HIMSS Security Survey

Supported by:

MGMA®
Medical Group
Management Association

2011 HIMSS Security Survey
Final Report
November 2, 2011

Now in its fourth year, the 2011 HIMSS Security Survey reports the opinions of information technology (IT) and security professionals from a wide range of healthcare provider organizations across the U.S. This survey seeks to identify key issues surrounding the tools and policies in place to secure electronic patient data at these healthcare organizations. The Medical Group Management Association (MGMA) has once again supported this research to encourage additional representation in the medical group and ambulatory space. The study collects information on a multitude of security-related items including organizations' general security environment, access to patient data, access tracking and audit logs, security in a networked environment and technology tools in place.

Contents

1. Executive Summary
2. Profile of Survey Respondents
3. General Information Security
4. Patient Data Access
5. Access Tracking/Audit Logs
6. Use and Measurement of Security Controls
7. Security in a Networked Environment
8. Use of Security Technologies
9. Patient Identity
10. Medical Identity Theft
11. Conclusion
12. About HIMSS
13. How to Cite This Study
14. 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. Role in Development of Organization's Security Policy
4. Participant Profile—Type of Medical Practice
5. Participant Profile—Method of Storing Data at Medical Practices
6. Participant Profile—Region
7. Participant Profile—Title
8. Percent of IT Budget Dedicated to Information Security
9. Change in Percent of IT Budget Dedicated to Information Security
10. Impact of Federal Initiatives on Federal Budget
11. Personnel Responsible for Securing Environment
12. Frequency of Conducting a Formal Risk Analysis
13. Uses for Risk Analysis Data
14. Length of Time Needed to Correct a Deficiency by Revising Security Controls
15. Length of Time Needed to Correct a Deficiency by Revising Policies/Procedures
16. Method for Controlling Organizational Access to Patient Information
17. Means by Which Organizations Provide Electronic Information to Patients
18. Method of Controlling Access to Health Websites/Portals Offered to Patientsjul
19. Types of Systems from Which Data is Collected and Analyzed
20. Events Captured by Audit Log Data
21. Use of Audit Log Data
22. Plan in Place to Respond to Threats or Security Breaches
23. Means for Measuring Success of Security Controls in Place
24. Existing Data Sharing Relationships
25. Future Data Sharing Relationships
26. Use of Security Technologies – Top Ten
27. Percent of Data on Laptop Computers that is Encrypted
28. Percent of Data on Desktop Computers that is Encrypted
29. Percent of Data on Servers that is Encrypted
30. Percent of Data on Back-up Devices that is Encrypted
31. Percent of Data on E-mail that is Encrypted
32. Method of Proving Patients' Identities
33. Method for Ongoing Validation at Subsequent Visits
34. Method for Identifying Duplicates Within MPI
35. Items Stored in Electronic Health Record
36. Has Organization Had One Case of Medical Identity Theft
37. Number of Cases of Medical Identity Theft

1. Executive Summary

In its fourth year, the 2011 HIMSS Security Survey, supported by MGMA, reports the opinions of 329 information technology (IT) and security professionals employed by hospitals and ambulatory care providers. This survey seeks to identify key issues surrounding the tools and policies in place to secure electronic patient data at these healthcare organizations. An important component explored in this study is the issue of risk analysis. A risk analysis offers healthcare organizations a comprehensive tool by which to gain a complete understanding of its security profile—the threat environment, system vulnerabilities and overall risk exposure. Risk analysis is also a key requirement of the Health Insurance Portability and Accountability Act (HIPAA) final security rule, and as such, has been a requirement for healthcare organizations for many years.

Risk analysis is also a key criterion of the federal government's electronic health record (EHR) "meaningful use" incentive programs. Eligible hospitals and eligible providers participating in the EHR incentive program are required to document that they have protected electronic health information created or maintained by the EHR *by conducting or reviewing a security risk analysis*. These organizations must also implement security updates as necessary and correct identified security deficiencies as part of its risk management process. Recent supporting research from a separate survey suggests that only 45 percent of U.S. hospital protect electronic health information created or maintained by your EHR by conducting and reviewing a security risk analysis[1].

Results from the 2011 HIMSS Security Survey indicated that three-quarters of all survey respondents reported that their organization performs a risk assessment to evaluate the risks to patient data at their organization. In the four years that HIMSS has been studying the security environments of healthcare organizations, the percent of respondents that have conducted a risk assessment has remained consistent at approximately three-quarters of respondents. Of concern, as in previous years, are the one-quarter of responding organizations that do not conduct a security risk assessment at all.

Healthcare organizations required to conduct a risk analysis, as a result of meaningful use criteria, also must correct deficiencies identified during the risk analysis process. Indeed, this study suggests that those respondents that *are* conducting a risk assessment are taking action based on the results of the risk assessment. For example, more than 80 percent of respondents used this information to determine which security controls should be put into place. Further, risk assessment results were also used to identify gaps in existing security controls, policies and/or procedures. This enables organizations to actively take steps to correct deficiencies.

Other key survey results include:

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 4.23. This is fairly consistent with what has been reported in previous years.

Security Budget: The majority of respondents reported that they spent three percent or less of their overall IT budget on information security. More than half of respondents

---

[1] HIMSS Analytics Report: Summary of Stage One Meaningful Use, September 2011. www.himssanalytics.org.

(59 percent) indicated that the IT budget dedicated to information security has increased in the past year.

Oversight of Information Security: Approximately half of respondents reported they have either a Chief Security Officer (CSO)/Chief Information Security Officer (CISO) or full-time staff in place to handle their organizations' security functions. Those working for a corporate organization or hospital were more likely to report that they had a CSO/CSIO in place compared to individuals working for medical practices. Respondents working for medical practices were more likely to indicate that they handled their security function using outsourced or part-time resources.

Employee/Patient Data Access: Nearly all respondents reported their organization monitors how their employees are accessing electronic patient information. Role-based and user-based controls were reported to be most widely used.   Approximately two-thirds of respondents noted that their organization provides information that is electronically stored to patients, surrogates and/or designated others.

Audit Logs: Nearly all of the respondents reported that their organization collects and analyzes audit log information from at least one system in their organization, with firewall logs being the most common source of audit log data. Audit log data is most widely used for policy compliance monitoring.

Security in a Networked Environment: Approximately 82 percent of respondents reported that their organization shares patient data in an electronic format with external organizations. Data is most frequently shared with other facilities within their corporate entity, third party service providers and state government entities.

Future Use of Security Technologies: The survey reports that healthcare organizations considering making a security purchase were most likely to identify data loss prevention, e-mail encryption and single-sign on as potential future procurement. Approximately one-quarter of *all* healthcare organizations in the survey plan to purchase these technologies.

Patient Identity: Most respondents reported that their organizations' validate the identity of patients at the time of a patient encounter. Use of a government or facility-issued photo ID was the most frequently reported means of validation. Approximately half of respondents use a formal reconciliation process to identify records in their master person index.

Medical Identity Theft: Fourteen 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. Those working for corporate entities were more likely to report a breach, compared to those working at medical practices or hospitals.

2. Profile of Survey Respondents

A total of 329 individuals completed this survey. Data was collected via a web-based survey between August 17 and October 7, 2011. The 2010 study had 272 respondents.

Qualifying Respondents

In order to qualify to participate in this research, respondents were asked to answer a series of qualifying questions. All respondents identifying their primary worksite as medical 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 indicate that their practice had either electronic health record (EHR) or document imaging management system.

All respondents from "other organization types" (e.g., hospitals, corporate entities, etc) were required to play at least some role in the information security arena at their organization. As such, respondents has 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; or
- I am an IT professional (outsourcer) who handles IT for a healthcare organization.

Nearly three-quarter of the respondents from "other organization types" (70 percent) answered "yes" to at two of the questions above. Respondents indicating that they played no role in the security of data were excluded from the data collection process. These respondents are not included in the 329 responses on which the analysis in this report is based.

Two-third of these respondents (67 percent) indicated that they are responsible for ensuring that their organization's data is secure on a day-to-day basis. Another 56 percent of respondents indicated that they are part of a committee that is responsible for developing the organization's policy on privacy and data security. Slightly more than half (53 percent) reported responsibility for developing the organization's policy on privacy and data security. The same percent reported that they are notified of all breaches that require notification.

Half of the survey respondents indicated that they are a senior Information Technology (IT) executive at their organization. Specifically, 37 percent of respondents indicated that they hold the title of Chief Information Officer. Another seven percent reported their title to be Vice President of IT/IS and six percent reported they were a Director-level professional in the IS department. Approximately 18 percent of respondents reported their title to be Chief Security Officer and one percent indicated their title is Chief Privacy Officer. Four percent of the respondents reported their title to be either Practice Administrator or Clinician. The remaining 27 percent of respondents reported their title

as "other", which includes a wide variety of IT and security titles. By design, respondents from medical practices were not asked their titles, suggesting that the percent of practice administrators and clinicians is actually greater than what is stated here. See Figure One.

Participant Profile – Title

Chief Information Officer — 37%
Chief Security Officer — 18%
VP of Information Systems — 7%
Director of IT — 6%
Practice Administrator — 3%
Chief Privacy Officer — 1%
Clinician — 1%
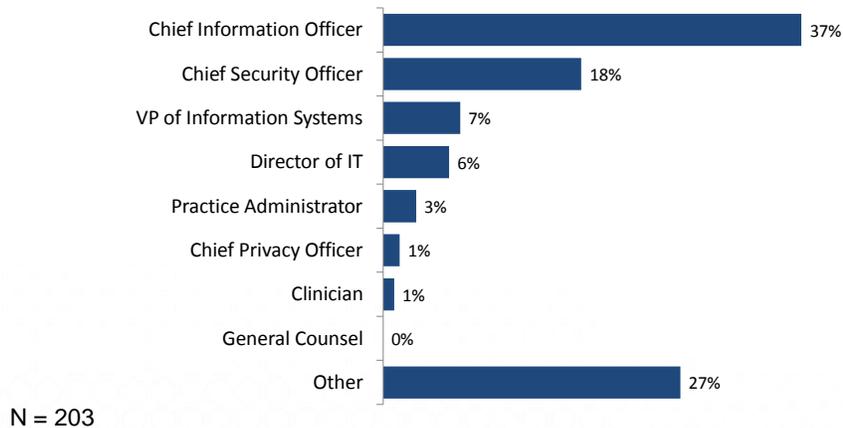General Counsel — 0%
Other — 27%

N = 203

Figure One. Participant Profile—Title

Organization Type

More than one-third of respondents (38 percent) reported that they work at a medical practice. Another third reported working for either a stand-alone hospital (21 percent) or a hospital that is part of a delivery system (16 percent). Sixteen percent work for the corporate offices of a healthcare system. The remaining nine percent of respondents work for a variety of healthcare organizations, including health plans, hospice facilities, military healthcare facilities or health information exchanges (HIEs).

