6th Annual HIMSS Security Survey
February 19, 2014

Sponsored by

Experian
In 2008, HIMSS launched the first Annual Security Survey. This survey captures the experiences of information technology (IT) and security professionals from U.S. healthcare provider organizations relating to electronic patient data security. The survey covers a multitude of topics including an organization’s general security environment, access to patient data, access tracking and audit logs, security in a networked environment, use of security technologies, security breaches and medical identity theft.

Over the past six years, the survey has been expanded continually to encompass new topics relevant to the current security environment. For four years, the Medical Group Management Association (MGMA) has been an active supporter of this research project and has been very instrumental in garnishing participation from physician practices. This year’s study is underwritten by Experian® Data Breach Resolution.

Contents

1. Executive Summary
2. Profile of Survey Respondents
3. Information Security Staffing & Budgets
4. Proactive Measures for Evaluating Risk to Patient Data
5. Employee/Patient Data Access
6. Access Tracking/Audit Logs
7. Use and Measurement of Security Controls
8. Security in a Networked Environment
9. Use of Security Technologies
10. Security Breaches and Medical Identity Theft
11. Conclusion
12. About HIMSS
13. About Experian
14. How to Cite This Study
15. For More Information
Figures

All figures in this report can be found in the report Appendix; several are also highlighted throughout the report.

1. Participant Profile—Organization Type
2. Level of Participation in Maintaining Privacy and Security
3. Hospital Participant Profile—Title
4. Participant Profile—Type of Medical Practice
5. Participant Profile—Region
6. Greatest Issue Concerning Security Threats
7. Human Factor Concerns
8. Infiltration/Intrusive Attack Concerns
9. Virus/Malware Concerns
10. Most Common Threat Motivators
11. Percent of IT Budget Dedicated to Information Security
12. Change in Percent of IT Budget Dedicated to Information Security
13. Impact of Federal Initiatives on Federal Budget
14. Percent of IT Budget Dedicated to Breach Remediation Efforts
15. Personnel Responsible for Securing Environment
16. Frequency of Conducting a Formal Risk Analysis
17. Uses of Risk Analysis Data
18. Length of Time Needed to Correct a Deficiency by Revising Security Controls
19. Length of Time Needed to Correct a Deficiency by Revising Policies/Procedures
20. Frequency of Auditing IT Security Plan
21. Frequency of Testing Data Breach Response Plan
22. Method for Controlling Organizational Access to Patient Information
23. Means by Which Organizations Provide Electronic Information to Patients
24. Method of Controlling Access to Health Websites/Portals Offered to Patients
25. Types of Systems from Which Audit Log Data is Collected and Analyzed
26. Events Captured From Audit Log Data
27. Use of Audit Log Data
28. Plan in Place to Respond to Threats or Security Breaches
29. Means for Measuring Success of Security Controls in Place
30. Existing Data Sharing Relationships
31. Future Data Sharing Relationships
32. Percent of Business Associates with Formalized Agreement
33. Use of Security Technologies – Top Ten
34. Devices on Which Data is Encrypted
35. Number of Cases of Medical Identity Theft
36. Instance of Security Breach
37. Percent of Breaches Reported to Authorized Groups
38. Breach is the Fault of Business Associate
1. Executive Summary

Concerns around the security of patient data have been a long standing issue in healthcare information technology circles. In fact, ten years ago, the 2004 HIMSS Leadership Survey indicated that two-thirds of respondents had concerns that internal breaches could compromise the security of electronic information, and breaches of electronic health data remain a concern in this year’s 2013 HIMSS Security Survey. The study was supported by MGMA and sponsored by Experian® Data Breach Resolution.

This survey, which profiles the data security experiences of 283 information technology (IT) and security professionals employed by U.S. hospitals and physician practices, found (among other things) that the greatest “security threat motivator” they encounter is that of healthcare workers potentially snooping into the electronic health information of friends, neighbors, spouses or co-workers.

Recognizing that inappropriate access of data by employees is a key area for which organizations are at risk of a security breach, healthcare organizations continue to strengthen the suite of technologies in place to secure data. Use of several key technologies related to employee access to patient data have all increased, including user access controls and audit logs of each access to patient health records.

Additionally, healthcare organizations are using multiple means of controlling employee access to patient information. Two-thirds of respondents reported that they use at least two access control mechanisms, such as user-based and role-based access controls, for controlling employee access to data. Furthermore, the number of respondents indicating their organization is collecting and analyzing data from audits logs is also increasing. For instance, the number of respondents that report their organization analyzes data from their firewalls, applications and servers has all increased in the past year.

Lastly, healthcare organizations are more frequently auditing their IT security plan to ensure they are ready in the event that a breach – internal or external – takes place.

Other key survey results include:

**Risk Analysis:** Ninety-two (92) percent of respondents noted their organization conducts a formal risk analysis. Significantly, while the number of respondents working for a hospital that conducted a risk analysis remained relatively consistent, the number of respondents working for physician practices that reported their organization conducted a risk analysis increased from 65 percent in 2012 to 78 percent in 2013.

**Data Breach Response Plan:** More than half of respondents (54 percent) reported that their organization has tested their data breach response plan. Those working for hospitals were more likely to report that this was the case, compared to respondents working for physician practices. Two-thirds of those who responded that their organization tests their data breach response plan reported that their plan was tested annually.

**Maturity of the Security Environment:** Using a scale of one to seven, where one is not at all a mature security environment and seven is highly mature, respondents recorded an average score of 4.35. This is a slight decrease from the average recorded in 2012 (4.64).
Security Budget: While more than half of respondents indicated that their security budget increased in the past year, half report spending three percent or less of their overall IT budget on securing patient data. Those working for physician practices tend to spend a higher percent of their IT budget on security than those working for hospitals.

Oversight of Information Security: About half of the hospital-based respondents reported that they had a Chief Security Officer, Chief Information Security Officer or other full-time resource in charge of the security of patient data. Approximately one-percent of respondents reported that this function is outsourced.

Patient Data Access: A majority of respondents (89 percent) reported making patient data available to patients, surrogates and/or designated others. Respondents were most likely to report that this data is shared via CD/DVD. Nearly half (43 percent) share data via a health website or web portal.

Significantly, in previous HIMSS Security Surveys, respondents have consistently indicated their organizations were most likely to use user-based controls to control access to patient information. While this type of access control is used by 71 percent of respondents, for the first time this year, it was eclipsed by the number of respondents indicating their organization relied on role-based access controls (78 percent).

Security in a Networked Environment: Respondents working for hospitals were much more likely than their counterparts at physician practices to report that they shared information with other healthcare organizations. Future participation in organized health information exchange organizations was expected to grow among all survey respondents.

Use of Security Technologies: While use of firewalls and user access controls has remained widespread in the past several years, growth of technologies such as biometric technologies and public key infrastructure continues to be limited.

Respondents were least likely to report encrypting data that was associated with their mobile medical devices, such as a wireless-enabled monitoring device. Only 17 percent of respondents indicated that data on these devices was encrypted.

Medical Identity Theft: Twelve percent of respondents reported that their organization has had at least one known case of medical identity theft reported by a patient in the previous 12 months.

Security Breaches: Nineteen percent of respondents reported that they had a security breach in the last year. The majority of these breaches involved less than 500 patients. Three-quarters (79 percent) reported that they notified patients impacted by the breach. Only eight percent of respondents indicated that the security breach was the result of actions taken by a business associate.
2. Profile of Survey Respondents

A total of 283 individuals completed the 2013 HIMSS Security Survey, sponsored by Experian® Data Breach Resolution. Data was collected via a web-based survey in the fourth quarter of 2013.

