

NOVEMBER 3, 2010

2010 HIMSS Security Survey

sponsored by Intel



2010 HIMSS Security Survey

Sponsored by Intel

Final Report

November 3, 2010

Now in its third year, the 2010 HIMSS Security Survey, sponsored by Intel reports the opinions of information technology (IT) and security professionals from healthcare provider organizations across the U.S. regarding key issues surrounding the tools and policies in place to secure electronic patient data at healthcare organizations. This year, the study was supported by Medical Group Management Association (MGMA) to encourage additional representation in the medical group and ambulatory space. The study was designed to collect 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. This year, we've added a series of questions to evaluate how healthcare organizations are handling patient identity issues.

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. About Symantec
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. Participant Profile—Type of Medical Practice
4. Participant Profile—Medical Practice Specialty
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. Components of a Formal Risk Analysis
14. Uses for Risk Analysis Data
15. Length of Time Needed to Correct a Deficiency by Revising Security Controls
16. Length of Time Needed to Correct a Deficiency by Revising Policies/Procedures
17. Method for Controlling Organizational Access to Patient Information
18. Access to Electronic Data by Patients, Surrogates or Designated Others
19. Types of Data Patients, Surrogates, Designated Others can Access
20. Means by Which Organizations Provide Electronic Information to Patients
21. Method of Controlling Access to Health Websites/Web Portals Offered to Patientsjul
22. Types of Systems from Which Data is Collected and Analyzed
23. Methods for Analyzing Log Information
24. Events Captured by Audit Logs
25. Use of Audit Log Data
26. Means by Which Accounting Disclosure is Made Available to Patients
27. Plan in Place to Respond to Threats or Security Breaches
28. Actively Determine of Cause/Origin of Security Breach
29. Means for Monitoring Success of Security Controls in Place
30. Means for Measuring Success of Security Controls in Place
31. Existing Data Sharing Relationships
32. Data Sharing Arrangements Require Use of Additional Security Tools
33. Use of Security Technologies
34. Percent of Data on Laptop Computers that is Encrypted
35. Percent of Data on Desktop Computers that is Encrypted
36. Percent of Data on Servers that is Encrypted
37. Percent of Data on Back-up Devices that is Encrypted
38. Percent of Data on E-mail that is Encrypted
39. Method of Proving Patients' Identities
40. Method for Ongoing Validation at Subsequent Visits
41. Method for Identifying Duplicates Within MPI
42. Items Stored in Electronic Health Record
43. Has Organization Had One Case of Medical Identity Theft

1. Executive Summary

In July 2010, the Centers for Medicare and Medicaid Services (CMS) published the final rules on the Electronic Health Record Incentive Program six months after they published a Notice of Proposed Rulemaking. In this set of final rules, CMS identified a core set of 14 meaningful use objectives in which eligible hospitals (EH) and 15 core meaningful use objectives in which eligible professionals (EP) need to focus to qualify for incentive funds provided through the new CMS Medicare and Medicaid incentive program. Additionally, EHs and EPs must also focus on five of 10 menu set objectives to qualify for incentive funds. One of these rules specifically stipulates that eligible hospitals and eligible providers must protect electronic health information created or maintained by the electronic health record (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

Risk analysis is the best process for a healthcare organization to gain a complete understanding of its security profile—the threat environment, system vulnerabilities and overall risk exposure. Risk analysis is 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. HIPAA requires covered entities and business associates to “conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.” The rule further states that “the required risk analysis is also a tool to allow flexibility for entities in meeting the requirements of this final rule...”¹

Results from the 2010 HIMSS Security Survey, sponsored by Intel, and supported by MGMA, indicated that three-quarters of all respondents reported that they perform a risk assessment at their organization. This is reflected in the assessment of 272 IT and security professionals of their own organization’s readiness for today’s risks and security challenges. While this is similar to the percentage reported last year, this year’s study has a greater representation of medical practices and there is a clear difference in the percent of respondents that indicated they conducted a risk analysis. Respondents working for medical practices were twice as likely to report that their organization does *not* conduct a risk analysis compared to those that work at a hospital (33 percent compared to 14 percent).

The meaningful use criteria states that not only are organizations required to conduct a risk analysis, but they must also correct deficiencies identified during the risk analysis process. Overall, a high percentage of those that *are* conducting a risk assessment reported using this information to determine which security controls should be put into place at their organizations. The risk assessment results were also used by many organizations to identify gaps in existing security controls, policies and/or procedures, and, as a result of the risk assessment, organizations were able to actively take steps to correct deficiencies and the survey data serves to emphasize the important role and value that ongoing security risk analysis can play in protecting health data.

¹ Federal Register, Department of Health and Human Services. 45 CFR Parts 160, 162, and 164, Health Insurance Reform: Security Standards; Final Rule <http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf>

Key survey results include:

Maturity of Environment: Respondents characterized their environment at a middle rate of maturity, with an average score of 4.43 on a scale of one to seven, where one is not at all mature and seven is a high level of maturity.