For the purposes of analysis, the sample was divided into four groups, those working for hospitals, those working at corporate organizations, those working for medical practices and those working for other types of organizations. Differences that exist between these groups in this study will be highlighted throughout the report. In addition, some of the questions in this research were not asked of individuals working at a medical practice. When this is the case, this will be noted in the report. See Figure Two.
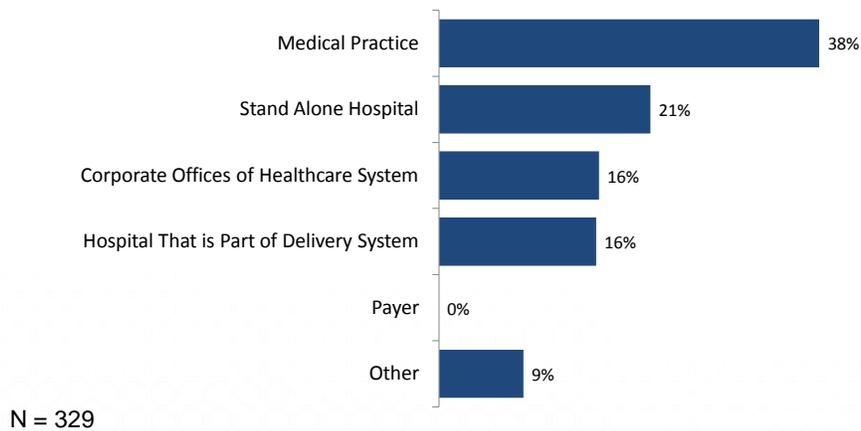
Participant Profile – Organization Type

Figure Two. Participant Profile—Organization Type

Medical practices sampled in this survey have an average of 36.80 physician FTEs (median 10.25). The vast majority of these practices (85 percent) classified themselves as an independent medical practice. Another seven percent of respondents indicated that they worked for an organization that is a medical practice owned by a hospital or integrated delivery system. Another three percent classified the practice as a federally qualified health center (FQHC[2]). Also represented in the sample were freestanding ambulatory surgery centers and retail walk in primary care clinics.

The greatest percentage of respondents (17 percent) comes from the South Atlantic region, followed by the East North Central region at 16 percent.   The Mid Atlantic and Mountain regions each had 11 percent of the respondents in the survey. The smallest number of respondents comes from New England (six percent).

3. General Information Security

Despite the fact that 43 percent of respondents indicated that their organization has increased the resources dedicated to information security as a result of the federal initiatives such as ARRA, HIPAA 5010 and ICD-10 approximately half of respondents reported that their organization spends three percent or less of their organization's IT budget on information security.

---

[2] A *FQHC is a "safety net" provider. Types of FQHCs can include community health centers, public housing centers, outpatient health programs funded by the Indian Health Service, and programs serving migrants and the homeless. The main purpose of the FQHC Program is to enhance the provision of primary care services in underserved urban and rural communities. From* http://www.cms.gov/MLNProducts/downloads/fqhcfactsheet.pdf *This site was accessed on October 22, 2010.*

Approximately half of the survey respondents noted that they have a full-time resource, such as a Chief Security Officer, in place to oversee the security environment. Nine percent of respondents reported that their entire security function is handled externally. Approximately three-quarters of respondents noted that they conduct a formal risk analysis and 58 percent indicated that this risk analysis is conducted at least annually.

Respondents were asked to identify the percent of their organization's overall IT budget that is dedicated to information security. Approximately one-third of respondents (35 percent) indicated that their organization spends between one and three percent of the organization's overall IT budget on information security. Another 18 percent noted that they spend less than one percent of the overall IT budget on security, while 16 percent noted that they spend four to six percent of their IT budget on information security. Only four percent of respondents noted that more than 12 percent of their organization's IT budget is dedicated to information security. See Figure Three.

Percent of IT Budget Dedicated to Information Security

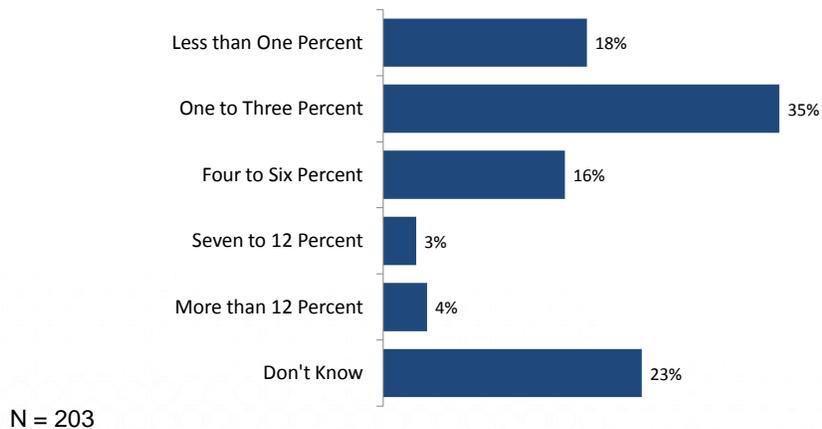| Category	Percent
Less than One Percent	18%
One to Three Percent	35%
Four to Six Percent	16%
Seven to 12 Percent	3%
More than 12 Percent	4%
Don't Know	23%

N = 203

Figure Three. Percent of IT Budget Dedicated to Information Security

In summary, *more than half of respondents in this year's survey reported that they spent three percent or less than their IT budget on information security.* This can be compared to 46 percent in last year's survey. However, a direct comparison needs to be made with caution, as individuals in medical practices were not asked this question in the 2011 survey.

All survey respondents were asked to indicate whether the amount of the IT budget dedicated to information security has changed in the past year. Approximately 59 percent of respondents indicated that their organization had increased during this period. This represents a slight increase from the 53 percent that indicated this was the case in the previous survey. Only two percent of respondents indicated that the security

budget at their organization decreased. The remaining respondents indicated no change in their information security budget in the past year.

Respondents were also asked to identify the impact that federal initiatives such as the EHR incentive program, HIPAA 5010 electronic transactions and ICD-10 had on budget/resources for information security. *A majority of respondents (43 percent) indicated that these federal initiatives have resulted in an increase in the budget and resources dedicated to information security.* Another third of respondents (34 percent) noted that federal initiatives have had no impact on the resources and budget dedicated to information resources at their organization. Approximately 15 percent of respondents noted that these federal initiatives have diverted resources and budget from information security initiatives. These responses were consistent to what was reported in 2010.

There was little difference in how respondents at different organization types responded to this question. The percent of respondents in each group indicating that their information security budget increased as a result of current federal initiatives is listed below:

- Corporate organizations – 47 percent;
- Hospitals – 38 percent; and
- Medical practices – 47 percent.

In addition to the budget dedicated to information security, respondents provided information on how their organizations allocate staff to manage their security function. Approximately half of respondents (50 percent) reported that they have either a Chief Security Officer (CSO)/Chief Information Security Officer (CISO) or have full time staff other than a CSO/CISO in place to handle the security function. This is consistent with 53 percent of respondents who reported this to be the case in 2010. Thirty percent of respondents noted that part-time staff handle their security function.

This question also tested whether or not organizations are outsourcing any of their IT security function. Approximately nine percent of respondents indicated that they outsource the *entire* information security function. Last year, five percent of respondents reported this to be the case.

By type of organization, respondents working for medical practices were less likely to report having a CSO or CISO than were respondents working at hospitals and or corporate organizations. More specifically, one-third of those at corporate organizations reported having a CISO, compared to 24 percent of hospital respondents and 14 percent of respondents at a medical practice.

Instead, those working at medical practices were more likely to handle their security function using outsourced staff or part-time staff. Indeed, 55 percent of respondents working for a medical practice reported that their security function was handled using this method. In comparison, 19 percent of respondents from a corporate organization and one-third of respondents from hospitals reported this to be the case.

Nearly three-quarters of respondents (74 percent) noted that their organization conducts a formal risk analysis to evaluate risks to patient data at their organization. This is consistent to the number that was reported in the 2010 and 2009 surveys. Nine percent of respondents were unsure if their organization conducted a risk analysis. Respondents

working for medical practices were twice as likely to report that their organization *did not* conduct a risk analysis (28 percent) as were respondents working for a hospital (14 percent). Only, seven percent of respondents working at a corporate office also reported this to be the case.

Among the respondents that reported that they conducted a risk analysis, nearly half reported that their organization conducts a formal risk analysis annually (49 percent). Another eight percent reported that they conduct a risk analysis once every six months and 21 percent conduct this type of analysis every other year. See Figure Four.

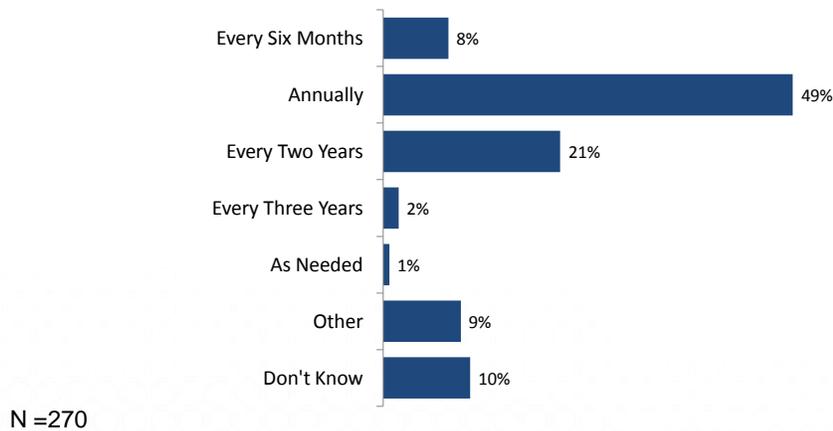## Frequency of Conducting a Formal Risk Analysis

N =270

Figure Four. Frequency of Conducting a Formal Risk Analysis

Respondents that conducted a risk analysis were asked how the information from their risk analysis could inform their security environment in three key areas:

- Use risk analysis to determine which security controls to put into place – 83 percent;
- Identify area where lack of security controls pose a risk – 67 percent; or
- Identify area where lack of security policies/procedures pose a risk – 62 percent.

These numbers are consistent with what was reported in 2010.

Respondents working for a medical practice were not asked this question. For the purposes of this survey, security controls are safeguards or countermeasures 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 logical access controls, antivirus software or firewalls.

Those individuals that indicated that 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 of respondents (37 percent) noted that their organization corrected the identified issues within six months. Another third (33 percent) noted that they resolved the deficiency within six months to one year. Only seven percent of respondents noted that they did not rectify the issues uncovered by the risk analysis.

Individuals that indicated that their risk analysis uncovered risks due to a lack of security policies and/or procedures were asked to identify how long it would took their organization to resolve these issues. Half of respondents noted that their organization resolved the issues within six months. Nearly another third (30 percent) rectified the issue in six months to one year. Only six percent of respondents noted that the issue still has not been resolved.