Qualifying Respondents

To ensure the data represents only the insights of individuals directly involved in maintaining a secure environment for patient data, respondents were asked qualifying questions.

Those respondents identifying their primary worksite as physician practice were required to answer “Yes” to the following question – “Do you play a role in developing the security environment at your organization?” These respondents also had to have worked for a physician’s practice with either an Electronic Health Record (EHR) or document imaging management system in order to be included in the survey.

All other respondents were required to answer “Yes” to at least one of the questions below in order to be eligible to take the survey.

- I am responsible for developing the organization’s policy on privacy and data security;
- I am part of a committee that is responsible for developing the organization’s policy on privacy and data security;
- I am responsible for ensuring that our data is secure on a day-to-day basis
- I am responsible for handling the remediation of a security breach at our organization;
- My department is notified of all security breaches in the organization that require notification;
- I am an IT professional (outsourcer) who handles IT for a healthcare organization; or
- I am responsible for interacting with all federal and/or state compliance authorities on a routine basis to and facilitate internal implementation of new privacy and data security protocols.

Approximately three-quarters of respondents (71 percent) answered “yes” to at least two of the above questions. Those individuals indicating they played no role in the security of data at their organization were excluded from the data collection process. These individuals are not included in the 283 responses upon which the analysis in this report is based.

Two-thirds of respondents (67 percent) reported they had responsibility for ensuring the day-to-day security of their organization’s data. Respondents were least likely (nine percent) to report being an outsourced IT professional who has responsibility for IT at a particular healthcare organization.

Approximately half (49 percent) of respondents indicated they are the Chief Information Officer at their organization and 11 percent are the Vice President of IS/IT. Another 12 percent of respondents reported their title to be IS/IT Director. An additional ten percent reported their title to be Chief Security Officer, while one percent reported being the Chief Privacy Officer at their organization. The remaining 15 percent of respondents reported their title as “other”, which includes a wide variety of IT and security titles. By
design, respondents from physician practices were not asked their titles. See Figure One for full details on title type.

![Hospital Participant Profile – Title](image)

**Figure One.** Hospital Participant Profile—Title

**Organization Type**

Slightly more than half of the respondents work for a stand-alone hospital (52 percent). An additional 18 percent work for a hospital that is part of a delivery system and 11 percent work at the corporate offices of a healthcare system. Physician practices comprise 16 percent of the sample. The remaining three percent of respondents work for a variety of healthcare organizations. The average number of licensed beds in this sample size is 265.80.

Physician practices sampled in this survey have an average of 18.28 physician FTEs. The largest practice in this sample has 100 physicians. The vast majority of these practices (89 percent) classified themselves as an independent physician practice. Another seven percent of respondents describe their organization as a federally qualified health centers (FQHC)1 and two percent describe their organization as a freestanding ambulatory surgery centers. The remaining facilities represent a social services agency and a multispecialty practice integrated with a hospital.

For the purposes of analysis in this report, the sample will be divided into two broad categories. The first will include hospitals and hospital-based organizations and will be referred to in this study as “hospitals”. The second group will be based on those respondents that work in an outpatient (ambulatory) setting. They will be referred to as physician practices. In addition, some of the questions in this research were not asked of individuals working at a physician practice. When this is the case, this will be noted in the report. Additionally, differences in security practices among hospitals and physician practices will be highlighted throughout the report only when they are statistically significant.

---

The greatest percentage of respondents (19 percent) comes from the East North Central region, followed by the West North Central region at 16 percent. The fewest respondents come from New England and East South Central (five percent each). The regions are defined by the U.S. Census Bureau².

3. Information Security Staffing & Budgets

Approximately half of respondents (51 percent) indicated that their organization has increased the budget and resources dedicated to information security as a result of federal initiatives impacting privacy and security such as OCR audits, Meaningful Use and the HIPAA Omnibus Rule. However, half of respondents continue to report spending three percent or less of their IT budget on security-related initiatives.

Additionally, half of respondents (52 percent) reported that they have a full-time resource, such as a Chief Security Officer, in place to oversee their organization’s security environment.

Information Security Budgets

In order understand the financial investment healthcare organizations are making to secure patient information, respondents were asked a series of questions surrounding their level of investment, as well as the factors that impact the choices made regarding investment levels. Respondents were asked to identify how federal privacy and security initiatives, such as OCR audits, HIPAA breach notifications, the HIPAA Omnibus Rule and Meaningful Use are impacting the budget and/or resources being dedicated to information security.

Approximately half of respondents (51 percent) indicated that their organization has increased the budget and resources dedicated to information security as a result of these federal initiatives. Another quarter (27 percent) of respondents indicated these federal initiatives have not impacted the budget/resources dedicated to information security. Sixteen (16) percent reported their organization had diverted resources from their information security efforts as a result of the federal initiatives they are presently addressing. This data is consistent with what was reported in 2012. There is no statistically significant relationship between the impact on budget/resources dedicated to information security and organization type.

Respondents were also asked to identify the percent of their organization’s overall IT budget that is dedicated to information security. Half of respondents indicated that their organization spends three percent or less of the organization’s overall IT budget on information security. Another 19 percent noted that they spend four to six percent of their IT budget on information security. Thirteen (13) percent indicated that they spend seven percent or more of their IT budget on information security. However, it should also be noted that 18 percent of respondents were not aware of the percent of their organization’s budget on IT. These numbers are consistent with what was reported in 2012. When this study was first conducted in 2008, more than half of respondents (57 percent) reported that their organization dedicated less than three percent of the overall IT budget to information security.

By organization type, respondents working for physician practices spent more of their overall IT budget on information security than did respondents working for hospitals. Approximately three percent of respondents working for hospitals reported spending more than 12 percent of their budget on information security, compared to seven percent of respondents working for physician practices.

With regard to how their IT security budget had changed in the past year, approximately half of respondents (51 percent) indicated that their budget had increased in the past year. This is similar to what was reported in 2012, when 56 percent of respondents reported a budget increase in this area. Four percent of respondents indicated that the security budget at their organization decreased, while the remaining respondents (39 percent) indicated no change in their information security budget in the past year. There are no statistically significant differences by organization type for this question.

Lastly, respondents were asked with regard to their IT budget the amount dedicated to breach remediation efforts. More than half of respondents (54 percent) indicated they spent less than one percent of their organizations’ overall IT budget on remediation efforts. Another 18 percent of respondents indicated that between one and three percent of their IT budget was dedicated to remediation. This is consistent with what was reported in 2012. Only two percent of respondents indicated they spend seven to 12 percent of their IT budget on remediation efforts. Twenty (20) percent of respondents were unsure how much of their IT budget is spent on these efforts.

**Information Security Staffing**

Respondents working for hospital-based organizations were asked to identify how their organizations staffed their security function. About half (52 percent) reported they have either a Chief Security Officer (CSO)/Chief Information Security Officer (CISO) or another full time staff member other than a CSO/CISO in place. This is a slight decrease from the 61 percent that reported this to be the case in 2012. Forty (40) percent of respondents reported that security functions at their organization are handled by part-time staff. Six percent of respondents indicated that no one at their organization was
4. Concerns Regarding Security of Patient Information

The greatest security threat to patient data is that it will be compromised by an organization’s staff. Eighty (80) percent of respondents noted that they were concerned that human-related factors would put data at risk. Furthermore, respondents were most likely to indicate the greatest motivator leading to the compromise of data is for workforce members to snoop on co-workers, friends and neighbors patient information.

For the first time in the 2013 study, respondents were asked to identify the areas they believed posed a security threat to health data at their organizations. Using a scale of one to seven, where one is not a threat and seven is an area that is of high threat concern, respondents were most likely to identify human-related factors such as individuals circumventing controls or disclosing information in error as the greatest area of concern (5.64). Respondents were least likely to identify loss of integrity of information, such as database corruption as a concern (4.32). The average scores of all areas of concern tested in this study are identified in the table below.