Security Budget: Approximately half percent of respondents reported that their organization spends three percent or less of their organization's IT budget on information security. However, while this was consistent with what was reported last year, many respondents indicated that their budget actually increased in the past year, primarily as a result of federal initiatives. There is little difference in response in this area by organization type.

Formal Security Position: Slightly more than half (53 percent) of respondents reported they have either a CSO/CISO or full-time staff in place to handle their organizations' security function. Those working for a hospital were more likely to report that they had a CSO/CSIO in place compared to individuals working for medical practices. Also, while 17 percent of respondents working for medical practices indicated that they handled their security function exclusively using external resources. None of the respondents from the hospitals reported that they used external resources exclusively.

Risk Analysis: Slightly more than half of respondents (59 percent) that reported that their organization conducts a formal risk analysis indicated that this type of analysis is conducted annually. Susceptibility to internal threats and external threats are nearly universally included in the risk analysis.

Patient Data Access: Surveyed organizations most widely use user-based and role-based controls to secure electronic patient information. More than half of respondents from hospital organizations reported that they used two or more types of controls to manage data access, compared to 40 percent of respondents from medical practices. Approximately half of respondents reported that their organization allows patients/surrogates to access electronic patient information.

Management of Security Environment: Nearly all respondents reported that their organization actively works to determine the cause/origin of security breaches and two-thirds reported having a plan in place for responding to threats or incidents related to a security breach. Respondents working for the hospital organizations in this sample were more likely to report that they worked to determine the cause/origin of security breaches than were their counterparts at medical practices.

Security in a Networked Environment: Approximately 85 percent of respondents reported that their organization shares patient data in an electronic format. Data is most frequently shared with third party providers, state government, third party providers and other facilities within the corporate organization. While respondents from hospitals are somewhat more likely to report (83 percent) that they will share data in the future than are those from medical practices (77 percent), the likelihood of data sharing in the future is high among both groups.

Future Use of Security Technologies: Mobile device encryption, e-mail encryption and single sign on and were most frequently identified by respondents as technologies that were not presently installed at their organization but were planned for future installation. Respondents from hospitals that were not presently using these

technologies are more likely to report installing them in the future, compared to respondents in medical practices.

Patient Identity: Half of respondents indicated that they validate patient identity by both requiring a government/facility-issued ID and checking the ID against information in the master patient index. A similar percent reported that they have a formal process for reconciling duplicate records in their master patient index.

Medical Identity Theft: One-third of respondents reported that their organization has had at least one known case of medical identity theft at their organization. Those working for a medical practice were much less likely to report that an instance of medical identity theft occurred at their organization (17 percent), when compared to those working for a hospital organization (38 percent).

In summary, undertaking a formal risk analysis and then using the outcomes to change use of controls and make modifications within policies and procedures is required to qualify for Stage One meaningful use incentives. At present, one-quarter of the sample population would not qualify for meaningful use. In addition, establishing a robust security environment is crucial as hospitals and medical practices increasingly share information outside of their organizations.

2. Profile of Survey Respondents

A total of 272 responses were received for this survey. Data was collected via a web-based survey between September 10 and October 8, 2010. The 2009 study had 196 respondents and the 2008 survey had 155 respondents.

In order to qualify to participate in this research, respondent had 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 responsible for ensuring that our data is secure on a day to day basis;
- I am part of a committee that is responsible for developing the organization’s policy on privacy and security;
- 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 requires notification.

Respondents were most likely to indicate that they are responsible for ensuring that their organization’s data is secure on a day-to-day basis (59 percent). Another 56 percent of respondents indicated that they sit on a committee that is responsible for developing the organization’s policy on privacy and data security. Nearly half (47 percent) reported responsibility for developing the organization’s policy on privacy and data security, while 42 percent reported that they held responsibility for remediation of a security breach.

More than half of the respondents (57 percent) answered “yes” to two or more 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 272 responses on which the analysis in this report is based.

One-third of respondents indicated that they are a senior Information Technology (IT) executive at their organization. Specifically, 27 percent of respondents indicated that they are the Chief Information Officer at their organization. Another ten percent reported their title to be Vice President of IT/IS. Another 10 percent reported their title to be at the Director-level in the IS department. Approximately 12 percent of respondents reported their title to be Chief Security Officer and three percent indicated their title is Chief Privacy Officer. Six percent reported a title that can be categorized as “other executive”, which includes titles such as General Counsel, CMIO or Chief Clinical Officer, CFO or Chief Technology Officer. Fourteen (14) percent of the respondents reported their title to be either Practice Administrator or Clinician. The remaining 19 percent of respondents reported their title as “other”, which includes a wide variety of IT and security titles. See Figure One.