Each year, respondents are asked to indicate how mature their security environment is, using a one to seven scale, where one is not at all mature and seven is very mature. Respondents recorded an average score of 4.23, which is consistent with what has been reported in previous reports (2010 – 4.43; 2009 – 4.27). A score of one was identified by only four percent of respondents and a score of seven was identified by three percent of respondents; respondents were most likely to select the value of five on this scale. Individuals working for a medical practice were not asked this question.

4. Employee/Patient Data Access

Nearly all of the individuals responding to this survey reported that their organization has mechanisms in place to monitor how their employees are accessing electronic patient information. Role-based and user-based controls were reported to be most widely used. Approximately two-thirds of respondents their organization provides information that is electronically stored to patients, surrogates and/or designated others.

In order to secure information, healthcare organizations in this survey use a variety of controls that limit employee access to patient information. This study explores five different means for controlling access to patient information. Only one percent of respondents did not report use of any of the controls tested in this research to secure patient data. Nearly half (46 percent) of respondents noted that their organizations use more than one of the controls tested for in this research. This is consistent with what has been reported in previous surveys. Last year, 56 percent of respondents reported using more than one tool to secure information.

User-based controls, which are those that control employee access based on a person's knowledge of user-based account credentials, were identified by 65 percent of respondents. Last year, this was selected by 74 percent of respondents and was the most frequently used method for controlling employee access to patient information.

Role-based controls, which are defined as those controls put into place based on an employee's job/role type. For instance, clinicians might have one type of access while nurses have another. Two-thirds of the survey respondents (67 percent) reported that

their organization uses this type of control. Last year, this item was selected by 71 percent of respondents.

Each of the three remaining types of controls were used much less widely. Group-based controls, which limits access to patient information to a specific group of people, such as all nurses who see patients in the ICU, was identified by only 19 percent of respondents. Location-based controls, defined in this research as those who work on a particular floor or unit, were reported to be used by 17 percent of respondents. Reported use of both of these controls declined from what was reported in 2010. One potential explanation for this is that more medical practices are included in this year's research and were asked this question. Respondents at medical practices were much less likely to report that they use these controls than were their counterparts at hospitals and corporate locations.

Finally, eight percent use rule-based access, to control employee access to patient information. This type of control limits access using an if/then statement. This is similar to what was reported in the 2010 research.

Those respondents working at a medical practice were more likely to report that their organization used a single means of control than were those respondents working for a hospital or corporate organization (66 percent compared to 46 and 51 percent respectively).

Nearly two-thirds of respondents (63 percent) reported that their organization provides access to electronic patient information to patients, surrogates and designated others. In comparison, 59 percent of respondents in the 2010 survey reported that they provide patients, surrogates and designated others this type of access.

Respondents were also asked to identify *how* access to this type of electronic information is provided to patients, surrogates and/or designated others. Among the respondents who reported they make this type of access available, CDs were identified as the most frequent means of sharing information. This media was identified by 56 percent of respondents; this was also the top item selected in 2010, identified by 54 percent of respondents. Web portals are also a commonly used means of providing patients access to information – 39 percent of respondents reported that their organization uses this means for providing access to data. The other choices offered in this study, as well as the percent of respondents that selected the choice, are shown below.

- Secure (encrypted) e-mail – (33 percent);
- USB thumb drive – (19 percent);
- Personal Health Record offered by a Third Party – (6 percent); and
- Unencrypted e-mail – (4 percent).

Respondents who provide access to electronic patient information through a health website/web portal were also asked to identify how their organization controls access to these mechanisms offered to patients. Twenty-one (21) percent of respondents indicated that they have no access controls restricting this type of access; this is an increase from the 17 percent reported in last year's survey. Among those that control access through a website or web portal, nearly 89 percent indicated that the patient is assigned a unique user id and login password; this was also the top response in the 2009 survey. Respondents were much less likely to report either that patients use a hard token (five percent) or biometric measures (two percent) to access websites/web portals.

5. Access Tracking/Audit Logs

Nearly all of the respondents reported that their organization collects and analyzes audit log information from at least one system in their organization, with firewall logs being the most common source of audit log data. Audit log data is most widely used for policy compliance monitoring.

Only a handful of respondents (five percent) reported that their organization does not collect and analyze log information from any system at their organization. This represents a slight decrease from the six percent that was reported last year. This question was not asked of respondents working for medical practices.

Among those respondents reporting the types of systems from which they collect and analyze logs, more than three-quarters of the respondents (84 percent) reported that their organization collects and analyzes information from their firewall log; this log was also reported as the most frequent system from which audit log was collected and analyzed in 2010. At least half of respondents also reported that their organization collects and analyzes information from servers, applications, intrusion detection systems and network devices. Respondents were least likely to report that they collect information from their enrollment systems. Respondents working for medical practices were not asked this question. A full list of systems from which respondents collect and analyze data is included in Figure Five.

Types of Systems From Which Organizations Provide Electronic Information to Patients

System	Percent
Firewall Log	84%
Servers	81%
Applications	73%
Intrusion Detection Systems	63%
Network Devices	60%
Billing Systems	37%
Practice Management Systems	36%
Case/Medical Management Systems	23%
Managed Security Service	20%
Additional Storage Devices	14%
Enrollment Systems	13%
Other	4%

N =181

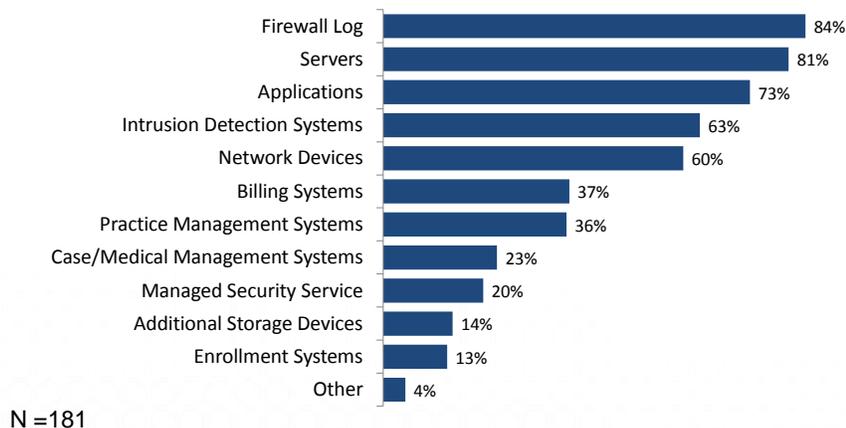Figure Five. Types of Systems from Which Data is Collected and Analyzed

Respondents were also asked to identify the types of events their audit log captures. Approximately two-thirds of respondents (67 percent) noted that their organization collects information about clinician access to data; this surpasses security critical events for the first time as the top choice. The percent of respondents indicated that security

critical events are reported in their audit logs is 64 percent; this is also the percent of respondents indicated that their organization's audit log captures information on non-clinician access to data. Only 18 percent of respondents indicated that their organization's audit logs capture information about patient access of data.

Respondents at corporate organizations were most likely to use the controls outlined in this study to secure access to data. Conversely, respondents working for medical practices were least likely to report using these types of controls. See Table One.

Types of Systems	Corporate	Medical Practice
Clinician Access to Data	85%	55%
Security Critical Events Only	79%	52%
Non-Clinician Access to Data	72%	56%
Patient Access to Data	34%	14%
Don't Know	8%	16%
N	53	130

Table One. Types of Systems from Which Data is Collected and Analyzed, By Facility Type

Nearly three-quarters of respondents reported that their organization actively uses audit log data for policy compliance monitoring (72 percent). Two-thirds of respondents indicated that their organization actively utilizes audit log data for system activity monitoring. These items were both increased slightly from what was reported in the 2010 survey. The percent of respondents reporting they use intrusion detection also increased this year, from 58 percent in 2010 to 64 percent this year. Importantly, while the least likely use for audit log information for providing an Accounting of Disclosures to patients; nearly half of respondents (46 percent) reported using audit log data in this manner. This was up from one-third of respondents in 2010. Respondents working for medical practices were not asked this question.

6. Use and Measurement of Security Controls

Over 80 percent of respondents were likely to report that their organization uses information generated in their risk assessment to identify which security controls to put into place. Respondents also indicated that the success of organizational security controls was measured using items such as number of detected security incidents and reduced risk of exposure.

While this survey no longer directly asks respondents if they have security controls in place, earlier in this paper we reported that the majority of respondents (83 percent) reported that they used the information generated in their risk assessment to determine which security controls to put in place at their organizations.

Respondents were presented 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. Slightly more than half of the

survey respondents indicated that their organization uses at least one of these tools to measure the success of the security controls at their organization.

Among those that reported that their organization measures the success of these controls, the most frequently used measure is identifying the number of detected security incidents; this was selected by 74 percent of respondents, an increase from the 59 percent of respondents who reported this to be the case in 2010. A similar percent (73 percent) reported that their organization measures success by evaluating the reduced risk exposure that their organization experiences as a result of use of these controls. Only eight percent reported that their organization measures the return on investment (ROI) that they get from the cost of tools when compared to the risk reduction.

Approximately three-quarters of respondents (34 percent) reported that they do not measure the success of their organization's security controls. Another 11 percent of respondents reported don't know to this question. Respondents who worked for a medical practice were not asked this question.

7. Security in a Networked Environment

Most survey respondents reported that their organization shares patient data in electronic format. Data is most frequently shared with other facilities within the corporate organization, third party providers and state governments. Survey responses also show that respondents expect that data sharing with health information exchanges is expected to increase substantially in the future.

Respondents were asked to identify the types of organizations with which they share patient data in electronic format. Approximately 82 percent of respondents reported that their organization shares information with at least one other type of organization; this is equivalent to the 85 percent of respondents who reported this to be the case in 2010. See Table Two.

Organizations with Which Data is Shared TODAY	Percent
Other Practices/Hospitals in Corporate Organization	65.96%
Third Party Service Providers/Vendors	49.54%
State Government Entities	39.51%
Other Local Practices/Hospitals that Aren't Part of Corporate Organization	39.21%
Public Health Entities	28.88%
Federal Government	26.44%
Local Government Entities	24.01%
Practices/Hospitals Outside of Local Region/State	19.45%
HIEs/RHIOs	18.54%
PHR Vendors	11.25%
NHIN-Facilitated Data Exchange	7.29%
Other	1.52%

Table Two. Organizations with Which Data is Shared Today.

Respondents working for medical practices were least likely to report that they shared patient data with at least one other type of organization listed above (75 percent), compared to 85 percent of hospital organizations and 93 percent of those working for a corporate organization.

With regard to future data sharing arrangements, respondents were most likely to report that their organizations would share with HIEs/RHIOs in the future. This is followed by other types of provider organizations, including both those that are local (but not part of their corporate entity) and those that are outside of their local region. See Table Three below for complete information on plans for future data sharing arrangements.