<table>
<thead>
<tr>
<th>Factor</th>
<th>Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>Human-related factors</td>
<td>5.64</td>
</tr>
<tr>
<td>Virus/malware/disruptive software</td>
<td>4.66</td>
</tr>
<tr>
<td>Infiltration/intrusive attacks</td>
<td>4.56</td>
</tr>
<tr>
<td>Lack of planning, policies and procedures</td>
<td>4.51</td>
</tr>
<tr>
<td>Functionality of devices</td>
<td>4.36</td>
</tr>
<tr>
<td>Loss of integrity of information</td>
<td>4.32</td>
</tr>
</tbody>
</table>

Table One. Factors Posing a Threat to Health Data

Respondents working for hospitals were more likely to indicate that human-related factors were of concern compared to respondents working for physician practices (83 percent compared to 61 percent)³.

Human-Related Factors

The 80 percent of respondents identifying human-related factors as a key area of concern⁴ were asked to elaborate on the specific areas that were of concern. More specifically, 86 percent of these respondents reported that negligence or unintentional mistakes that expose information, such as the disclosure of information on websites or lost/misplaced files or devices was of greatest concern. Two-thirds of respondents (68 percent) also indicated that they were concerned that workforce members would bypass security access controls or interfere with access controls. More than half of respondents (58 percent) indicated concerns about insider threats, which include deliberate and authorized activity by workforce members. Respondents were least likely to report having concerns that outsourced staff would bypass security controls (20 percent).

---

³ Percent represents those respondents that identified this as a 5, 6 or 7.
⁴ Respondents got this question if they identified human-related factors as a concern as a 5, 6 or 7.
Viruses, Malware and Disruptive Software

Slightly more than half of respondents (56 percent) indicated a high degree of concern about viruses, malware and other disruptive software. Among these respondents, three-quarters noted that their concerns were specifically regarding viruses, malware and spyware. Another 70 percent indicated concerns in this area related to personal health information (PHI) and data that was exposed through software applications.

Infiltration/Intrusive Attacks

Approximately half of respondents (52 percent) indicated that they had a high degree of concern with regard to infiltration and intrusive attacks, such as hacking to obtain credentials or other sensitive information. Among these respondents, concern was greatest that their organization would be exposed to phishing attacks, where an individual would pose as an otherwise reputable organization to gain access to personal information. This was identified by 68 percent of respondents. At least half of these respondents also raised concerns about hacking (56 percent) and elicitation or social engineering of information (56 percent). Respondents were least likely to raise concerns that their organizations’ websites and/or domain name would be compromised or hijacked (19 percent).

Functionality of Devices

Approximately half of respondents (51 percent) noted that functionality of devices was of concern with regard to security at their organization. Among these respondents, approximately three-quarters (77 percent) noted that operational errors or failure of systems, devices and software was of concern. Another two-thirds (66 percent) noted that software vulnerabilities or errors, including both applications and embedded software, were of concern at their organizations.

Threat Motivators

In addition to being asked which areas they were most concerned about with regard to security, respondents were also asked to identify the threat motivators and influencers that motivate a perpetrator’s attack. Respondents were most likely (80 percent) to identify work force members snooping on information of others, such as a spouse, co-worker, neighbor or friend as a threat motivator. Two-thirds also identified financial identity theft as a threat motivator, while half (51 percent) indicated that medical identity theft was a threat motivator. A full list of threat motivators is provided in the chart below.
4. Proactive Measures for Evaluating Risk to Patient Data

Nearly all respondents (92 percent) reported that their organization conducts a formal risk analysis. Additionally, three-quarters (74 percent) of these individuals reported that their organization conducts a risk analysis annually. Furthermore, most respondents reported using the data uncovered in the risk analysis to correct deficiencies in controls and/or policies and procedures.

More than three-quarters of respondents (84 percent) reported that their organization conducted an audit of their IT security plan, while more than half (54 percent) reported that their organization tested their data breach response plan.

Risk Analysis

Nearly all respondents (92 percent) noted that their organization conducts a formal risk analysis to evaluate risks to patient data at their organization. Four percent of respondents were unsure if their organization conducted a risk analysis. This is a substantial increase from the 77 percent of respondents that reported their organization conducted a risk analysis in 2012.

Much of this increase can be explained by the type of individuals responding to the 2013 study, as the large majority of this year’s responses come from hospital-based individuals, who tend to be more likely to report that their organization conducted a risk analysis. Indeed, 95 percent of respondents working for a hospital reported that their organization conducted a risk analysis, compared to only 78 percent of respondents working for a physician practice. Significantly, while the number of respondents working for a hospital that conducted a risk analysis remained relatively consistent, the number of respondents working for physician practices that reported their organization conducted a risk analysis increased from 65 percent in 2012.
Among the respondents that reported that they conducted a risk analysis, three-quarters (74 percent) indicated that their organization conducts a formal risk analysis annually; up from approximately two-thirds a year ago. Another five percent reported conducting a risk analysis once every six months and 22 percent conduct this type of analysis every two years. See Figure Four.

**Figure Four. Frequency of Conducting a Formal Risk Analysis**

Furthermore, those working for a hospital were more likely to report conducting a risk analysis on at least an annual basis (73 percent), compared to 63 percent of physician practices.

As defined by HIPAA and for the purposes of this survey, security controls are safeguards or countermeasures used to avoid, counteract or minimize security risks. Most commonly, they are categorized as:

- Physical controls (such as fences, doors, locks, fire extinguishers);
- Administrative controls (such as incident response processes, management oversight and security awareness/training); and
- Technical controls (such as user authentication and access controls, antivirus software and/or firewalls).

Those respondents working for a hospital that conducted a risk analysis were asked how this information informs their security controls in three key areas:

- Determine which security controls to put into place – 93 percent;
- Identify area where lack of security controls pose a risk – 71 percent; and
- Identify area where lack of security policies/procedures pose a risk – 68 percent.

This data is consistent with the data reported in 2012.

Respondents indicating their risk analysis identified areas in which a lack of security controls posed a risk were asked to identify how long it took their organization to correct these deficiencies. One-third (34 percent) of these respondents noted that their organization corrected the identified issues within six months. Another 42 percent noted that they resolved the deficiency within six months to one year and 18 percent indicated that it took their organization more than a year to respond to the identified risk. Only
four percent of respondents noted that they did not rectify the issues uncovered by the risk analysis. In the 2012 study, 46 percent of respondents resolved risks associated with a lack of security controls in six months. This question was not asked of those working for physician practices.

Individuals who indicated that their organization’s risk analysis uncovered risks resulting from a lack of security policies and/or procedures were also asked to identify how long it took their organizations to resolve these issues. Nearly half of respondents (48 percent) noted that their organization resolved the issues within six months and another 35 percent rectified the issue within six months to one year. Three percent of respondents noted that the issue still has not been resolved. This is consistent with the data reported in 2012. This question was not asked of those working for physician practices.

Data Breach Response Plan

In addition to information about risk analyses, respondents were asked to identify whether or not their organization had tested their data breach response plan. Slightly more than half of respondents (54 percent) reported this to be the case, although 16 percent of respondents were unsure of their processes, so this number could, in fact, be slightly higher.

Among respondents who do test their data breach response plan, slightly less than two-thirds (63 percent) reported conducting the test on an annual basis. Another quarter conducted a test of their plan every two years (23 percent). The remaining respondents 14 percent of respondents conducted a test every six months.

By organization type, individuals working for a hospital were more likely to report testing their data breach response plan (57 percent) than were respondents working for a physician practice (39 percent). These numbers are consistent with those reported in 2012.