Participant Profile – Title

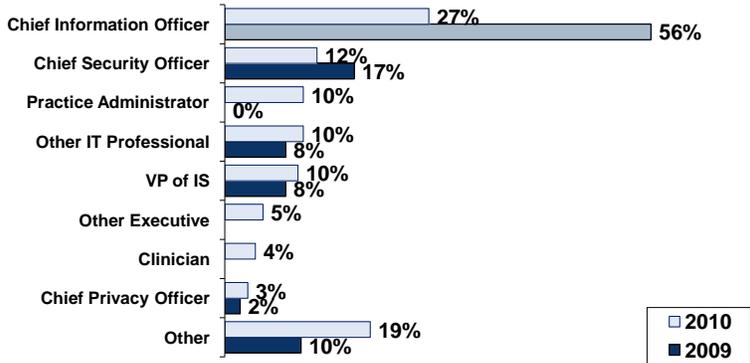


Figure One. Participant Profile—Title

Nearly half of respondents reported working for either a stand-alone hospital (29 percent) or a hospital that is part of a delivery system (17 percent). Fifteen percent work for the corporate offices of a healthcare system. Approximately one-quarter of the respondents (23 percent) reported working for a medical practice. The remaining respondents work for a variety of healthcare organizations, including payers, home health agencies, military healthcare facilities or health information exchanges (HIEs). For the purposes of analysis, the sample will be divided into three groups, those working for hospitals, those working for medical practices and those working for other types of organizations. Data in this research will be examined for statistically significant differences in these areas and will be noted as they emerge. See Figure Two.

Participant Profile – Organization Type

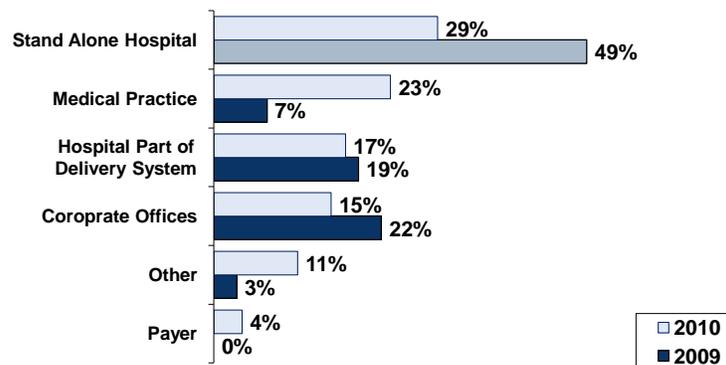


Figure Two. Participant Profile—Organization Type

Additional data was also collected on the medical practices. In order for a medical practice to be included in this research, they were required to store information in an electronic format. Nearly all respondents (91 percent) reported that their organization had either an electronic medical record (EMR) or an electronic health record (EHR). The remaining nine percent of respondents reported that their organization used a document imaging management system (DIMS) to store data electronically.

On average, these organizations have 57.54 physician FTEs (median 11.25). Three-quarters of the respondents (73 percent) at the medical practices characterized themselves as an independent medical practice. Another six percent classified the practice as a federally qualified health center (FQHC²) and five percent were classified as a retail walk-in primary care clinic. The remaining practices include hospital-owned facilities, management services organizations, physician practice management companies, independent practice associations.

By service offered, one-quarter of the respondents at medical practices characterized their practice as a multispecialty practice that offered both primary and specialty care. Another eight percent of respondents noted that their practice was a multispecialty organization that offered only specialty care. Other types of practices represented in this study include cardiology, family practice, orthopedic surgery, general pediatrics, OB/GYN, endocrinology, gastroenterology, and nephrology.

The greatest percentage of respondents (16) comes from the South Atlantic region. This is followed by the East North Central region (15 percent). The West North Central and

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.

Pacific regions each had 13 percent of the respondents in the survey. The smallest number of respondents comes from New England (five percent).

3. General Information Security

Approximately half of respondents reported that their organization spends three percent or less of their organization's IT budget on information security; half of respondents noted that federal initiatives facilitated an increase in budget/resources for information security. Half of the survey respondents noted that they have a full-time resource, such as a Chief Security Officer, in place and only five percent reported that their entire security function is handled externally. Approximately three-quarters of respondents noted that they conduct a formal risk analysis, and two-thirds indicated that this risk analysis is conducted at least annually.

Respondents were asked to identify the amount of their organization's overall IT budget that is dedicated to information security. One-quarter of respondents (27 percent) reported that they spent between one and three percent of the overall IT budget on security. Another 19 percent noted that they spent less than one percent of their overall IT budget on information security. Sixteen (16) percent reported that they spent four to six percent of their IT budget on information security. Twelve percent reported that they spend seven percent or more of the IT budget on information security. This is consistent with data from 2009, when 40 percent of respondents reported that their organization's spent between one and three percent of the overall IT budget on information technology.

New to the study in 2010 was a question as to whether or not the percent of the IT budget dedicated to information security has changed in the past year. Half of survey respondents (53 percent) noted that the amount of the IT budget dedicated to security has increased in the past year. Another third noted that the amount remained unchanged and only two percent reported a decrease in the percent of IT dollars allocated to information security.