FUTURE DATA SHARING PLANS	Percent
HIEs/RHIOs	61.70%
Other Local Practices/Hospitals that Aren't Part of Corporate Organization	45.29%
Practices/Hospitals Outside of Local Region/State	44.68%
Public Health Entities	43.47%
PHR Vendors	43.47%
NHIN-Facilitated Data Exchange	39.51%
Federal Government	34.35%
State Government Entities	33.74%
Local Government Entities	32.22%
Third Party Service Providers/Vendors	19.45%
Other Practices/Hospitals in Corporate Organization	16.11%
Other	6.08%
Total	100.00%

Table Three. Organizations with Which Data will be Shared in the Future.

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 table above; half of these respondents worked for a medical practice.

8. Use of Security Technologies

Firewalls and user access controls are used nearly universally by the respondents in this survey. By volume of hospitals making a purchase, respondents were most likely to identify data loss prevention, e-mail encryption and single-sign on.

Respondents were asked to identify the types of security tools that are in place at their organization. All of the respondents reported that at least one type of the technologies listed in this question is present at their organization. Firewalls were identified most frequently as the security tool in place at healthcare organizations; they are used at 99 percent of respondents' organizations. Also used by at least 90 percent of respondents were user access controls, identified by 95 percent of respondents. Utilization of all technologies in this survey is listed in Table Four below:

Security Tool in Use Today	Percent
Firewalls	99.09%
User Access Controls	94.53%
Audit Logs of Each Access to Patient Health Records	83.28%
Off-Site Storage	76.29%
Disaster Recovery	75.99%
Wireless Security Protocols	71.12%
Electronic Signature	65.96%
Data Encryption (Data in Transmission)	65.05%
E-Mail Encryption	58.36%
Data Encryption (Data in Storage)	53.80%
Intrusion Prevention/Detection Services	51.67%
Mobile Device Encryption	44.07%
Network Encryption	41.95%
Single Sign On	40.43%
Data Loss Prevention	37.08%
Two-Factor Authentication	27.36%
Log Aggregation Tool	17.63%
Public Key Infrastructure	14.29%
Biometric Technologies	11.55%
None of the Above	0.00%
Total	100.00%

Table Four. Security Tool in Use Today.

There are also differences in the types of technologies that are in place at the various organization types. In summary, respondents working for corporate organizations were more likely to report that their organizations used the security technologies identified in this research. The exceptions are wireless security protocols, electronic signature, single sign on, and public key infrastructure. The technologies are more widely used in hospitals. None of the technologies in this report are most frequently used in medical practices. The percent of respondents reporting "yes" by organization type is shown in Table Five Below.

Security Tool in Place Today	Corporate Organizations	Hospitals	Medical Practices
Firewalls	100.00%	99.19%	99.23%
User Access Controls	98.25%	94.31%	94.62%
Audit Logs of Each Access to Patient Health Records	91.23%	85.37%	81.54%
Off-Site Storage	80.70%	75.61%	77.69%
Disaster Recovery	92.98%	76.42%	68.46%
Wireless Security Protocols	82.46%	84.55%	54.62%
Electronic Signature	61.40%	73.17%	67.69%
Data Encryption (Data in Transmission)	80.70%	70.73%	55.38%
E-Mail Encryption	78.95%	73.98%	33.08%
Data Encryption (Data in Storage)	68.42%	52.03%	48.46%
Intrusion Prevention/Detection Services	73.68%	55.28%	39.23%
Mobile Device Encryption	66.67%	49.59%	26.15%
Network Encryption	52.63%	34.15%	45.38%
Single Sign On	47.37%	47.97%	30.77%
Data Loss Prevention	43.86%	30.08%	43.08%
Two-Factor Authentication	42.11%	32.52%	15.38%
Log Aggregation Tool	33.33%	20.33%	6.15%
Public Key Infrastructure	19.30%	20.33%	4.62%
Biometric Technologies	22.81%	15.45%	3.85%
None of the Above	0.00%	0.00%	0.00%

Table Five. Security Tool in Use Today, by Type of Organization.

Respondents were also asked to identify those tools that they plan to add to their environment in the future. By number of hospitals making a purchase, respondents were most likely to identify data loss prevention, e-mail encryption and single-sign on. Approximately, one-quarter of all hospitals in the sample plan to purchase these technologies.

Another way to evaluate the data is to look at the number of facilities that plan to purchase these security tools for the first time. Two-thirds of hospitals that don't presently use a disaster recovery solution plan to make this purchase in the future. More than half of the hospitals that don't currently use e-mail encryption solutions plan to purchase this type of solution in the future. This is also the case for data encryption (data in transmission) and wireless security protocols.

Biometric technologies, public key infrastructure and log aggregation tools are all used at less than 20 percent of respondents' organizations. One-quarter of respondents not presently using log aggregation tools reported that they will do so in the future. However, future use of public key infrastructure and biometric technologies is not expected to increase greatly. Only 12 percent of respondents that don't currently use public key infrastructure plan to do so in the future. For biometric technologies, only seven percent of healthcare organizations not using this technology at this time plan to do so in the future.

This research also evaluates the use of encryption technology on specific device types. Only seven percent of respondents reported that they don't encrypt any data on any of the devices tested in this research. This is down from 15 percent of respondents who reported this to be the case in the 2010 survey.

Respondents were most likely to report that none of the data on their desktop computers were encrypted; 42 percent of respondents noted that this is the case at their organization. This is similar to what was reported in 2010, when 42 percent of respondents reported that none of the data on their desktop computers is encrypted. One third of respondents (35 percent) noted that their servers are not encrypted and 31 percent of respondents noted that their organization does not encrypt any of their back-up tapes.

Respondents were most likely to report that the encrypt data on laptop computers. Slightly more than 40 percent of respondents noted that at least 75 percent of the data on their organizations' laptop computers is encrypted. One-third of respondents noted that at least 75 percent of the data on their organizations' back-up tapes is encrypted.

9. Patient Identity

Most respondents reported that their organizations' validate the identity of patients at the time of a patient encounter. Use of a government or facility-issued photo ID was the most frequently reported means of validation. Approximately half of respondents use a formal reconciliation process to identify records in their master person index.

Four percent of respondents reported that their organization does not use any tools to validate the identity of the patient at the point of care. This is a very slight increase from the percent of respondents who indicated this to be the case in 2010. More than half of respondents (56 percent) noted that their organization checks a person's valid government/facility-issued photo ID. Slightly more than 40 percent (42 percent) reported that their organizations asks a patient for valid ID and compares that information with data in their system. Only 29 percent of respondents reported that they compare the information provided by the patient to information contained in the master person index.

Most respondents also noted that they had a means of identifying patients on subsequent visits. Most frequently used is a process whereby patients are assigned unique identifiers; this was selected by 62 percent of respondents. This represents an increase from the 46 percent of respondents who indicated this was the case in the 2010 survey. Nearly one-quarter of respondents (21 percent) that their organization offers a facility issued ID card; nine percent noted that their organization created a facility issued smart card with processing capability. Both items are reported to be used more widely today than they were in the 2010 survey. One percent of respondents reported that they used either a fingerprint or palm scan for identification and one respondent reported that his/her organization uses iris scan or retinal scan technology for identification purposes. Eighteen (18) percent were not sure how this validation was accomplished. This question was not asked of individuals working at a medical practice.

Respondents were also asked to identify how duplicate records were identified in the master person index. Approximately half of respondents (49 percent) reported that they had a formal reconciliation process with their staff. Another 29 percent reported that the

process was an informal manual process. Approximately 14 percent were not sure how this was accomplished. Three percent reported that they did not have a process for managing duplicate records and four percent of the respondents noted that they do not have an MPI. These responses were similar to those reported in 2010. Those working for a medical practice were not asked this question.

Finally, respondents were asked to identify if and how their electronic health record (EHR) stores data used for identifying the patient. Ninety percent of respondents indicated that they enable alphanumeric storage of demographic information, such as name, address, phone, date of birth, gender or social security number; this was the type of data most frequently identified in 2010. Approximately 60 percent of respondents indicated that their EHR can store analog, scanned or digital photos. While respondents were less likely to report that their EMR could store alphanumeric digital representations such as smart card identifiers 24 percent, this does represent an increase from the 16 percent of respondents who noted they could store this type of information in the 2010 survey. Six percent of respondents reported that they don't have an EHR.

10. Security Breaches and Medical Identity Theft

Nearly three-quarters 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. Fourteen (14) percent of respondents reported that their organization had experienced at least one instance of medical identity theft.

Respondents were asked to indicate whether or not they have policies and procedures in place to respond to threats and/or incidents relating to a security breach. Nearly three-quarters of respondents (71 percent) indicated that their organization has these types of policies and procedures in place. This is a slight increase from last year.

One-quarter of respondents reported that they are currently developing these types of policies and procedures. This represents a slight decrease from the 27 percent of respondents who reported this to be the case last year. Three percent of respondents indicated that they do not have this type of plan in place and have no plans to establish one in the future.

Only 14 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. This is a substantial decrease from the 31 percent of respondents who reported this to be the case in the 2010 survey. Those working for a corporate entity were most likely to report a breach (22 percent), followed by those working for medical practices (15 percent) and hospitals (12 percent).

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".

11. Conclusion

One of the required items for both EHs and EPs to qualify for the EHR incentive program is that they must protect electronic health information created or maintained by the electronic health record (EHR) by conducting or reviewing a security risk analysis. Our survey suggests that three-quarters of survey respondents have met this requirement at this time.

Going forward, all EPs and EHs need to ensure that a risk assessment is the cornerstone of managing their security environment. A risk assessment gives EPs and EHs the information they need to ensure that they have appropriate policies, procedures and controls in place at their organization to not only secure data as it resides electronically in their EHRs, but also that the data is secure as it is being shared outside the organization.

The results also continue to demonstrate that medical practices are not as advanced in many of the areas for security data, when compared to hospitals and corporate organizations. For instance, respondents working for a medical practice were less likely to report that their organization conducted a risk assessment, when compared to those working at other types of healthcare facilities. In addition, respondents at medical practices were less likely than their counterparts to report that security tools such as wireless security protocols, e-mail encryption or mobile device encryption. In order to manage their security environment, the respondents at the medical practices in this study rely on part time staff and consultants.

In addition to meeting the incentive program requirements, establishing a robust environment is crucial as organizations share information outside of their organizations. Only a handful of survey respondents indicated that they do not presently have any data sharing arrangements in place and do not plan to add any in the future. However, data sharing with organizations such as health information exchanges is expected to grow extensively. Respondents are also widely sharing electronic information with their patients and surrogates. As such, while organizations are widely using security technologies and tools to secure data, we expect that options such as data encryption for data that is being transmitted and e-mail encryption, each of which is used by less than two-thirds of respondents, will be more widely implemented in the future.