Audit of IT Security Plan

Finally, respondents were asked to identify if their organization conducted an audit of its IT security plan. The vast majority of respondents (84 percent) reported that this type of analysis was conducted at their organization. This is an increase from the two-thirds of respondents who reported conducting a test in 2012. However, much of this increase can be explained as a result of the large number of hospital respondents in the study this year, as those working for a hospital were more likely to report conducting an audit (89 percent) than were those working for a physician practice (65 percent).

Three-quarters of respondents reported that this type of analysis was conducted on an annual basis (75 percent). Ten percent reported conducting the analysis every six months while 16 percent audited their IT security plan every two years.

Maturity of Security Environment

Respondents were also asked to indicate the maturity of their organizations’ security environment, using a one to seven scale, where one is not at all mature and seven is very mature. Respondents recorded an average score of 4.35, a slight decrease from the 4.64 reported one year ago. This question was not asked of those working for a physician practice.
Only three percent of respondents identified their organization as very mature, as indicated with a score of seven. The same percent indicated that their organization was not at all mature, as indicated with a score of one. Respondents were most likely to give their organization a score of five on this rating scale (34 percent). Individuals working for a physician practice were not asked this question.

5. Employee/Patient Data Access

Healthcare organizations continue to deploy technologies to ensure that patient information is available only to authorized employees. Role-based and user-based controls continue to be most widely used.

A vast majority of respondents (89 percent) reported that their organization provides access to electronic patient information to patients, surrogates and designated others.

Organizational Control for Patient Access to Data

A key aspect of securing data at healthcare organizations is to provide clinicians and employees access to data on a “need to know” basis. This study specifically asks respondents to identify use of five specific means of controlling access to patient information.

The types of access tested for in this study include:

- Group-based, where all members of a particular group have access (i.e. all clinicians in a specific practice specialty)
- Location-based, where all employees working in the same location have access (i.e. all clinicians working in a specific unit)
- Role-based, where all individuals in a certain role have access to information (i.e. physicians)
- Rule-based, where access is based on an if/then statement
- User-based, where access is specific to a particular employee

Nearly two-thirds of respondents (63 percent) reported using two or more means of controlling employee access to patient information. This is an increase from last year, when 43 percent of respondents reported this to be the case.

Respondents working at a hospital were more likely to report using multiple methods for securing patient information than were respondents working for physician practices. Nearly two-thirds of respondents working for hospitals use multiple means of controlling access to patient information (67 percent), compared to 44 percent of respondents working for a hospital organization. Additionally, 20 percent of respondents working for a hospital reported using four or five methods for controlling employee access, compared to nine percent of respondents working for a physician practice.

In previous HIMSS Security Surveys, respondents have always indicated their organizations were most likely to use user-based controls to control access to patient information. While this type of control is used by 71 percent of respondents, for the first time, it was eclipsed by the number of respondents indicating their organization relied on role-based controls (78 percent).
The frequency with which all types of controls were selected is listed in the table below.

<table>
<thead>
<tr>
<th>Mechanism</th>
<th>Count</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role-based</td>
<td>220</td>
<td>77.70%</td>
</tr>
<tr>
<td>User-based</td>
<td>200</td>
<td>70.70%</td>
</tr>
<tr>
<td>Group-based</td>
<td>91</td>
<td>32.20%</td>
</tr>
<tr>
<td>Location-based</td>
<td>66</td>
<td>23.30%</td>
</tr>
<tr>
<td>Rule-based</td>
<td>43</td>
<td>15.20%</td>
</tr>
<tr>
<td>Other</td>
<td>2</td>
<td>0.07%</td>
</tr>
<tr>
<td>Don't Know</td>
<td>2</td>
<td>0.07%</td>
</tr>
</tbody>
</table>

Table Two. Types of Controls Used to Secure Electronic Information

Availability of Electronic Data to Patients

Respondents were also asked to identify if their organizations provide electronically stored patient information to their patients/surrogates and designated others. A vast majority of respondents (89 percent) reported that their organization provides access to electronic patient information to patients, surrogates and designated others. This represents an increase from approximately three-quarters in the 2012 study. Those working for a hospital were more likely to report offering access to electronic patient information than were those working at physician practices (93 percent compared to 74 percent). In general, respondents to this year’s survey were more likely to report the ability to share electronic information than were respondents to the 2012 study.

The most frequently identified means for sharing patient information is via CD/DVD. Three-quarters of respondents who reported sharing information electronically indicated that they used a CD/DVD to facilitate data sharing. This was also the most frequently identified means of data sharing in the 2012 study. Rounding out the top three most frequently used means of sharing data were encrypted e-mail (45 percent) and a website (43 percent). The other choices offered in this study, as well as the percent of respondents that selected the choice, are shown below.

<table>
<thead>
<tr>
<th>Mechanism</th>
<th>Count</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>CD/DVD</td>
<td>188</td>
<td>74.60%</td>
</tr>
<tr>
<td>Secure (Encrypted) E-Mail</td>
<td>114</td>
<td>45.24%</td>
</tr>
<tr>
<td>Health Website/Web Portal</td>
<td>108</td>
<td>42.86%</td>
</tr>
<tr>
<td>USB Thumb Drive</td>
<td>84</td>
<td>33.33%</td>
</tr>
<tr>
<td>Personal Health Record (PHR)</td>
<td>43</td>
<td>17.06%</td>
</tr>
<tr>
<td>PHR Hosted by Third Party</td>
<td>32</td>
<td>12.70%</td>
</tr>
<tr>
<td>Other</td>
<td>12</td>
<td>4.76%</td>
</tr>
<tr>
<td>Unencrypted E-Mail</td>
<td>2</td>
<td>0.79%</td>
</tr>
</tbody>
</table>

Table Three. Mechanisms Used to Share Electronic Patient Information

Respondents who indicated that their organization provides patients/surrogates with access to electronic patient information through a health website/web portal were asked to identify how their organization controls access to the data made available through these portals. All but one of the respondents to this year’s study indicated that data was

---

5 For the purposes of this study, a surrogate is defined as a person who has power of attorney to act on behalf of the patient. A designated other is a person whom the patient has indicated can view or be sent a copy of their records.
protected using at least one security control. This is similar to the information provided in the 2012 study.

The most frequent means of controlling access to patient data through a website/web portal is via a unique log-in or password; this option was identified by 98 percent of survey respondents. This is consistent with the data reported in 2012. Hard tokens, such as a driver’s license or other type of access card and biometric devices were each in use at two percent of respondents’ organizations.

6. Access Tracking/Audit Logs

More than 90 percent of respondents working for hospital organizations reported that their organization collects and analyzes audit log information from at least one system in their organization. Firewalls are the most common source of audit log data.

The majority of respondents (93 percent) reported that they collect and analyze information from either security or access logs; this represents a slight increase from the 91 percent of respondents that reported this to be the case in 2012. Only one percent of respondents reported that this type of data was not collected and/or analyzed. The remaining respondents either did not know their organizations strategy in this area or did not answer the question. This question was not asked of respondents working for physician practices.

Among those indicating their organizations collect information from audit logs, the majority (84 percent) reported that their organization collects and analyzes information from their organization’s firewall log. Three-quarters of respondents also reported that they collect and analyze data from their organization’s applications (75 percent) and servers (74 percent). These numbers are higher than reported in 2012. Respondents were least likely to report their organization collected information from their additional storage devices (nine percent); this is consistent with what was reported in 2012. Respondents working for physician practices were not asked this question.