For the first time in 2010, respondents were also asked to identify the impact that federal initiatives such as the EHR incentive program, ICD-10, and HIPAA 5010 electronic transactions had on budget/resources for information security. Respondents were most likely (43 percent) to report that these federal initiatives facilitated an increase in budget/resources from information security. Another third (33 percent) reported that the amount of budget/resources dedicated to information security was unchanged as a result of these federal initiatives. However, 14 percent reported that these initiatives diverted budget/resources from being spent on information security at their organizations. There was relatively little difference in how respondents at different organization types responded to this question; 39 percent of those at medical practices reported that they had increased the budget/resources dedicated to information security, compared to 44 percent of respondents at hospital-based organizations. This difference is not statistically significant.

Percent of IT Budget Dedicated to Information Security

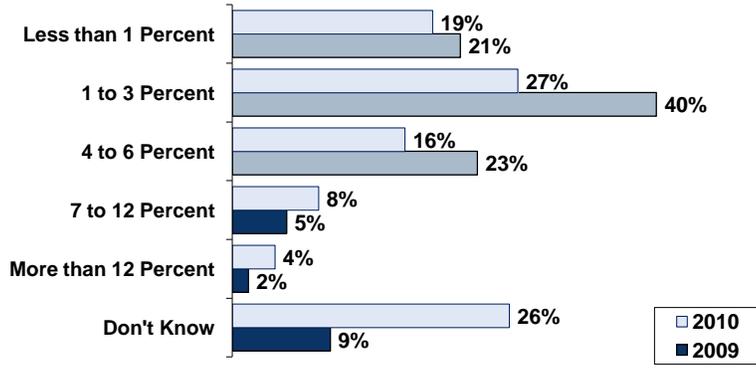


Figure Three. Percent of IT Budget Dedicated to Information Security

In the 2009 survey, respondents were asked to identify whether or not their organization has either a formally designated CISO (Chief Information Security Officer) or CSO (Chief Security Officer). In that research, more than half of survey respondents (58 percent) indicated that their organization did NOT have an individual with this title employed at their organization.

In the 2010 survey, the question was reframed to address how organizations allocate staff to their security functions. Slightly more than half of respondents (53 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. Another 21 percent of respondents indicated that they have only part-time staff allocated to information security.

By type of organization, those working for an organization characterized as a hospital were more likely to report that they had a CSO/CSIO in place, when compared to those individuals working for medical practices. More specifically, one-third of respondents at a hospital organization reported that a CSO/CISO was in place at their organization compared to eight percent of respondents working for a medical practice.

A similar trend exists with regard to the presence of full-time staff. Fourteen (14) percent of respondents working for a medical practice noted that they have full-time staff responsible for information security. In comparison, 45 percent of respondents working for hospitals reported this to be the case.

This question also tested whether or not organizations are outsourcing any of their IT security function. Five percent of respondents indicated that they outsource the entire information security function; another 18 percent reported that they outsourced at least some portion of their security function. By organization type, 17 percent of respondents

working for medical practices indicated that they handled their security function exclusively using external resources. None of the respondents from the hospitals reported that they used external resources exclusively. Respondents working for medical practices were also twice as likely to report using a combination of internal and external resources when compared to those working for a hospital organization – (31 percent compared to 15 percent).

Respondents were also asked to identify how frequently their organization conducts a formal risk analysis to evaluate risks to patient data at their organization. About three-quarters of the total respondents (76 percent) reported that their organization does conduct a formal risk analysis. This is comparable to the 74 percent that reported this to be the case in the 2009 survey. Five 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 does not conduct a risk analysis compared to those that work at a hospital (33 percent compared to 14 percent).

The majority of respondents that reported that their organization conducts a formal risk analysis indicated that this type of analysis is conducted on an annual basis (59 percent). Another nine percent reported that they conduct a risk analysis once every six months. Nearly one-quarter (22 percent) conduct this type of analysis every other year. See Figure Four.



Frequency of Conducting a Formal Risk Analysis

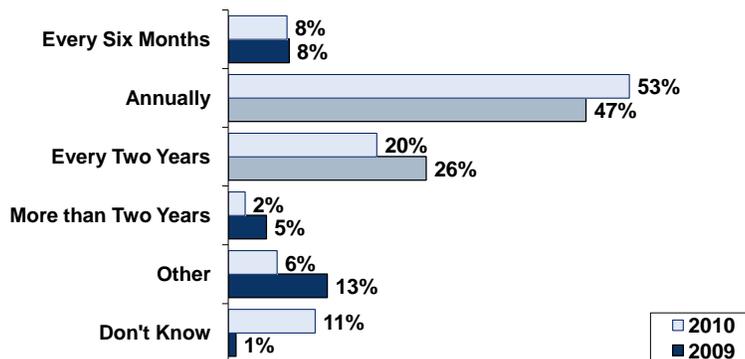


Figure Four. Frequency of Conducting a Formal Risk Analysis

Nearly all respondents (91 percent) indicated that internal threats are included as part of their organization’s formal risk analysis. A nearly identical percentage of respondents (90 percent) indicated that external threats are included as part of their organization’s formal risk analysis. These responses are similar to the data from 2009, where 91 percent of respondents indicated that internal threats were included in the formal risk analysis and 94 percent of respondents indicated that external threats were included in the formal risk analysis.