12. About HIMSS

HIMSS is a cause-based, not-for-profit organization exclusively focused on providing global leadership for the optimal use of information technology (IT) and management systems for the betterment of healthcare. Founded 50 years ago, HIMSS and its related organizations are headquartered in Chicago with additional offices in the United States, Europe and Asia. HIMSS represents more than 38,000 individual members, of which more than two thirds work in healthcare provider, governmental and not-for-profit organizations. HIMSS also includes over 540 corporate members and more than 120 not-for-profit organizations that share our mission of transforming healthcare through the effective use of information technology and management systems. HIMSS frames and leads healthcare practices and public policy through its content expertise, professional development, research initiatives, and media vehicles designed to promote information and management systems' contributions to improving the quality, safety, access, and cost-effectiveness of patient care. 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. 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 4th Annual HIMSS Security Survey.

14. 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

Appendix

Participant Profile – Organization Type

Figure 1

N = 329
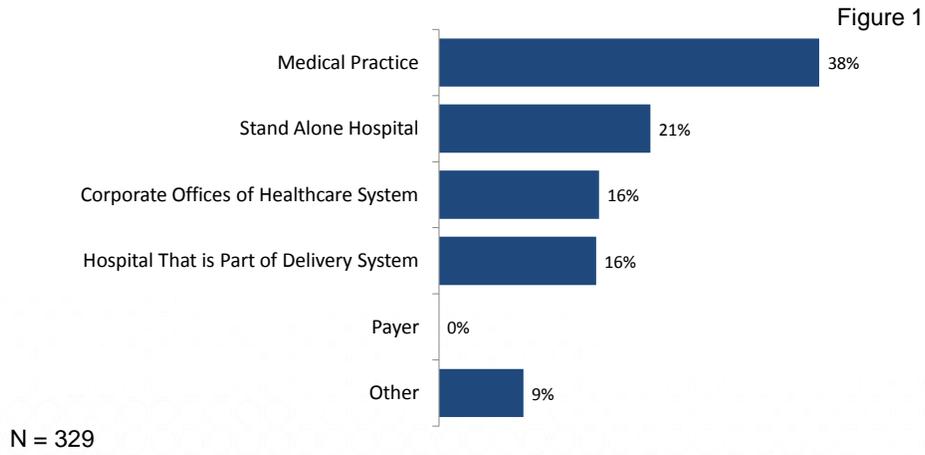
Level of Participating in Maintaining Privacy and Security

Figure 2

N = 203
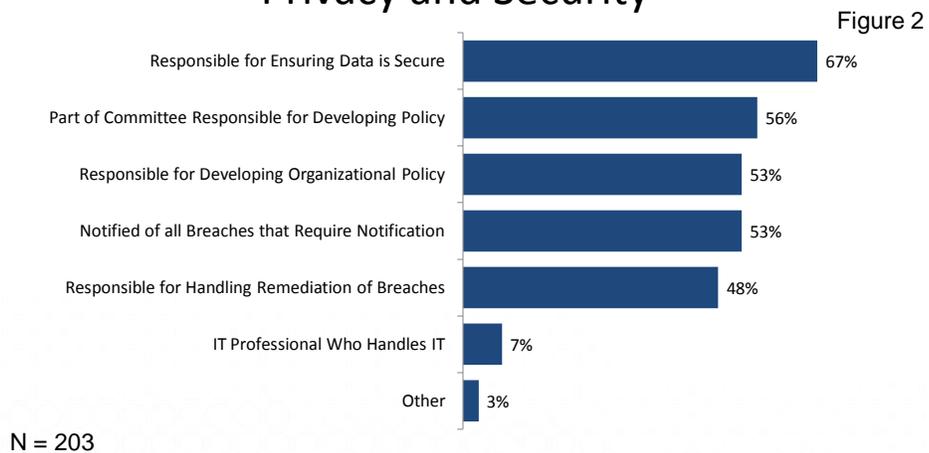
Appendix

Role in Development of Organization's Security Policy

Figure 3

Response	Percentage
Yes	100%
No	0%
Don't Know	0%

N = 126
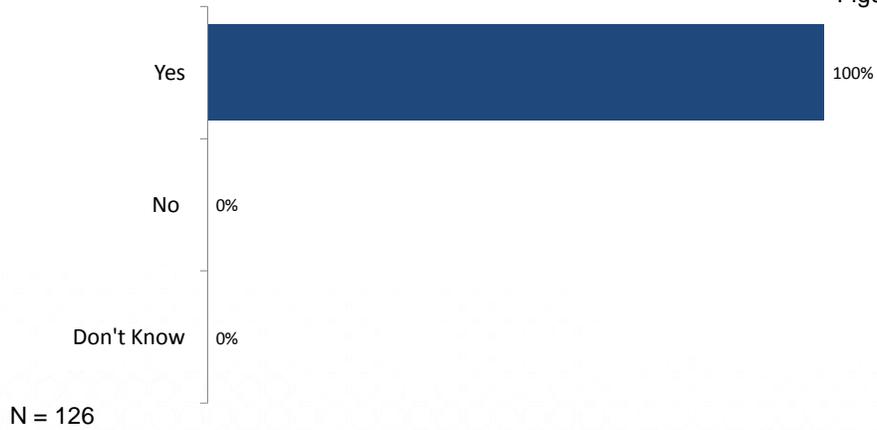
Participant Profile – Type of Medical Practice

Figure 4
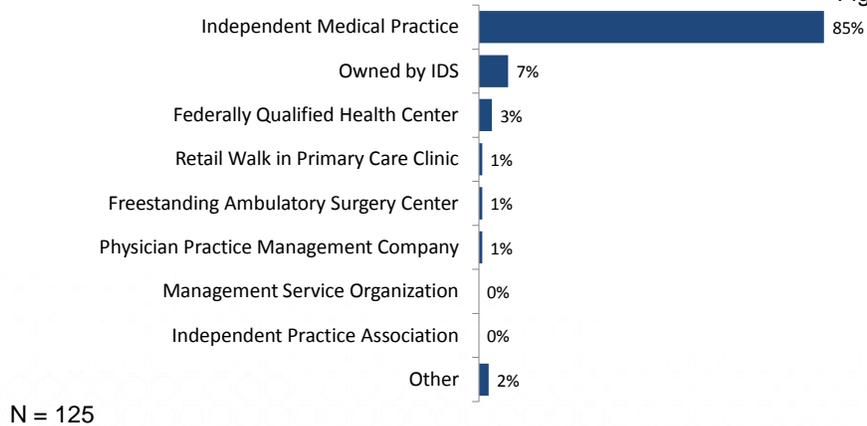
Practice Type	Percentage
Independent Medical Practice	85%
Owned by IDS	7%
Federally Qualified Health Center	3%
Retail Walk in Primary Care Clinic	1%
Freestanding Ambulatory Surgery Center	1%
Physician Practice Management Company	1%
Management Service Organization	0%
Independent Practice Association	0%
Other	2%

N = 125

Appendix

Participant Profile – Method of Storing Data at Medical Practices

Figure 5

Category	Percentage
EHR/EMR	90%
Document Imaging Management System	70%

N = 126
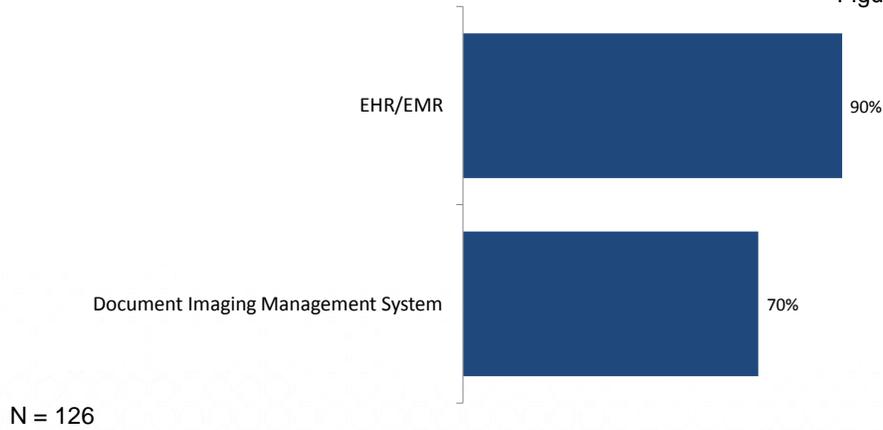
Participant Profile – Region

Figure 6

Region	Percentage
South Atlantic	17%
East North Central	16%
Mid Atlantic	11%
Mountain	11%
West North Central	10%
Pacific	10%
0.48	9%
East South Central	7%
New England	2%

N = 329
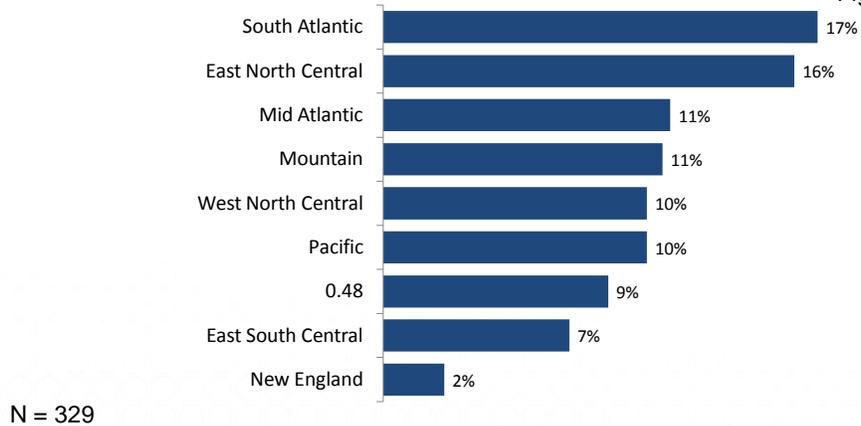
Appendix

Participant Profile – Title

Figure 7

Title	Percent
Chief Information Officer	37%
Chief Security Officer	18%
VP of Information Systems	7%
Director of IT	6%
Practice Administrator	3%
Chief Privacy Officer	1%
Clinician	1%
General Counsel	0%
Other	27%

N = 203

Percent of IT Budget Dedicated to Information Security

Figure 8

Budget Percent	Percent
Less than One Percent	18%
One to Three Percent	35%
Four to Six Percent	16%
Seven to 12 Percent	3%
More than 12 Percent	4%
Don't Know	23%