A full list of systems from which respondents collect and analyze data is included in the figure below.
All respondents were also asked to identify the types of events their audit log captures. Respondents were most likely to indicate that they audit clinician access to data (69 percent), followed by non-clinician access to data (62 percent) and security critical events (61 percent). Twenty percent of respondents indicated that their organization captures information regarding patient access to data (20 percent). Because of a different question structure from 2013, a direct comparison to 2012 data cannot be made.

Finally, respondents were asked to identify how they actively utilize audit log data. More than 90 percent of respondents reported that they actively use their audit log data for at least one of the functions listed as options in this study. Respondents indicating they actively used audit log data were asked to identify how this data was being used.

- Policy compliance monitoring – 92 percent;
- System activity monitoring – 83 percent;
- Intrusion detection – 80 percent; and
- Provide “Accounting of Disclosure” – 27 percent.

With the exception of Accounting of Disclosure to patients, these numbers all represent an increase from that reported in 2012. Those using an Accounting of Disclosures to patients declined from the 47 percent that reported this to be the case in 2012. Respondents working for physician practices were not asked this question.

7. Use and Measurement of Security Controls

Hospital organizations are continuing to use reduced risk exposure and the number of security incidents as a means to determine the effectiveness of their security controls. Return on investment is used much less frequently as a metric.

Earlier in this paper it was noted that the majority of respondents working for a hospital (93 percent) used the information generated in their risk analysis to determine which security controls to put in place at their organizations.

Hospital respondents were asked to identify three areas/tools that they might use to measure the success of their organization’s security controls. These were number of detected security incidents, reduced risk exposure and return on investment (ROI). Slightly more than half (53 percent) of respondents reported using at least one of these tools to measure the success of the security controls at their organization. However, one-quarter of respondents did not answer this question or reported that they did not know if their organization measured the success of security controls.

Among the respondents that do measure the success of their organizations’ security controls, nearly three-quarters indicated they used the reduced risk of exposure as a success measure. Additionally, more than two-thirds (70 percent) indicated that their organization uses number of detected incidents to measure success. Ten percent of respondents use return on investment (ROI) to measure the success of security controls.
in place at their organization. Respondents working for a physician practice were not asked this question.

8. Security in a Networked Environment

More than three-quarters of respondents reported having data sharing arrangements with other healthcare organizations; respondents working for hospitals were more likely to report sharing information with other organizations than were respondents working for a physician practice.

More than 80 percent of respondents reported having a Business Associate Agreement in place with at least 75 percent of their business associates.

Respondents were asked to identify the types of organizations with which they share patient data in electronic format. The majority of respondents (88 percent) indicated that their organization currently shares information with at least one other type of organization. Those working for hospitals (93 percent) were more likely than their counterparts at physician practices (67 percent) to report sharing data with other organizations.

A full list of the organizations that the respondents in this sample share data with is listed in the table below. See Table Four.

<table>
<thead>
<tr>
<th>Type of Data Sharing Arrangement – Current</th>
<th>Percent Current</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other facilities within corporate organization</td>
<td>71.00%</td>
</tr>
<tr>
<td>State government entities</td>
<td>60.10%</td>
</tr>
<tr>
<td>Other facilities within local region</td>
<td>57.20%</td>
</tr>
<tr>
<td>Public health entities</td>
<td>55.50%</td>
</tr>
<tr>
<td>Third party service providers</td>
<td>54.80%</td>
</tr>
<tr>
<td>Health Information Exchange Organization (HIOs)</td>
<td>32.50%</td>
</tr>
<tr>
<td>Other facilities outside of local region/state</td>
<td>29.30%</td>
</tr>
<tr>
<td>Federal government entities</td>
<td>29.00%</td>
</tr>
<tr>
<td>Local government entities</td>
<td>27.60%</td>
</tr>
<tr>
<td>Personal Health Record vendor</td>
<td>17.00%</td>
</tr>
<tr>
<td>eHealth Exchange</td>
<td>7.40%</td>
</tr>
<tr>
<td>Facilitated data exchange</td>
<td>6.00%</td>
</tr>
</tbody>
</table>

Table Four. Type of Data Sharing Arrangement – Current

In all instances, respondents working for hospitals were more likely to report participating in a data sharing arrangement than were respondents working for physician practices. Those relationships that are statistically significant are noted with an asterisk (“*”).
### Current Exchange Entity

<table>
<thead>
<tr>
<th>Current Exchange Entity</th>
<th>Hospitals</th>
<th>Physicians Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other facilities within corporate organization *</td>
<td>76.30%</td>
<td>43.50%</td>
</tr>
<tr>
<td>State government entities *</td>
<td>65.40%</td>
<td>32.60%</td>
</tr>
<tr>
<td>Other facilities within local region*</td>
<td>61.00%</td>
<td>37.00%</td>
</tr>
<tr>
<td>Public health entities*</td>
<td>61.00%</td>
<td>23.90%</td>
</tr>
<tr>
<td>Third party service providers*</td>
<td>57.90%</td>
<td>37.00%</td>
</tr>
<tr>
<td>Health information exchange organizations*</td>
<td>37.30%</td>
<td>10.90%</td>
</tr>
<tr>
<td>Other facilities outside of local region/state</td>
<td>31.60%</td>
<td>17.40%</td>
</tr>
<tr>
<td>Local government entities*</td>
<td>31.60%</td>
<td>10.90%</td>
</tr>
<tr>
<td>Federal government entities*</td>
<td>30.70%</td>
<td>13.00%</td>
</tr>
<tr>
<td>Personal health record vendors</td>
<td>18.00%</td>
<td>13.00%</td>
</tr>
<tr>
<td>eHealth Exchange</td>
<td>8.30%</td>
<td>2.20%</td>
</tr>
<tr>
<td>Facilitated data exchange</td>
<td>6.60%</td>
<td>4.30%</td>
</tr>
</tbody>
</table>

Table Five. Type of Data Sharing Arrangement – Current, by Type of Organization

With regard to future data sharing arrangements, respondents were most likely to report that their organizations would share information as part of an HIE in the future. See Table Five below for complete information on plans for future data sharing arrangements.

### Type of Data Sharing Arrangement – Future

<table>
<thead>
<tr>
<th>Type of Data Sharing Arrangement – Future</th>
<th>Percent Future</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health Information Exchange Organizations (HIOs)</td>
<td>44.20%</td>
</tr>
<tr>
<td>eHealth Exchange</td>
<td>41.00%</td>
</tr>
<tr>
<td>Other facilities outside of local region/state</td>
<td>38.20%</td>
</tr>
<tr>
<td>Other facilities within local region</td>
<td>36.40%</td>
</tr>
<tr>
<td>Personal Health Record Vendor</td>
<td>31.10%</td>
</tr>
<tr>
<td>Facilitated data exchange</td>
<td>28.60%</td>
</tr>
<tr>
<td>Public health entities</td>
<td>27.90%</td>
</tr>
<tr>
<td>State government entities</td>
<td>23.70%</td>
</tr>
<tr>
<td>Federal government entities</td>
<td>22.60%</td>
</tr>
<tr>
<td>Local government entities</td>
<td>22.30%</td>
</tr>
<tr>
<td>Other facilities within corporate organization</td>
<td>20.10%</td>
</tr>
<tr>
<td>Third party service providers</td>
<td>18.00%</td>
</tr>
</tbody>
</table>

Table Six. Type of Data Sharing Arrangement – Future

Only four percent of respondents reported that they had no plans to share data at this time or in the future with any of the organizations listed in the tables above.

Respondents were also asked to identify the percent of their business associates with whom they have a formal Business Associate Agreement (BAA), as required by HIPAA. Nearly half of respondents (43 percent) reported that they have formal BAAs with all of their business associates. Another quarter (40 percent) indicated that they a formal BAA with 75 to 99 percent of their business associates. None of respondents noted that they did not have a formal BAA with any of their business associates.
9. Use of Security Technologies

Respondents continue to report using multiple technologies to secure information at their organization. Firewalls and user access controls continue to be the most frequently used types of security technology in use by healthcare organizations. Use of biometric technologies continues to be limited among the surveyed organizations. Encryption technologies are most widely used on laptop computers and for e-mail.