The frequency with which the other items are included in the formal risk analysis process are listed below.

- Compliance requirements (87 percent);
- Risk to the confidentiality of patient data (84 percent);
- Evaluation of the effectiveness of your organization's security controls (80 percent);
- Evaluation of the adequacy of your organizations policies/procedures (78 percent);
- Risks to the integrity of patient data (72 percent);
- Risks to the availability of patient data (68 percent);
- Evaluation of new opportunities to cost-effectively improve security (43 percent).

There are two areas in which respondents working for hospitals were more likely to include in a risk analysis than were those respondents working for a medical practice. These are internal threats (94 percent compared to 81 percent) and compliance requirements (91 percent compared to 77 percent). The differences in both areas are statistically significant.

Respondents were also asked for whether or not they used their risk analysis to either determine which security controls to put into place or to identify gaps in the use of either security controls or security policies and/or procedures. In order to make sure that all respondents were approaching this question from a consistent perspective, a definition of a security control was offered. For the purposes of this research, a security control was referred to as safeguards or countermeasures used to avoid, counteract or minimize security risks. We also offered three categories of security controls and provided a definition of each. These are:

- **Physical controls** – (e.g. fences, doors, locks and fire extinguishers)
- **Administrative controls** – (e.g. incident response processes, management oversight, security awareness and training)
- **Technical controls** – (e.g. user authentication (login) and logical access controls, antivirus software, firewalls).

A high percent of respondents (84 percent) noted that they used their risk analysis process to determine which security controls should be put into place at their organization. There are no statistically significant differences by organization type in this area.

Among those respondents who reported that their organization conducted a formal risk analysis, approximately two-thirds of respondents (70 percent) noted that a lack of effective security controls that pose a serious or significant risk to patient information was identified during the risk analysis. Forty-three (43) percent of the respondents who identified a gap in their security controls indicated that it took them less than six months to rectify the gap; another third (33 percent) indicated that it took them between six months and one year to correct the deficiency. Only five percent indicated that the risk identified at the time of the assessment has not yet been corrected.

Two-thirds of respondents (66 percent) that conducted a formal risk analysis indicated that they identified an area in which there was a lack of adequate policies and/or procedures that posed a serious or significant risk to patient information. Half of those respondents identifying a deficiency in this area indicated that the issue was corrected

within six months. Another third (30 percent) indicated that the issue was fixed within six months to one year. Six percent indicated that the issue is still unresolved.

At present, on a scale of one to seven, where one is not at all mature and seven is very mature, respondents rated the maturity of their systems as a 4.43. This is nearly identical to the score of 4.27 that was recorded in the 2009 survey. A score of one was identified by only four percent of respondents and a score of seven was identified by five percent of respondents.

4. Patient Data Access

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, with user-based and role-based controls being the most widely used. Slightly more than half of respondents reported that their organization allows patients and/or their surrogates to access information in an electronic format.

Respondents were asked to identify how their organizations controlled employee access to electronic patient information. Indeed, all organizations that maintain electronic patient information also reported that they use at least one method for controlling access to electronic patient information, such as user-based, role-based or rule-based access. This is consistent to what was reported in the past. Approximately 44 percent of respondents reported that their organization uses only one method of controlling access and another 22 percent reported that their organization uses two methods of control. The remaining respondents reported that they use three or more methods of controlling access to data. This is very consistent with what was reported in the past.

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 (60 percent compared to 40 percent).

The most frequently reported means of controlling employee access to patient information is the use of user-based controls, which limits access to data based on a person's knowledge of user-based account credentials. This option was selected by 74 percent of respondents. Selected by 71 percent of respondents are role-based controls. For the purposes of this research, role-based controls are defined as a person being able to access patient information based on their job/role type, such as clinician or nurse. The majority of respondents (97 percent) use one or both of these methods of controlling access to patient information.

The other means of controlling access to patient data tested in this research are group-based access, location-based access and rule-based controls. These methods are used much less frequently. Among these three, 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 is used most frequently; approximately one-third of respondents note this type of control is in place at their organization. Another quarter (23 percent) reported that they use location-based access, which was defined in this research as those who work on a particular floor or unit. Finally, ten percent use rule-based access, which limits access using an if/then statement. These are all consistent with the information reported in the 2009 survey.

Slightly more than half of respondents (59 percent) reported that they provide information electronically stored by their organization in an electronic format to patients/surrogates/designated others. This represents an increase from the half of respondents that reported this to be the case in 2009.