N = 203
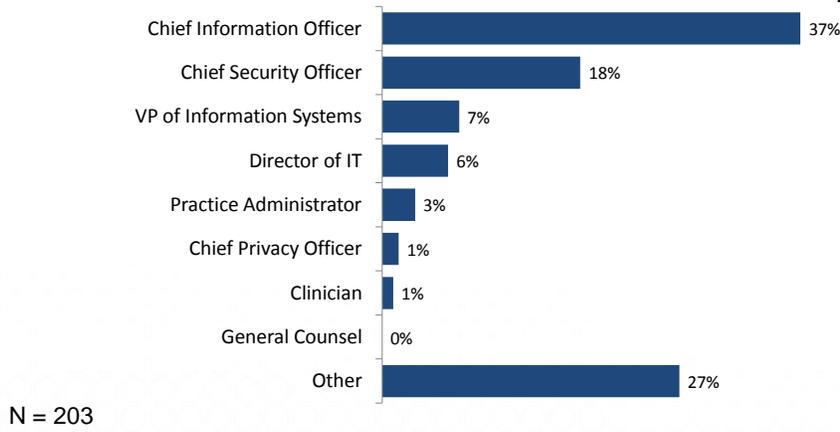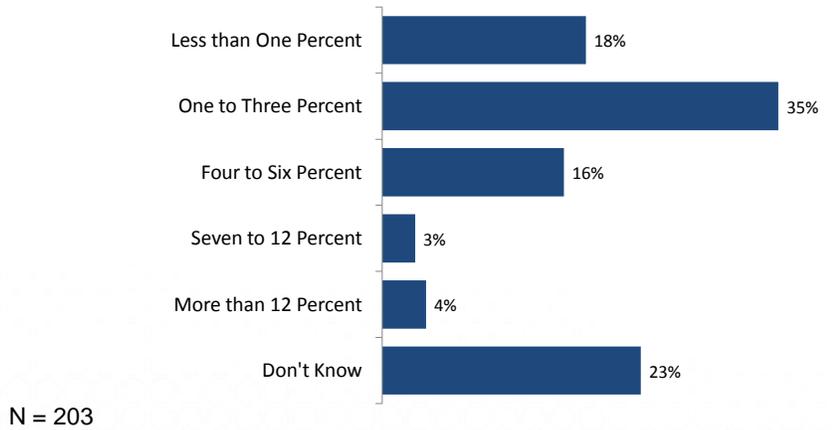
Appendix

Change in Percent of IT Budget Dedicated to Information Security

Figure 9

- Increased — 59%
- No Change — 32%
- Decreased — 2%
- Don't Know — 7%

N = 329
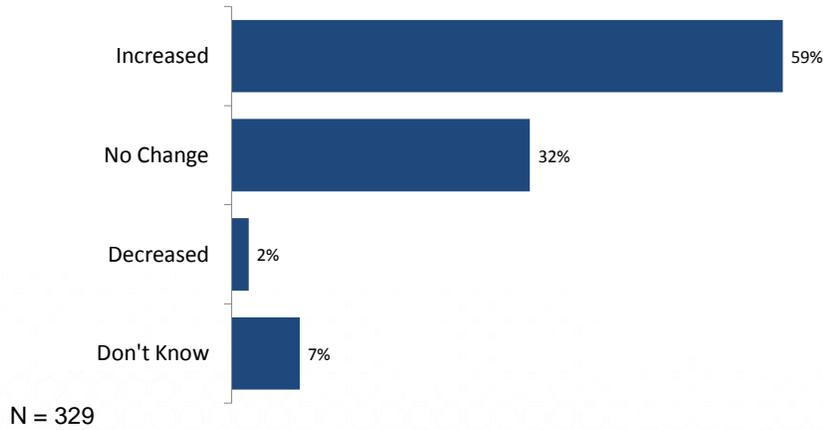
Impact of Federal Initiatives on Security Budget

Figure 10

- Resulted in Increase of Budget/Resources — 43%
- No Impact — 35%
- Resulted in Decrease in Budget/Resources — 15%
- Don't Know — 7%

N = 329
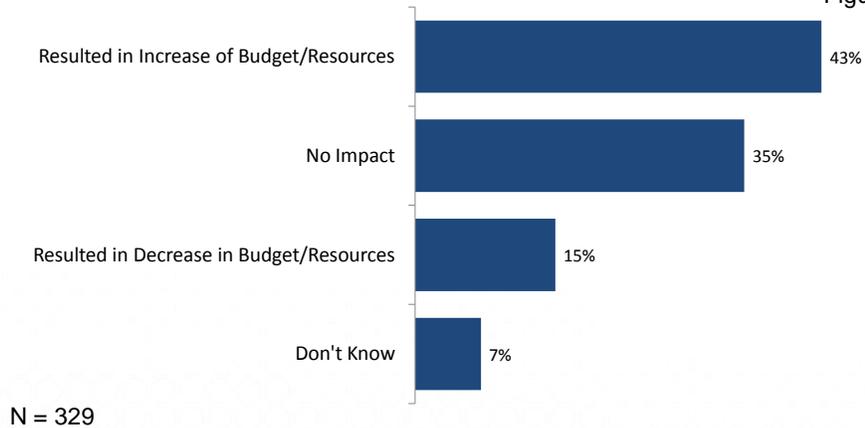
Appendix

Personnel Responsible for Securing Environment

Figure 11

Chief Security Officer — 21%
Other Full Time Staff — 29%
Part-Time Staff — 30%
Fully Outsourced — 9%
No Staff Responsible for Security — 9%
Don't Know — 2%

N = 329
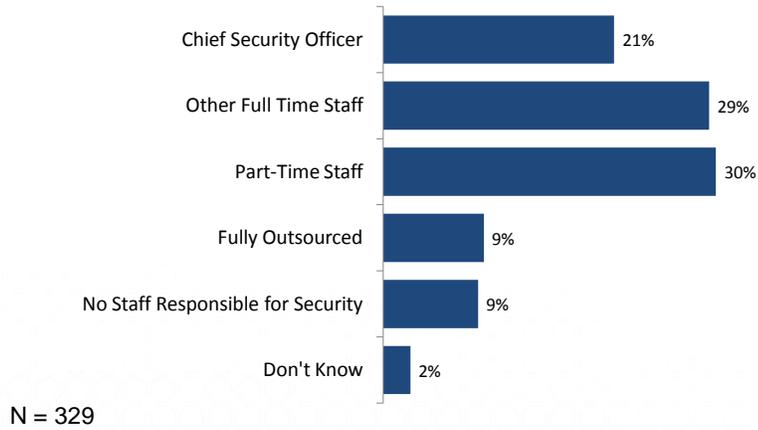
Frequency of Conducting a Formal Risk Analysis

Figure 12

Every Six Months — 8%
Annually — 49%
Every Two Years — 21%
Every Three Years — 2%
As Needed — 1%
Other — 9%
Don't Know — 10%

N = 270
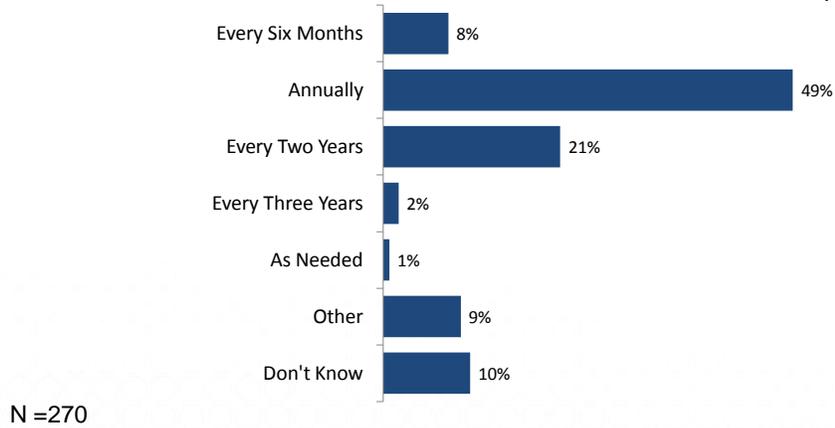
Appendix

Uses for Risk Analysis Data

Figure 13

Category	Percent
Use Risk Analysis to Determine Which Security Controls to Put Into Place	83%
Identify Area Where Lack of Security Controls Pose a Risk	67%
Identify Area Where Lack of Security Policies/Procedures Pose a Risk	62%

N = 180
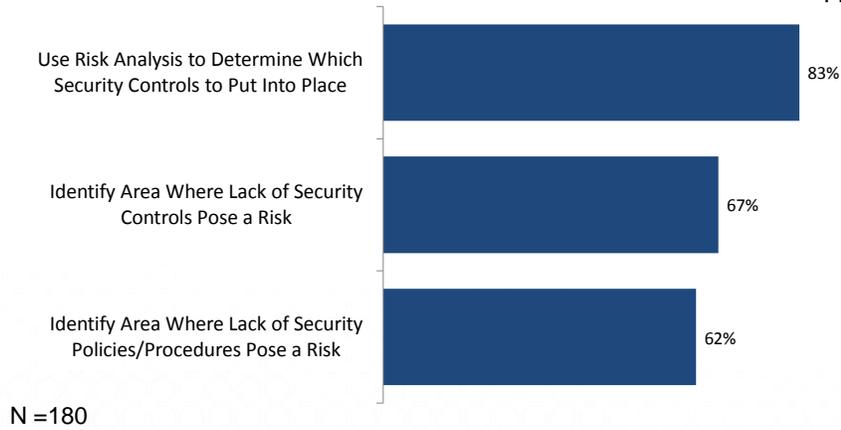
Length of Time Needed to Correct a Deficiency by Revising Security Controls

Figure 14

Category	Percent
Less than Six Months	37%
Six Months to One Year	33%
More than One Year	19%
Risk Hasn't Been Corrected	7%
Don't Know	5%

N = 120
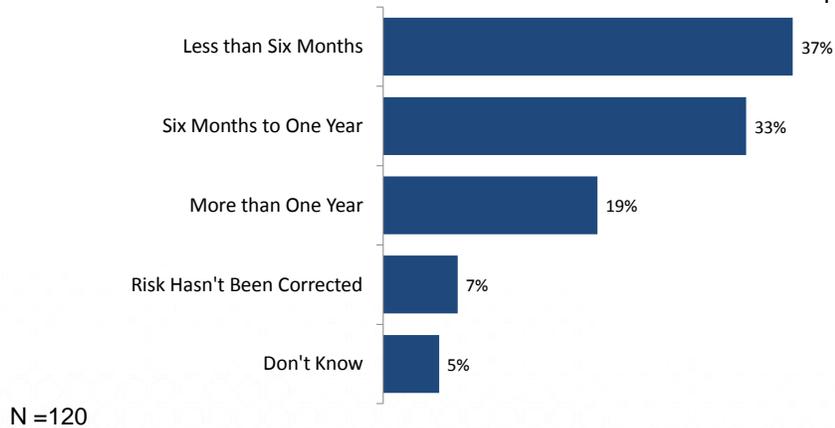
Appendix

Length of Time Needed to Correct a Deficiency by Revising Policies/Procedures

Figure 15

Category	Percentage
Less than Six Months	50%
Six Months to One Year	30%
More than One Year	13%
Risk Hasn't Been Corrected	6%
Don't Know	0%
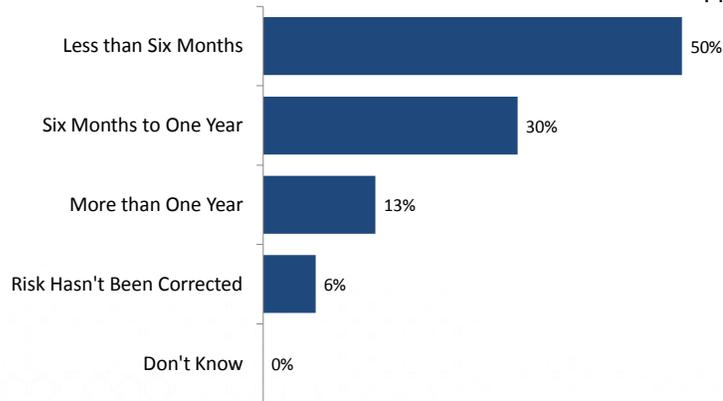
N =112

