal business process. Three-quarters of respondents also take external policies and regulations, such as ARRA HITECH, into consideration.

Respondents were asked to identify what triggered their most recent update to their organizations’ action plan. Approximately 13 percent of respondents reported that a key trigger was that they did not have an action plan in place previously; this is consistent with previous studies.

Most respondents, however, continue to report that updating their organizations’ action plan takes place routinely to ensure it remains effective and appropriate (85 percent). Changes in external policies and regulations, such as ARRA HITECH, are also frequently taken into consideration, as evidenced by nearly three-quarters (73 percent) of responses. More than half of respondents (57 percent) also considered items identified in their risk analysis when evaluating their security action plan.
A security breach at their own organization was least likely to trigger an update to a security action plan, with only 14 percent of responses. Of those who experienced a security breach in the past 12 months, only one-quarter said it triggered an update to their organization’s security action plan.

In addition, 97 percent of respondents’ organizations use data analytics to inform the efficacy of their security environments. Respondents were most likely to report analyzing data from IT audit logs for inappropriate access to patient data; this response was selected by 84 percent of respondents. Three-quarters of respondents (74 percent) monitor movement of certain types of data across the different systems in their environment. A similar percentage (72 percent) indicated that their organization analyzes financial transactions for anomalies that might indicate fraud. There was no relationship by bed size or organization type.

13. Security Breach

More than one-quarter of all respondents reported their organization has had a security breach in the past 12 months, up from the 19 percent in the 2010 study. Most frequently compromised were patient name and birth date.
More than one quarter of all respondents (27 percent) indicated that their organization had experienced at least one security breach that required notification in the past 12 months. This represents a continued increase in the number of respondents reporting a breach, when compared to the past two surveys. Figure Thirteen below provides additional detail.

![PERCENT OF ORGANIZATIONS REPORTING A SECURITY BREACH IN THE PAST 12 MONTHS](chart)

**Figure Thirteen.** Percent of Organizations Reporting a Security Breach in the Past 12 Months

In general, respondents were more likely to report multiple security breaches than they were in the past. Among respondents reporting a breach, approximately one-third (31 percent) reported their organization had one breach in the past 12 months; another 28 percent reported having two breaches in the past 12 months. One-third (35 percent) reported having three to nine data breaches in the past 12 months. Six percent of respondents reported that they had experienced more than 10 breaches at their organization in the past 12 months.
Figure Fourteen. Number of Reported Security Breaches

By organization type, a greater percentage of academic medical centers were more likely to report security breaches than were other types of organizations:

- Academic Medical Centers – 43 percent
- General Medical/Surgical Hospitals – 36 percent
- Other Hospitals – 19 percent
- Critical Access Hospitals – 13 percent

Respondents working for larger hospitals continue to be more likely to report a security breach than those working for smaller hospitals.

- Large (300 or more beds) – 46 percent
- Medium (100 to 299 beds) – 38 percent
- Small (under 100 beds) – 14 percent

This is consistent with what has been reported in both the 2010 and 2008 studies.

Respondents were asked to identify the type of data that was compromised in a security breach. Nearly 90 percent of respondents noted that a patient’s name was compromised in one or more security breaches at their organization, consistent with the data most likely to be breached in
previous years. Another two-thirds (65 percent) reported that date of birth was compromised, and 60 percent reported that other demographic information, such as gender or employer, was compromised. Figure Fifteen below provides a full list of data types compromised.

![INFORMATION COMPROMISED IN A SECURITY BREACH](image)

In 2012, only two percent of respondents indicated credit card information was breached.

Figure Fifteen. Information Compromised in a Security Breach

In the past, respondents were most likely to indicate that breaches at their organizations resulted from unauthorized access to information by an individual employed by the organization at the time of the breach. This continues to be the case, with 56 percent of this year’s respondents reporting this was the source of a breach that took place at their organization in the past 12 months. One-third of respondents indicated that a breach was the result of wrongful access of paper-based patient information. Rounding out the top three responses is data accessed when a laptop/hand-held device or computer hard drive is stolen or lost. A full list of data breach sources and a comparison to the past two years of data is provided below.
Other breach sources included data housed by third-party vendors (10 percent), improper destruction of paper-based records (nine percent), network access by an individual outside the organization (three percent) and a second-hand computer from which data wasn’t removed (two percent).