The types of data that are provided electronically that were tested in this research include high level clinical information (such as diagnoses or lab information), detailed clinical information (such as a clinicians note), financial/insurance information and/or scheduling information. In summary, among the respondents for which patients, surrogates or designated others were provided information electronically by their organization, 82 percent reported that they share high-level clinical information. Nearly three-quarters (70 percent) also reported that patients, surrogates or designated others could receive financial/insurance information. A similar percent (69 percent) reported that patients, surrogates and designated others can receive detailed clinical information. Scheduling information is less frequent, identified by 59 percent of those who reported that they permitted patients, surrogates and/or designated others to receive this type of information.

Respondents were most likely to report that they share information with a patient, when compared to surrogates or designated others; 88 percent of respondents that make electronic information available to patients, surrogates or designated others reported that they make this information available to patients (this is equal to 54 percent of the total sample population). Three-quarters of respondents noted that their organization makes this data available to designated others; two-thirds noted that they make information available to surrogates.

Finally, respondents were asked to identify *how* this type of electronic information is provided to patients, surrogates and/or designated others. Among the respondents who reported that they make this type of information available, the most frequently selected means of sharing this data is via a CD-Rom, which was identified by 54 percent of respondents. Forty-three percent of respondents noted that they share this information via a Web portal. The other choices offered in this study, as well as the percent of respondents that selected the choice, is shown below.

- Secure (encrypted) e-mail – (24 percent);
- USB thumb drive – (19 percent);
- Unencrypted e-mail – (2 percent);
- Personal Health Record offered by a Third Party – (2 percent).

In the 2009 study, respondents were asked to identify if their organization had implemented security controls on the health website/portal that was offered to patients. Nearly half indicated this was the case. This question was modified slightly this year, asking how the organization controls access to health websites/web portals offered to patients. Among those that allow access through a web portal, three-quarters (72 percent) of respondents noted that the patient is assigned a unique user id and login password. Three percent reported that the patients use a hard token; none of the respondents reported that individuals access this type of portal using a biometric device. A substantial portion (17 percent) reported that they don't have access controls that restrict access to health websites/web portals.

5. Access Tracking/Audit Logs

Audit logs are widely used among the healthcare organizations represented in this survey. Data from firewalls, application logs and server logs are common sources of information. While manual analysis is still widespread, approximately one-third of respondents reported that all analysis is done electronically.

Only six percent of respondents reported that their organization does not collect and analyze log information from any system at their organization. This is consistent with the data that was collected in 2009. While the percent of respondents at medical practices were twice as likely as those working for hospital-based organizations (11 percent compared to five percent) to report that their organization does not collect and analyze log information, this difference is not statistically significant.

Slightly more than three-quarters (78 percent) of the respondents collecting and analyzing information in an audit log reported that the firewall log is a source of information that is reviewed. Nearly three-quarters of respondents also reported that they collect and analyze information from their servers. More than half of respondents that collect and analyze log information also do so from the following sources – intrusion detection systems (61 percent), applications (59 percent) and network devices (57 percent). Respondents were least likely to collect and analyze log information from their additional storage devices (16 percent) or use a data reduction/analysis tool (15 percent). A full list of systems from which respondents collect and analyze data is included in Figure Five.



Types of Systems from Which Data is Collected and Analyzed

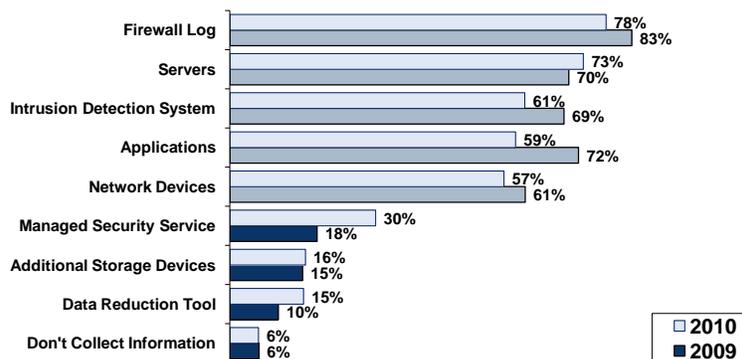


Figure Five. Types of Systems from Which Data is Collected and Analyzed

With respect to the manner in which information from the audit logs is analyzed, one quarter (25) percent reported that the information was analyzed only via a manual

process. Another 28 percent indicated that they used a combination of manual and other means, such as a Syslog server or log management appliance to analyze the information. Nearly one-third (31 percent) reported that their organization audited information solely using an automated process. The remaining respondents did not know what process their organization used to evaluate this data. Respondents working for medical practices were less likely than those working at hospital organizations to report that they use a manual only process for this type of analysis (21 percent compared to 27 percent).

It appears as though while still widespread, use of manual process to collect and analyze audit log data is less widespread than it was in the past. Last year, nearly three-quarters of respondents reported using this method for collecting and analyzing log information. This year, only 53 percent of respondents reported this to be the case. With regard to the automated methods in place for collecting and analyzing log information, 41 percent of respondents reported using a log management appliance and slightly more than one-third of respondents (35 percent) reported that they use a Syslog server. While the number of respondents using a Syslog server has remained constant, the percent of respondents reported using a log management appliance has more than doubled, from 18 percent in 2009. Organic application log management capability was reported to be used by 16 percent of respondents.