Method for Controlling Organizational Access to Patient Information

Figure 16

Category	Percentage
Role-Based Access	67%
User-Based Access	65%
Group-Based Access	19%
Location-Based Access	17%
Rule-Based Access	8%
Other	1%
Don't Know	0%
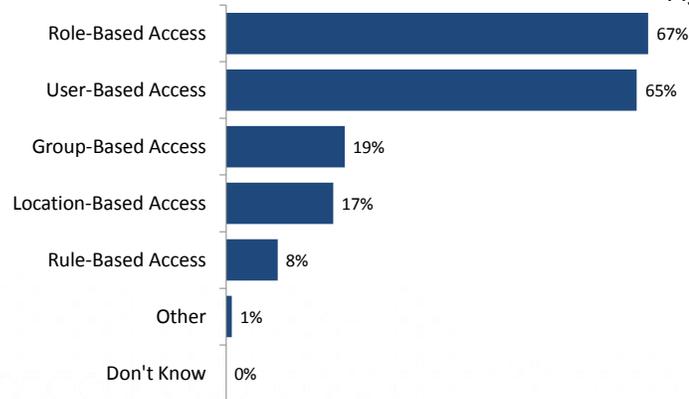
N =329

Appendix

Means by Which Organizations Provide Electronic Information to Patients

Figure 17

Means	Percentage
CD	56%
Web Portal	38%
Secure/Encrypted E-Mail	33%
USB (Thumb Drive)	19%
PHR Hosted by 3rd Party	6%
Unecrypted E-Mail	4%
Other	2%
Don't Know	0%

N =206
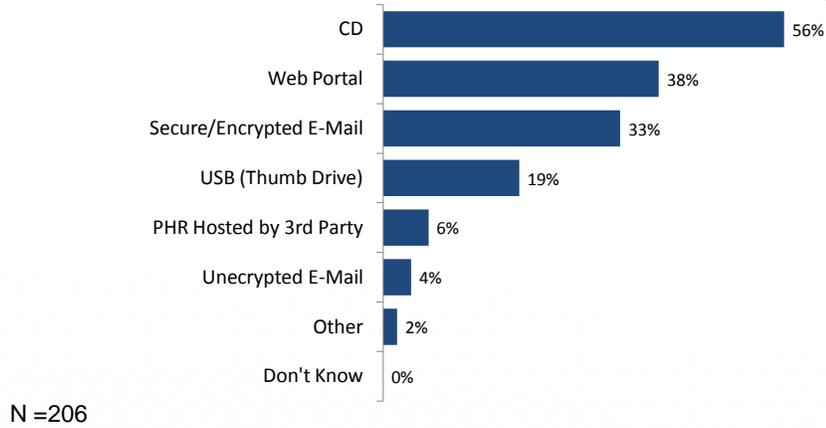
Method of Controlling Access to Websites/Portals Offered to Patients

Figure 18

Method	Percentage
Patient Given Unique Login Password	89%
Patient Uses Hard Token	5%
Patient Uses Biometric	2%

N =133
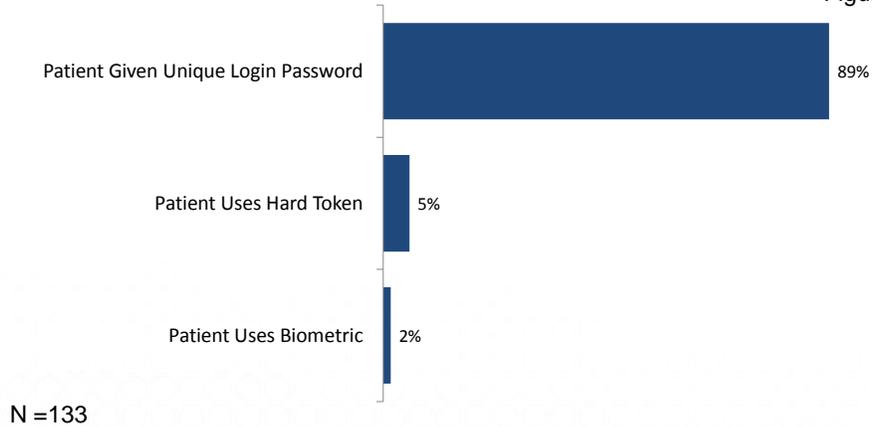
Appendix

Types of Systems From Which Data is Collected and Analyzed

Figure 19

System	Percentage
Firewall Log	84%
Servers	81%
Applications	73%
Intrusion Detection Systems	63%
Network Devices	60%
Billing Systems	37%
Practice Management Systems	36%
Case/Medical Management Systems	23%
Managed Security Service	20%
Additional Storage Devices	14%
Enrollment Systems	13%
Other	4%
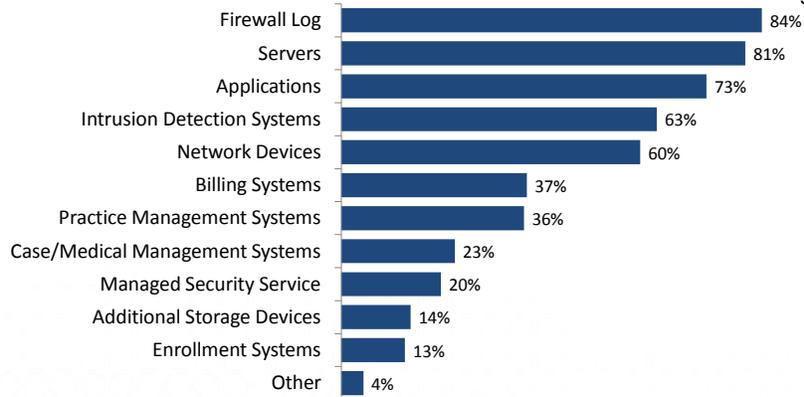
N =181

Events Captured by Audit Log Data

Figure 20

Event	Percentage
Clinician Access to Data	67%
Security Critical Events	64%
Non-Clinician Access to Data	64%
Patient Access to Data	18%
Other	3%
Don't Know	11%
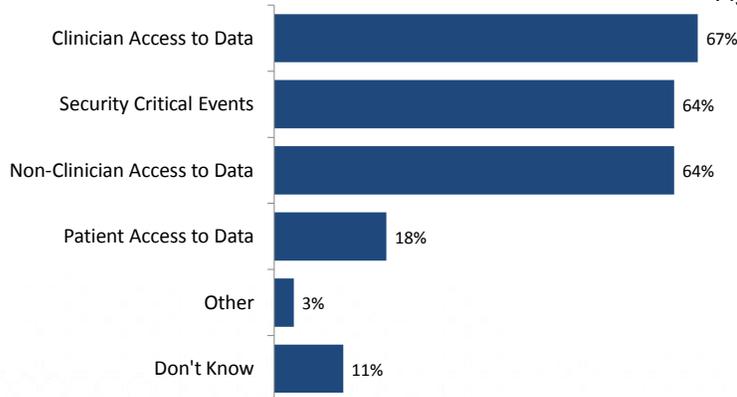
N =319

Appendix

Use of Audit Log Data

Figure 21

Category	Percentage
Policy Compliance Monitoring	72%
System Activity Monitoring	69%
Intrusion Detection	64%
Provide Accounting of Disclosure to Patients	46%
None of the Above	3%
Other	2%
Don't Know	6%
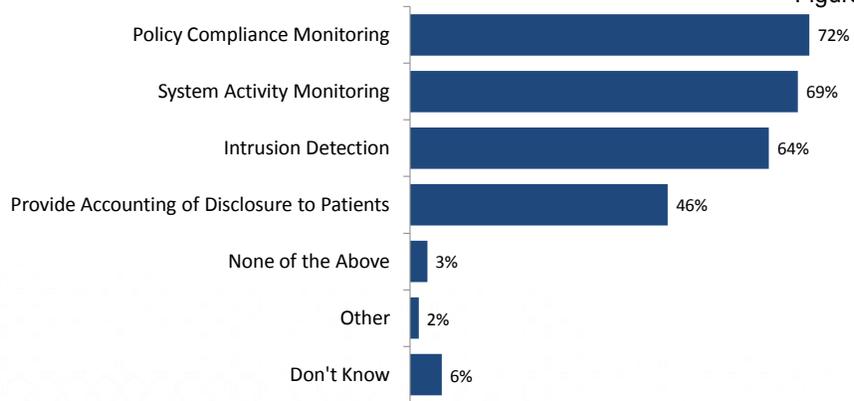
Plan in Place to Respond to Threats or Security Breaches

Figure 22

Category	Percentage
Policies in Place	71%
Currently Developing Plans	25%
No Plans in Place	3%
Don't Know	2%
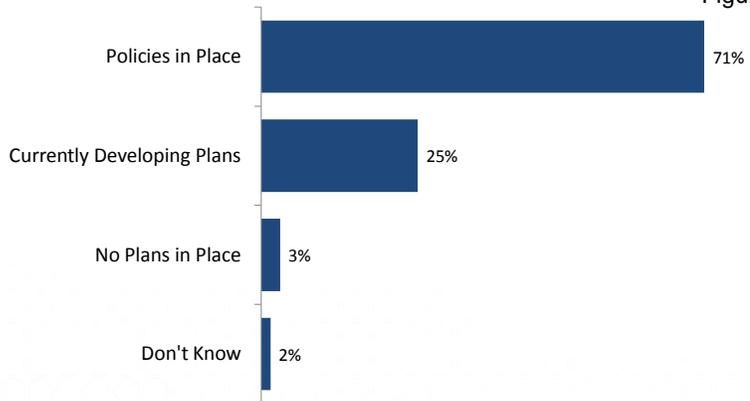
N =329

APPENDIX

Means for Measuring Success of Security Controls in Place

Figure 23

Category	Value
Number of Detected Security Incidents	74%
Reduced Risk Exposure	73%
Return on Investment	8%
Other	5%