Respondents were asked to identify the types of technical security tools that are in place today at their organization. On average, respondents have eleven of the technologies identified in this research in place. Almost all of the respondents in this study (99 percent) reported having at least one of the security tools tested for in place at their organization; the remaining respondents either did not know the types of technologies used or did not respond.

Firewalls were identified most frequently as a security tool in place at healthcare organizations; they are used at 98 percent of respondents’ organizations. User access controls (95 percent) and remote access controls to EHR data for clinicians/employees (90 percent) were each used by at least 90 percent of respondents. Also used by 95 percent of respondents were user access controls. Use of all technology types in this survey is listed in the table below:

<table>
<thead>
<tr>
<th>Security Technologies</th>
<th>Percent Current</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewalls</td>
<td>97.50%</td>
</tr>
<tr>
<td>User Access Controls</td>
<td>95.10%</td>
</tr>
<tr>
<td>Remote Access Controls to EHR Data for Clinicians/Employees</td>
<td>90.10%</td>
</tr>
<tr>
<td>Audit Logs of Each Access to Patient Health Records</td>
<td>89.80%</td>
</tr>
<tr>
<td>Wireless Security Protocols</td>
<td>84.50%</td>
</tr>
<tr>
<td>Disaster Recovery</td>
<td>78.80%</td>
</tr>
<tr>
<td>Data Encryption (Data in Transmission)</td>
<td>75.60%</td>
</tr>
<tr>
<td>Electronic Signature</td>
<td>73.90%</td>
</tr>
<tr>
<td>Off-site Storage</td>
<td>72.80%</td>
</tr>
<tr>
<td>Data Encryption (Data in Storage)</td>
<td>68.20%</td>
</tr>
<tr>
<td>Access Control Lists</td>
<td>70.30%</td>
</tr>
<tr>
<td>Intrusion Prevention/Detection Services</td>
<td>62.20%</td>
</tr>
<tr>
<td>Single Sign-On</td>
<td>45.90%</td>
</tr>
<tr>
<td>Data Loss Prevention</td>
<td>43.50%</td>
</tr>
<tr>
<td>Two-Factor Authentication</td>
<td>39.60%</td>
</tr>
<tr>
<td>Log Aggregation Tool</td>
<td>22.60%</td>
</tr>
<tr>
<td>Public Key Infrastructure</td>
<td>20.50%</td>
</tr>
<tr>
<td>Biometric Technologies</td>
<td>14.10%</td>
</tr>
</tbody>
</table>

Table Seven. Security Technologies in Use Today

There are also differences in the types of technologies used by organization type. These differences are highlighted in the table below (the cells highlighted in blue represent the higher percentage). In the instance where the differences in use are statistically significant, that data has been marked with an asterisk (“*”).
### Table Eight. Security Technologies in Use Today, by Type of Organization.

<table>
<thead>
<tr>
<th>Security Technologies</th>
<th>Hospitals</th>
<th>Physician practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewalls</td>
<td>97.40%</td>
<td>97.80%</td>
</tr>
<tr>
<td>User Access Controls</td>
<td>95.20%</td>
<td>93.50%</td>
</tr>
<tr>
<td>Remote Access to EHR Data for Clinicians/Employees</td>
<td>90.80%</td>
<td>84.80%</td>
</tr>
<tr>
<td>Audit Logs of Each Access to Patient Health Records</td>
<td>89.90%</td>
<td>87.00%</td>
</tr>
<tr>
<td>Wireless Security Protocols*</td>
<td>89.00%</td>
<td>60.90%</td>
</tr>
<tr>
<td>Disaster Recovery</td>
<td>80.70%</td>
<td>69.60%</td>
</tr>
<tr>
<td>Data Encryption (Data in Transmission)*</td>
<td>78.50%</td>
<td>56.50%</td>
</tr>
<tr>
<td>Electronic Signature*</td>
<td>76.80%</td>
<td>60.90%</td>
</tr>
<tr>
<td>Off-site Storage</td>
<td>71.50%</td>
<td>78.30%</td>
</tr>
<tr>
<td>Data Encryption (Data in Storage)</td>
<td>69.70%</td>
<td>54.30%</td>
</tr>
<tr>
<td>Access Control Lists*</td>
<td>74.60%</td>
<td>47.80%</td>
</tr>
<tr>
<td>Intrusion Prevention/Detection Services*</td>
<td>66.70%</td>
<td>41.30%</td>
</tr>
<tr>
<td>Single Sign-On*</td>
<td>50.40%</td>
<td>26.10%</td>
</tr>
<tr>
<td>Data Loss Prevention Tools</td>
<td>43.40%</td>
<td>41.30%</td>
</tr>
<tr>
<td>Two-Factor Authentication</td>
<td>42.10%</td>
<td>26.10%</td>
</tr>
<tr>
<td>Log Aggregation Tool*</td>
<td>24.60%</td>
<td>6.50%</td>
</tr>
<tr>
<td>Public Key Infrastructure*</td>
<td>24.60%</td>
<td>2.20%</td>
</tr>
<tr>
<td>Biometric Technologies*</td>
<td>17.10%</td>
<td>0.00%</td>
</tr>
</tbody>
</table>

In addition to the technologies being used currently, respondents were also asked to identify which technologies they plan to add to their environment in the future. By number of facilities, respondents were most likely to report plans to purchase single sign on and log aggregation tools. At least 20 percent of the overall sample expressed plans to purchase this technology.

Another way to evaluate this data is to examine the number of facilities planning to purchase these security tools for the first time. At least 40 percent of the facilities not presently using a tool, plan to make a purchase of one or more of the below technologies in the future.

- Disaster recovery (51.7 percent);
- Data encryption – transmission (49.3 percent);
- Single sign-on (41.80 percent).

Respondents were also asked to provide detailed information on the devices on which data encryption was employed at their organization. On average, respondents indicated that their organization encrypts data in 3.93 of the areas tracked in this research; this is a slight increase from the 3.68 reported in the 2012 study. Two percent indicated that they encrypt data in all areas included in this study and all respondents encrypt data in at least one of the areas tested in this study. Five percent reported that they did not know the status of encryption at their organization.
Respondents were most likely to report that they encrypted information stored on laptop computers (80 percent). Two-thirds of respondents also reported that their organization encrypted e-mail. Respondents were least likely to report encrypting data that was associated with their mobile medical devices, such as a wireless-enabled monitoring device. Only 17 percent of respondents indicated that data on these devices was encrypted.

There are number of differences in the way in which these encryption technologies are deployed at hospitals and at physician practices. The table below highlights these differences. Those that are statistically significant are noted with an *.