Respondents were also asked to identify the types of events their audit log captures. As in 2009, the most frequently identified type of event was security-critical events only, such as the use of authorization mechanisms like passwords. This was identified by 70 percent of respondents. This year again, this is followed by clinician access to data, which was identified by 62 percent of respondents. Slightly more than half of respondents (56 percent) indicated that their audit log captures information on non-clinician access to data. Sixteen percent noted that their audit log captures information on patient access to data; this is up from 12 percent in 2009.

Approximately two-thirds of respondents (69 percent) reported that their organization actively uses audit log data for policy compliance monitoring. A similar percent (63 percent) reported using this data for system activity monitoring. These numbers are similar to what was reported last year. However, last year's most frequently mentioned use of audit log information, intrusion detection, was identified by only 58 percent of respondents (compared to 72 percent in 2009). The least likely use for audit log information for providing Accounting of Disclosure to patients; only 36 percent of respondents reported using audit log data in this manner.

Only 20 percent of respondents indicated that they do not currently make Accounting of Disclosures available to patients. By organization type, 31 percent of respondents working for a medical practice report this to be the case, compared to 16 percent of respondents working for hospitals. Among the respondents who indicated that their organization provides an Accounting of Disclosures to patients when necessary, 39 percent reported that the audit log is the primary source of information from which they get this information. This is a slight decrease from the 46 percent of respondents who reported this to be the primary method of reporting in the 2009 study. One-quarter reported that this service is used only for non-TPO disclosures, while 13 percent reported that Accounting of Disclosures that include TPO. Eight percent reported that they provide this solution using an alternate solution, such as a proactive notification of routine disclosures.

6. Use and Measurement of Security Controls

Two-thirds of survey respondents were likely to report that their organization uses information generated in their risk assessment to identify which security controls to put into place. The majority of respondents indicated that the success of these security controls was measured using items such as number of detected security incidents and reduced risk of exposure.

Approximately two-thirds of respondents indicated that they used the information generated in their risk assessment to determine which security controls to put into place.

The majority of respondents (96 percent) reported that they have security controls in place and 89 percent of these respondents *monitor* the success of these controls. This is consistent to the data reported in 2009. Respondents working for a hospital were slightly more likely to report having these controls in place than were those working for a medical practice (98 percent compared to 92 percent).

More than half of the respondents with security controls in place (59 percent) reported that they monitor the success of these controls by using an internal risk analysis. This is much greater than the percentage of respondents who reported this to be the case in the 2009 research. Approximately half (47 percent) reported that their organization monitors the success of the security controls by using an internal compliance audit tool. A similar percent (46 percent) reported that they have an external risk analysis/vulnerability analysis/penetration testing. Approximately 44 percent noted that they have an external compliance audit. With the exception of the use of internal risk analysis tools, these numbers are similar to those reported in 2009.

Nearly three-quarters of respondents (72 percent) that monitor the success of their security controls also *measure* the success of these controls. This is an increase from the percentage identified in 2009, but consistent with the three-quarters of respondents who reported this to be the case in 2008. Among those that do measure the success of these controls, the most frequently used measure is identifying the number of detected security incidents; this was selected by 59 percent of respondents. Half indicated that their organization measures success by evaluating the reduced risk exposure that their organization experiences as a result of use of these controls. Only seven 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. With the exception of the percent of respondents who measure ROI, all of these numbers are slightly less than reported in 2009.

7. Security in a Networked Environment

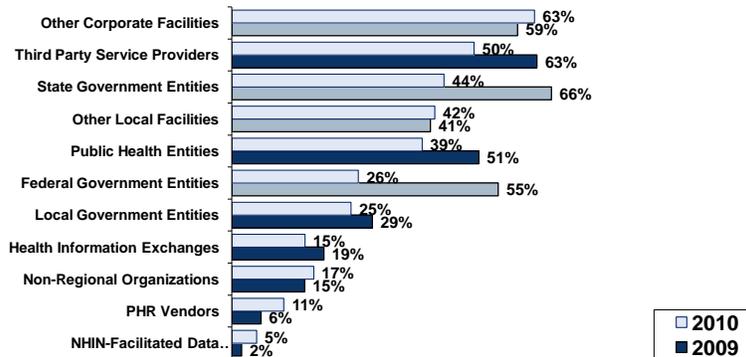
A large majority of respondents reported that their organization shares patient data in an electronic format. Data is most frequently shared with third party providers, state government, and other facilities within the corporate organization.

Respondents were asked to identify the types of organizations with which they share patient data in electronic format. Approximately 85 percent of respondents reported that their organization shares information with at least one other type of organization; this is a slight decrease from the 91 percent of respondents who reported this to be the

case in 2009. The percentage of respondents sharing information with different types of organizations is identified in the table below. Figure Six.