Compared to the data from previous studies, respondents were still most likely to report that a security breach was the result of an action taken by an individual affiliated with the organization at the time of the breach. Three-quarters of respondents (79 percent) reported that the breach was perpetrated by an employee and 16 percent stated that the breach was the result of actions taken by an outsourced or contract employee.

While respondents in the 2012 study were less likely to report that a breach was the result of the actions of an individual not associated with the organization, these numbers did rise in comparison to previous studies. For instance, 20 percent of this year’s respondents noted that a breach was the result of actions taken by individuals not associated with the organization. This was more than three times the six percent recorded in 2010. The number of respondents reporting that a breach was the result of actions taken by a third party, contractor or former employee are also greater than they were in past studies. Figure Seventeen below provides a full list of perpetrators.
In 2012, only two percent of respondents indicated another perpetrator for the security breach.

Figure Seventeen. Perpetrator of a Security Breach

Most respondents (93 percent) reported that their organization had a breach incident response plan in place. When asked to rate their level of “preparedness” to address a security breach, respondents who work for organizations at which a breach was reported indicated an average preparedness level of 6.40, on a one-to-seven scale—where one is “not at all prepared” and seven is “extremely prepared.” In fact, more than half of respondents (54 percent) rated their readiness as a seven. None of the respondents indicated that their readiness at the time of the security breach was a one or two. This is a slight increase from the 6.06 preparedness level reported in 2010.
Figure Eighteen. Organizational Preparedness to Address a Security Breach

Nearly 90 percent of respondents noted that their organization made changes in their security practices as a result of a security breach. This represents a continued increase from what has been reported in the past two surveys conducted. The 12 percent of respondents who reported that their organization had taken no action as a result of a security breach compares to 17 percent of respondents in 2010 and 35 percent in 2008. A full list of actions is shown below.
Increased employee training was the most frequent response to a security breach, with 84 percent of responses. This was also the top response selected in both the 2010 and 2008 studies. Nearly one-third of respondents (31 percent) noted they had increased the frequency of their risk analysis to identify security risks and vulnerabilities. Also selected by at least one-quarter of respondents were changes to organizational policies/procedures (29 percent) and organizational data breach incident response plans (28 percent).

Respondents were least likely to terminate contracts with their third parties after a breach (four percent); this was the same percentage that reported this option in the 2010 study. Additionally, respondents in this year’s study were much less likely to purchase additional security tools in response to a breach (six percent), compared to 19 percent in the 2010 study.

Organizations must address the consequences of inadvertent data breach. As such, 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 37 percent of respondents; this is consistent with what was reported in the 2010 study. Another quarter of respondents were concerned about the financial impact, such as additional costs associated with credit monitoring; this is an increase from the 15 percent of respondents who identified this as a key concern in 2010.
Approximately 10 percent of respondents indicated that they were concerned about the impact the breach had on their ability to conduct business as usual and six percent were concerned about lawsuits that would be filed by patients impacted by the breach. Only two percent of respondents indicated that they would have to switch a third-party vendor because of a security breach.

Figure Twenty. Perceived Impact of a Security Breach

Respondents were much more likely to report that they would offer remediation services to patients impacted by a security breach than they were in the past. In 2012, 95 percent of respondents indicated that they would offer some type of service. In comparison, three-quarters of respondents noted this was the case in 2010. A full list of the remediation services offered by respondents is identified in Figure Twenty-One below.
Patient notification continues to be the most frequent response, identified by 90 percent of respondents. However, compared to 2010, respondents were much more likely to report that they would take additional actions. Nearly half of respondents reported that they would offer a customer service line for patients whose data had been breached and one-third would offer credit monitoring. Both of these are double the percentages of respondents who reported offering these services in 2010. However, the percentage of respondents offering identity theft consultation/restoration has changed little in the past two years. In this year’s study, this was offered by 18 percent of respondents, compared to 13 percent of respondents in 2010.