<table>
<thead>
<tr>
<th>Use of Encryption by Device Type</th>
<th>Percent All Facilities</th>
<th>Percent Hospitals</th>
<th>Percent Physician Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Laptop Computers*</td>
<td>79.51%</td>
<td>85.10%</td>
<td>47.80%</td>
</tr>
<tr>
<td>E-Mail*</td>
<td>69.96%</td>
<td>75.40%</td>
<td>41.30%</td>
</tr>
<tr>
<td>Mobile Devices*</td>
<td>57.24%</td>
<td>60.10%</td>
<td>39.10%</td>
</tr>
<tr>
<td>On-Site Back Up Tapes</td>
<td>50.53%</td>
<td>50.90%</td>
<td>45.70%</td>
</tr>
<tr>
<td>Servers</td>
<td>37.46%</td>
<td>34.60%</td>
<td>50.00%</td>
</tr>
<tr>
<td>Desktop Computers*</td>
<td>34.63%</td>
<td>35.10%</td>
<td>26.10%</td>
</tr>
<tr>
<td>Cloud Computing*</td>
<td>27.21%</td>
<td>24.60%</td>
<td>32.60%</td>
</tr>
<tr>
<td>Mobile Medical Devices</td>
<td>16.61%</td>
<td>16.20%</td>
<td>17.40%</td>
</tr>
</tbody>
</table>

Table Nine. Use of Encryption by Facility Type

10. Security Breaches and Medical Identity Theft

More than two-thirds of respondents reported that their organization has formal policies/procedures in place related to addressing a security breach; most of the remaining respondents are moving forward to develop policies/procedures in this area.

One-quarter of respondents reported having either a case of medical identity theft or a security breach in the past year.

Respondents were asked to identify whether or not their organization has policies and/or procedures in place to respond to threats to data security and/or incidents related to a security breach. Slightly more than two-thirds (69 percent) indicated they did have such a security policy in place. This is an increase from the 62 percent of organizations that reported that their organization has formal security policies and/or procedures in place in 2012. Another quarter (27 percent) reported that they are presently developing a security policy. Less than one percent reported that they had no security policy in place and did not intend to develop a security policy in the future. There is no statistically significant difference in adoption of a policy between hospitals and physician practices.

In this survey, medical identity theft was defined as “the use of an individual’s identity specific information such as name, date of birth, social security number, insurance information, etc. without the individual’s knowledge or consent to obtain medical services or goods. It may also extend to cases where an individual’s beneficiary information is used to submit false claims in such a manner that an individual’s medical record or insurance is corrupted, potentially impacting patient care.”
Twelve (12) percent of respondents reported that their organization has had at least one known case of medical identity theft reported in the previous 12 months. This is consistent to the 11 percent of respondents that reported this to be the case in 2012. Slightly more than one-quarter of respondents (26 percent) indicated that they had experienced a single incident in the past year. The average number of cases of medical identity theft was 2.89.

Those working for a hospital organization were more likely to report a case of medical identity theft (15 percent) when compared to those respondents working for a physician practice (four percent).

Respondents were also asked to indicate if they had a security breach in the past year. Nineteen (19) percent of respondents reported that they had a security breach during that time frame. While respondents working for hospitals were more likely to report a security breach than their counterparts at a medical facility, this difference was not statistically significant.

In addition to whether or not an organization had experienced a security breach, respondents were also asked to identify how many patients were impacted by the breach. Most of the respondents (87 percent) indicated that their breach impacted 499 patients or fewer. Nineteen (19) percent of respondents also indicated that their organization experienced a security breach that impacted 500 or more patients. Three respondents reported experiencing briefs of both sizes.

Respondents experiencing a security breach were also asked to identify the steps they took regarding breach notification. Approximately three-quarters (79 percent) reported that they notified impacted patients of the breach. A smaller percentage (47 percent) reported that they notified the government of the breach. Half of the respondents with a breach that impacted more than 500 patients also reported the breach to the local media.

Only eight percent of respondents indicated that the security breach was the result of actions taken by a business associate.

11. Conclusion

This year’s HIMSS Security Survey brought focus to Survey respondent’s concerns that electronic patient data at their organization will be breached by either existing staff or by individuals who are brought in to work on behalf of the healthcare organization. As such, healthcare organizations have continued to augment their security environment with new technologies that will ensure that employees have access only to the data that is necessary to successfully perform their jobs.

The majority of respondents were proactively managing their information security environment. Most respondents have a security policy in place and those that have not implemented a policy at this time expect to do so in the future. Many are using a wide variety of technologies to secure data. Additionally, respondents are conducting routine testing, such as risk analyses and IT security plan audits, to ensure that the security technologies that are in place are working as expected.

This proactive stance puts healthcare organizations in a position of being able to identify and manage deficiencies in their security environment. Indeed, respondents who conduct risk analyses indicated that they were able to correct problems with organizational security policy and security controls in place.
Despite the advances healthcare organizations have made in their security environment, there is still room for improvement. Healthcare executives continue to identify their security environment as an average level of maturity, and while they are using an impressive array of security technologies, there are a number of solutions, such as biometric technologies, that are used by less than half of respondents. Additionally, only half of respondents reported having a full-time staff member to oversee information security initiatives, and investment in security continues to remain relatively low at many healthcare organizations.

12. About HIMSS

HIMSS is a global, cause-based, not-for-profit organization focused on better health through information technology (IT). HIMSS leads efforts to optimize health engagements and care outcomes using information technology. HIMSS is a part of HIMSS WorldWide, a cause-based, global enterprise producing health IT thought leadership, education, events, market research and media services around the world. Founded in 1961, HIMSS WorldWide encompasses more than 52,000 individuals, of which more than two-thirds work in healthcare provider, governmental and not-for-profit organizations across the globe, plus over 600 corporations and 250 not-for-profit partner organizations, that share this cause. HIMSS WorldWide, headquartered in Chicago, serves the global health IT community with additional offices in the United States, Europe, and Asia. To learn more about HIMSS and to find out how to join us and our members in advancing our cause, please visit our website at www.himss.org.

13. About Experian® Data Breach Resolution

Experian Data Breach Resolution, powered by the nation’s largest credit bureau, is a leader in helping businesses plan for and mitigate consumer risk following data breach incidents. With more than a decade of experience, Experian Data Breach Resolution has successfully serviced some of the largest and highest-profile breaches in history. The Group offers swift and effective incident management, notification, call center support and reporting services while serving millions of affected consumers with proven credit and identity protection products. In 2013, Experian Data Breach Resolution received the “Customer Service Team of the Year” award from the American Business Awards. Experian Data Breach Resolution is active with the International Association of Privacy Professionals, Health Care Compliance Association, Ponemon Institute RIM Council, InfraGuard and is a founding member of the Medical Identity Fraud Alliance. For more information, visit www.experian.com/databreach and follow us on Twitter @Experian_DBR.

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 6th Annual HIMSS Security Survey, sponsored by Experian® Data Breach Resolution.
15. For More Information, Contact:

Joyce Lofstrom  
Senior Manager, Corporate Communications  
HIMSS  
33 West Monroe  
Suite 1700  
Chicago, IL  60603  
312-915-9237  
jlofstrom@himss.org
Hospital Participant Profile – Title

- Chief Information Officer: 48%
- IT Director: 12%
- VP of Information Technology: 11%
- Chief Security Officer: 10%
- Practice Administrator: 1%
- Chief Privacy Officer: 1%
- Compliance Officer: 0%
- Other: 15%

N = 223

Participant Profile – Type of Medical Practice

- Independent Medical Practice: 89%
- Freestanding Ambulatory Surgery Center: 2%
- Federally Qualified Health Center: 1%
- Retail Walk-in Primary Care Clinic: 0%
- Medical Practice Owned by Delivery System: 0%
- Management Services Organization: 0%
- Independent Practice Association: 0%

N = 48
Participant Profile – Region

<table>
<thead>
<tr>
<th>Region</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>East North Central</td>
<td>16%</td>
</tr>
<tr>
<td>West North Central</td>
<td>16%</td>
</tr>
<tr>
<td>Mid Atlantic</td>
<td>12%</td>
</tr>
<tr>
<td>Mountain</td>
<td>12%</td>
</tr>
<tr>
<td>South Atlantic</td>
<td>11%</td>
</tr>
<tr>
<td>West South Central</td>
<td>11%</td>
</tr>
<tr>
<td>Pacific</td>
<td>8%</td>
</tr>
<tr>
<td>New England</td>
<td>5%</td>
</tr>
<tr>
<td>East South Central</td>
<td>5%</td>
</tr>
</tbody>
</table>