N =106

Existing Data Sharing Relationships

Figure 24

Category	Value
Other Entities in Corporate Organization	66%
Third Party Service Provider	50%
State Government Entities	40%
Other Non-Corporate Entities	39%
Public Health Entities	29%
Federal Government	26%
Local Government Entities	24%
Practices/Hospitals Outside State	19%
HIEs	19%
PHR Vendors	11%
NHIN-Facilitated Data Exchange	7%
Other	2%

N =329

APPENDIX

Future Data Sharing Relationships

Figure 25

Category	Percentage
HIEs	62%
Other Non-Corporate Local Entities	45%
Entities Outside State	45%
Public Health Entities	43%
PHR Vendors	43%
NHIN-Faciliated Data Exchange	40%
Federal Government	34%
State Government Entities	34%
Local Government Entities	32%
Third Party Service Providers	19%
Other Corporate Entities	16%
Other	6%
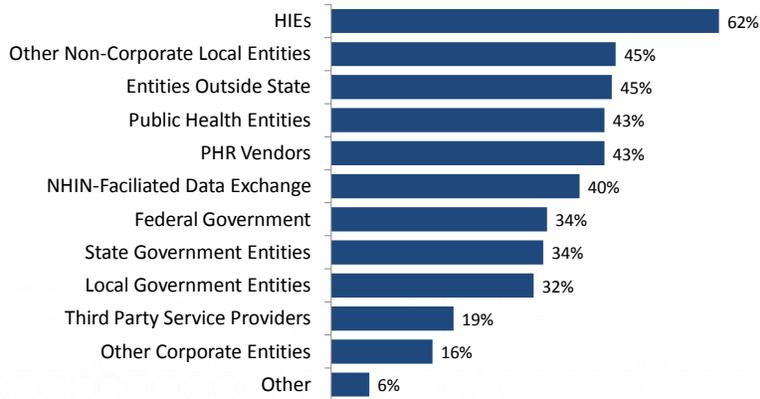
N =329

Use of Security Technologies – Top Ten

Figure 26

Category	Percentage
Firewalls	99%
User Access Controls	95%
Audit Logs of Each Access to Patient Heatlh Records	83%
Off-Site Storage	76%
Disaster Recovery	76%
Wireless Security Protocols	71%
Electronic Signature	66%
Data Ecryption (Transmission)	65%
E-Mail Encryption	58%
Data Encryptions (Storage)	54%

N =329

Percent of Data on Laptop Computers that is Encrypted

Figure 27

None	25%
Less than 10 Percent	5%
10 to 24 Percent	5%
25 to 49 Percent	3%
50 to 74 Percent	5%
75 to 99 Percent	12%
100 Percent	29%
Don't Know	16%

N =329

Percent of Data on Desktop Computers that is Encrypted

Figure 28

None	42%
Less than 10 Percent	13%
10 to 24 Percent	3%
25 to 49 Percent	3%
50 to 74 Percent	3%
75 to 99 Percent	4%
100 Percent	14%
Don't Know	18%

N =329

APPENDIX

Percent of Data on Servers that is Encrypted

Figure 29

Category	Percent
None	35%
Less than 10 Percent	9%
10 to 24 Percent	3%
25 to 49 Percent	3%
50 to 74 Percent	4%
75 to 99 Percent	6%
100 Percent	18%
Don't Know	20%

N =329

Percent of Data on Back Up Tapes that is Encrypted

Figure 30

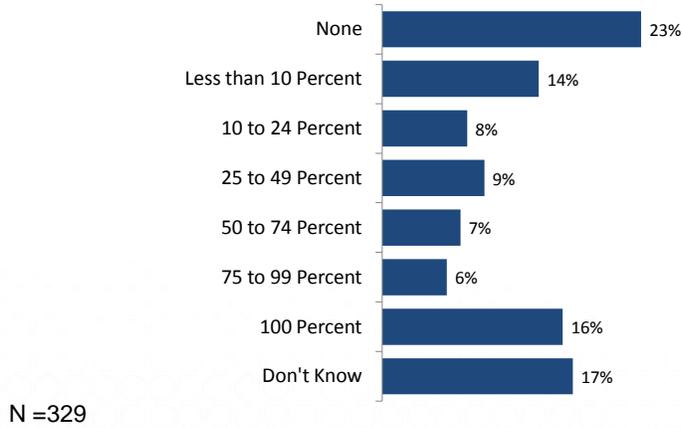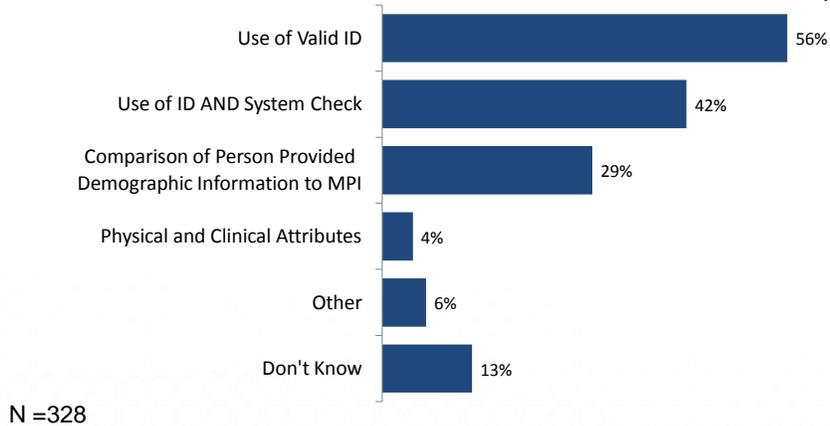| Category	Percent
None	31%
Less than 10 Percent	3%
10 to 24 Percent	2%
25 to 49 Percent	3%
50 to 74 Percent	4%
75 to 99 Percent	5%
100 Percent	30%
Don't Know	23%

N =329
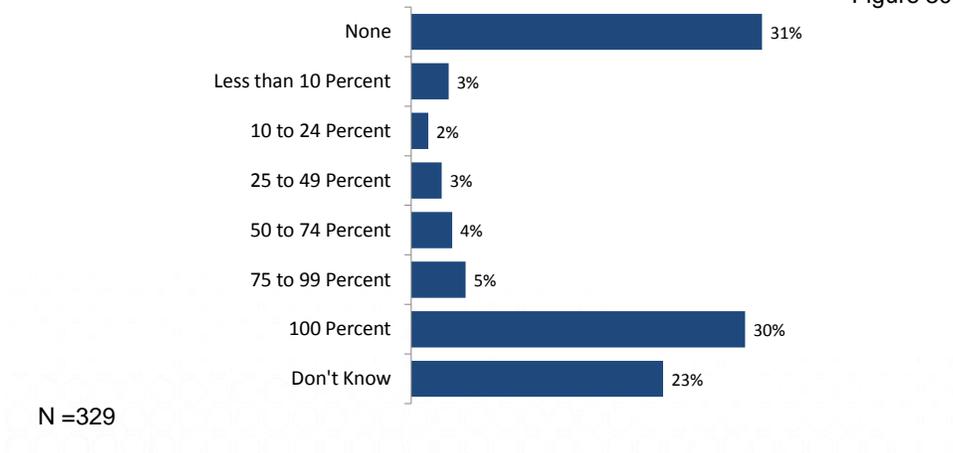
APPENDIX

Percent of Data on E-Mails that is Encrypted

Figure 31

N =329

Method of Proving Patients' Identities

Figure 32

N =328

APPENDIX

Method for Ongoing Validation at Subsequent Visits

Figure 33

- Assign Unique Identifiers — 62%
- Facility-Issued ID Cards — 21%
- Facility-Issued Smart Card — 9%
- Finger Print — 1%
- Iris Recognition — 1%
- None — 5%
- Other — 4%
- Don't Know — 18%

N =201
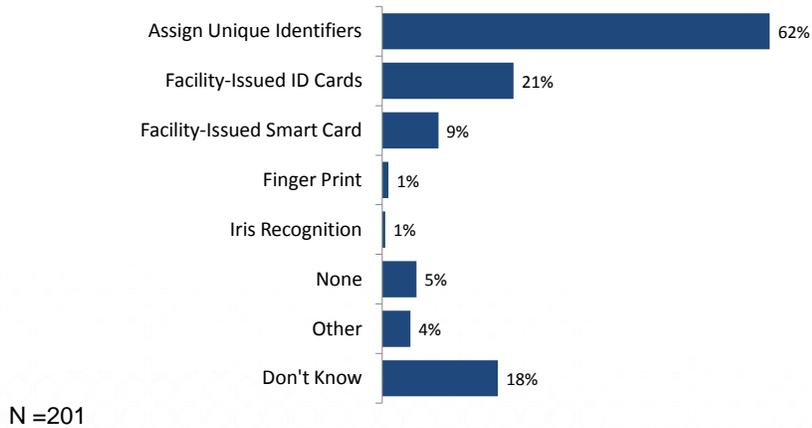
Method for Identifying Duplicates within MPI

Figure 34

- Formal Reconcilliation Process with Staff — 49%
- Informal Manual Process Only — 29%
- Don't Have a Process — 3%
- Don't Maintain an MPI — 4%
- Don't Know — 14%

N =201
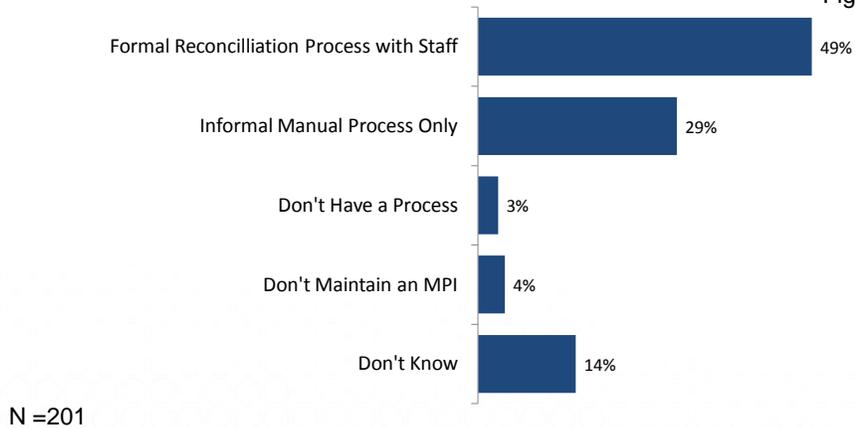
APPENDIX

Items Stored in Electronic Health Record

Figure 35

Alphanumeric Demographic Data	90%
Analog/Scanned or Digital Photograph	60%
Alphanumeric Digial Representations	24%
None of the Above	0%
Don't Have an EHR	6%
Other	1%
Don't Know	4%

N =201

Has Organization Had One Case of Medical Identity Theft

Figure 36

Yes	14%
No	66%
Don't Know	20%

N =326

Number of Cases of Medical Identity Theft

Figure 37

One	36%
Two	15%
Three	26%
Four	4%
Five	6%
Six	4%
Seven	0%
Eight	0%
Nine	0%
Ten	2%
More than Ten	6%

N =47