Most respondents are open to the idea of using an outside service provider in the event of a future data breach, particularly to get assistance in notifying individuals whose records have been breached.

Respondents that had experienced a data breach at their organization 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 (91 percent) were likely to consider using an outside service provider in the event of a future data breach. Respondents were most likely to consider using an outside service provider to notify individuals whose records were breached (60
percent). At least half of those that had experienced a breach would consider using external resources to conduct a security assessment to enhance future prevention (56 percent), to provide compliance and litigation support (53 percent) and to notify public and/or registry agencies (50 percent). Respondents were least likely to use outside assistance to handle public relations (PR) and crisis communications (31 percent).

Figure Twenty-Two. Use of Outside Provider in Event of a Future Data Breach

All 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 (90 percent) indicated it would be of value to debrief after a security breach to identify areas of improvement. More than three-fourths (80 percent) also noted that it would be of value to have employees practice the steps outlined in the response plan on a regular basis and two-thirds (68 percent) noted that it would be beneficial to increase the frequency of risk analysis to identify security risks and vulnerabilities. Respondents were least likely (48 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. Twelve percent (12 percent) of respondents stated that no additional steps were required at their organization.
15. Conclusion

There continues to be a lack of awareness of the financial implications associated with a healthcare breach. While the number of respondents reporting concern about the financial impact of a breach increased from the last time the study was conducted, only one-quarter of respondents reported concerns in this area. 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, will make the costs associated with a breach even more burdensome.

While hospitals are conducting the formal risk analysis mandated (89 percent reported that they conduct periodic risk analysis), they are not taking the proactive steps to move further than the end goal of compliance. While a strong step in the right direction, it is only the first half of the equation. The industry must move from a monitoring and reactive stance to more proactive measures to protect against the rapidly evolving threats facing the protection of patient data.

Until the industry begins to link security with compliance, confronting the risks – from employees to new technologies – head on, patient data will continue to be at risk. Knowing that the continued implementation of EHRs and introduction of new technologies in the workplace will only complicate the security landscape, the sense of urgency is clear. When it comes to taking proactive steps to protect the security and integrity of patient information, the time is now.

16. Survey Sponsors

*HIMSS Analytics*

HIMSS Analytics is a wholly owned not-for-profit subsidiary of the Healthcare Information and Management Systems Society. The company collects and analyzes healthcare data related to IT processes and environments, products, IS department composition and costs, IS department management metrics, healthcare trends and purchase-related decisions. HIMSS Analytics delivers high quality data and analytical expertise to healthcare delivery organizations, healthcare IT companies, state governments, financial companies, pharmaceutical companies, and consulting firms. Visit [www.himssanalytics.org](http://www.himssanalytics.org) for more information.

*Kroll Advisory Solutions*

Kroll Advisory Solutions, the global leader in risk mitigation and response, delivers a wide range of solutions that span investigations, due diligence, compliance, cyber security and physical security. Clients partner with Kroll Advisory Solutions for the highest-value intelligence and
insight to drive the most confident decisions about protecting their companies, assets and people.

Kroll Advisory Solutions is recognized for its expertise, with 40 years of experience meeting the demands of dynamic businesses and their environments around the world. Headquartered in New York with offices in 29 cities across 17 countries, Kroll Advisory Solutions has a multidisciplinary team of 700 employees. For more information, visit: www.krolladvisorysolutions.com.

17. 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 2012 HIMSS Analytics Report: Security of Patient Data commissioned by Kroll Advisory Solutions.

18. For More Information

HIMSS Analytics
Joyce Lofstrom
Director, Corporate Communications
312-915-9237
jlofstrom@himss.org

Kroll Advisory Solutions
Susan Moerschel
Senior Director, Marketing & Communications
615-340-9684
SMoerschel@Kroll.com