Greatest Issues Concerning Security Threats

- Human Related Factors: 5.64
- Virus/Malware/Disruptive Software: 4.65
- Infiltration/Intrusive Attacks: 4.56
- Lack of Planning, Policy, Procedures: 4.51
- Functionality of Devices: 4.38
- Loss of Integrity of Information: 4.32

© 2014 Healthcare Information and Management Systems Society
**Human Factor Concerns**

- Negligence/Unintentional Mistakes: 66%
- Staff Bypassing Security Access Controls: 68%
- Insider Threats: 58%
- External Threats: 39%
- Outsourcing Bypassing Security Controls: 20%
- Other: 0%
- Don't Know: 0%

N = 225

---

**Infiltration/Intrusive Attack Concerns**

- Phishing: 68%
- Hacking: 56%
- Elicitation of Information: 50%
- Eavesdropping: 38%
- Website/Domain Name Hijacking: 19%
- Other: 1%
- Don't Know: 1%

N = 148
### Percent of IT Budget Dedicated to Information Security

- Less than One Percent: 10%
- One to Three Percent: 30%
- Four to Six Percent: 10%
- Seven to 12 Percent: 9%
- More than 12 Percent: 4%
- Don't Know: 18%

**N = 200**

### Change in Percent of IT Budget Dedicated to Information Security

- Increase: 61%
- No Change: 39%
- Decrease: 4%
- Don't Know: 6%

**N = 200**
Impact of Federal Initiatives on Security Budget

- Increase in Budget: 51%
- No Impact: 27%
- Decrease in Budget: 18%
- Don’t Know: 6%

Percent of IT Budget Dedicated to Breach Remediation Efforts

- Less than One Percent: 54%
- One to Three Percent: 18%
- Four to Six Percent: 6%
- Seven to 12 Percent: 2%
- Don’t Know: 21%
Personnel Responsible for Securing Environment

- Part-Time Staff: 40%
- Other Full Time Staff (Not CSO): 37%
- Chief Security Officer (CSO): 15%
- No One Assigned to This: 6%
- Don't Know: 1%
- Handled Externally: 1%

N = 227

Frequency of Conducting a Risk Analysis

- Every Six Months: 5%
- Annually: 74%
- Every Two Years: 22%

N = 281
Uses of Risk Analysis Data

- Determine Which Security Controls to Put in Place: 93%
- Identify Areas with a Lack of Security Controls: 71%
- Identify Areas Lacking Adequate Protection Controls: 68%

N = 224

Length of Time Needed to Correct an Identified Deficiency by Revising Security Controls

- Less than Six Months: 34%
- Between Six Months and One Year: 42%
- More than One Year: 18%
- Risk Has Not Been Corrected: 4%
- Don’t Know: 3%

N = 185
Length of Time Needed to Correct an Identified Deficiency by Revising Policies/Procedures

- Less than Six Months: 45%
- Between Six Months and One Year: 35%
- More than One Year: 13%
- Risk Has Not Been Corrected: 3%
- Don’t Know: 2%

N = 180

Frequency of Auditing IT Security Plan

- Every Six Months: 10%
- Annually: 75%
- Every Two Years: 16%
- Don’t Know: 7%

N = 230
Frequency of Testing Breach Response Plan

- Every Six Months: 14%
- Annually: 63%
- Every Two Years: 23%

Method for Controlling Organizational Access to Patient Information

- Role-Based Controls: 78%
- User-Based Controls: 71%
- Group-Based Controls: 32%
- Location-Based Controls: 23%
- Rule-Based Controls: 15%
- Other: 0%
- Don't Know: 0%

N = 155
N = 200
Means By Which Organizations Provide Electronic Information to Patients

- CD/DVD: 75%
- Encrypted E-Mail: 45%
- Health Website/Web Portal: 43%
- USB/Thumb Drive: 33%
- PHR Hosted by Organization: 17%
- PHR Hosted by Third Party: 13%
- Uncrypted E-Mail: 0%
- Other: 5%

Methods of Controlling Access to Health Websites/Portals Offered to Patients

- User Name/Password: 98%
- Hard Token: 2%
- Biometric: 2%
- None: 0%

N = 253
N = 100
Types of Systems from Which Audit Log Data is Collected and Analyzed

- Firewall Log: 84%
- Applications: 75%
- Servers: 74%
- Intrusion Detection Systems: 61%
- Network Devices: 59%
- Billing Systems: 36%
- Other Administrative Management Systems: 31%
- Clinical/Medical Management Systems: 25%
- Managed Security Service: 23%
- Enrollment System: 18%
- Additional Storage Device: 9%
- Other: 1%

N = 220

Events Captured From Audit Log Data

- Clinician Access: 60%
- Non-Clinician Access: 62%
- Security Critical Events: 51%
- Patient Access to Data: 20%
- Other: 1%
- Don't Know: 5%

N = 220
Use of Audit Log Data

- Policy/Compliance Monitoring: 60%
- System Activity Monitoring: 77%
- Intrusion Detection: 76%
- Provide Accounting of Disclosure to Patients: 25%
- None: 8%
- Other: 1%
- Don't Know: 4%

N = 200

Plan in Place to Respond to Threats or Security Breaches

- Policy/Procedures in Place: 69%
- Developing Policy/Procedures: 27%
- No Policy: 1%
- Don't Know: 3%

N = 200
Means for Measuring Success of Security Controls in Place

- Reduced Risk Exposure: 74%
- Number of Detected Incidents: 70%
- Return on Investment: 11%
- Other: 0%
- Don’t Know: 0%

Existing Data Sharing Relationships

- Organizations in My Corporation: 71%
- State Government Agencies: 60%
- Other Local/Regional Facilities: 57%
- Public Health Entities: 55%
- Third Party Service Providers: 55%
- Health Information Exchange Organizations: 33%
- Facilities Outside of Local/Regional Area: 29%
- Federal Government Agencies: 29%
- Local Government Agencies: 28%
- Personal Health Record Vendors: 17%
- eHealth Exchange: 7%
- Facilitated Data Exchange: 6%

N = 121

N = 200
Future Data Sharing Relationships

- Health Information Exchange Organizations: 44%
- eHealth Exchange: 41%
- Facilities Outside of Local/Regional Area: 30%
- Other Local/Regional Facilities: 26%
- Personal Health Record Vendor: 31%
- Panoramic Data Exchange: 29%
- Public Health Entities: 26%
- State Government Agencies: 24%
- Federal Government Agencies: 23%
- Local Government Agencies: 22%
- Organizations in MyCorporation: 20%
- Third Party Services Providers: 18%

Percent of Business Associates with Formalized Agreement

- Less than 10 Percent: 1%
- 10 Percent to 24 Percent: 2%
- 25 Percent to 49 Percent: 1%
- 50 Percent to 74 Percent: 6%
- 75 Percent to 99 Percent: 40%
- All: 43%
- Don't Know: 7%

N = 200
Number of Cases of Medical Identity Theft

- None: 67%
- One: 3%
- Two: 5%
- Three: 1%
- Four: 1%
- Five: 1%
- Six: 0%
- Seven: 0%
- Eight: 0%
- Nine: 0%
- Ten: 0%
- Don't Know: 21%

N = 200

Instance of Security Breach

- Yes: 19%
- No: 71%
- Don't Know: 10%

N = 200
Percent of Breaches Reported to Authorized Groups

- Reported to Patients: 79%
- Reported to Government: 47%
- Reported to Local Media: 9%

Breach is the Fault of Business Associate

- Yes: 8%
- No: 93%

N = 53