Existing Data Sharing Relationships



Source: The HIMSS Security Survey

Figure Six. Existing Data Sharing Relationships.

There is also a substantial amount of activity surrounding *future* plans for sharing electronic data. Overall, 79 percent of respondents reported that they plan to share data in an electronic format in the future.

Finally, while respondents from hospitals are somewhat more likely to report (83 percent) that they will share data in the future than are those from medical practices (77 percent), the likelihood of data sharing in the future is high among both groups.

Respondents are unlikely to report that data sharing agreements require them to implement additional data security tools. Only one-third of respondents (34 percent) indicated that their current data sharing arrangements have resulted in the use of additional security controls beyond those that were already in place at their organization. Respondents working for a hospital organization were more likely to report (36 percent) that their data sharing agreements required them to implement additional data security tools than were respondents who work for medical practices (23 percent).

8. Use of Security Technologies

Firewalls and user access controls have reached a level of saturation in the market. In general, satisfaction with the existing security technologies in place in their organizations is high among respondents. Among survey respondents, mobile device encryption, e-mail encryption and single sign-on were the technologies that are most likely to be considered for future use.

Respondents were asked to identify the types of security tools that are in place at their organization. Nearly all respondents (97 percent) reported that a firewall is in place and 93 percent indicated that user access controls have been established. Utilization of the *remaining* technologies in this survey are listed below:

- Audit logs of each access to patient health records – 80 percent;
- Disaster recovery – 73 percent;
- Wireless security protocols – 70 percent;
- Electronic signature – 68 percent;
- Data encryption (data in transmission) – 65 percent;
- Intrusion prevention/detection service – 56 percent;
- E-mail encryption – 59 percent;
- Off-site electronic data storage – 56 percent;
- Data encryption (data in storage) – 52 percent;
- Network encryption – 42 percent;
- Mobile device encryption – 39 percent;
- Single sign on – 36 percent;
- Data loss prevention – 30 percent;
- Two-factor authentication – 30 percent;
- Public key infrastructure – 25 percent;
- Biometric technologies – 16 percent;
- E-discovery – 13 percent.

Among the technologies that at least half of the respondents are using, satisfaction is highest for firewalls (6.44) and data encryption for data that is in transmission (6.22)³. Firewalls and wireless security protocols were the top tools with which users were satisfied in the 2009 survey (6.37 and 6.21 respectively); however data encryption for data in transmission had a high rate of satisfaction (6.13) in 2009.

Satisfaction levels for the other technologies used in at least half of respondents' organizations are also high, with averages of more than five. A list of the remaining technologies is provided below.

- Wireless security protocols – 5.99
- Off-site electronic data storage – 5.96
- Electronic Signature – 5.87
- Intrusion prevention/detection service – 5.82
- User access controls – 5.82
- Data encryption (data in storage) – 5.81
- E-mail encryption – 5.78
- Audit logs of each access to patient health records – 5.35
- Disaster recovery – 5.35

There are also numerous differences in the types of technologies that are in place at medical practices and hospitals. In summary, respondents working for hospitals were more likely to report that a number of technologies were in place than were respondents in medical practices. This is particularly the case for several of the encryption technologies identified in this research. The number of respondents reporting “yes” by organization type is shown in the table below; the * indicates a statistically significant relationship.

³ This is based on a one to seven scale, where one is not at all successful and seven is very successful.

Security Tool	Hospital Use	Medical Practice Use
Audit Logs*	84.30%	70.30%
Biometric Technologies*	19.80%	6.30%
Data Encryption (Storage)*	53.50%	40.60%
Data Encryption (Transmission)*	68.00%	48.40%
Data Loss Prevention	28.50%	25.00%
Disaster Recovery	74.40%	65.60%
eDiscovery*	16.90%	3.10%
Electronic Signature*	72.10%	67.20%
Email Encryption*	68.00%	32.80%
Firewalls	97.10%	95.30%
Intrusion Prevention	57.60%	43.80%
Mobile Device Encryption*	45.30%	15.60%
Network Encryption	39.50%	42.20%
Off-Site Electronic Data Storage	53.50%	60.90%
Public Key Infrastructure*	27.30%	7.80%
Single Sign On*	41.30%	20.30%
Two-Factor Authentication*	34.90%	17.20%
User Access Controls*	94.20%	89.10%
Wireless Security Protocols*	80.20%	48.40%

As in 2009, e-mail encryption technology and single sign-on (SSO) technology continue to be top areas in which respondents have plans to purchase technology in the future. Approximately one-quarter of respondents in the sample reported that they would purchase these technologies. However, both technologies were eclipsed by mobile device encryption; 29 percent of respondents that don't presently use this technology plan to make a purchase in the future. Respondents working for hospital organizations were more likely to report that they would purchase SSO technology than were those working at a medical practice (47 percent compared to 16 percent).

Biometric and e-discovery technologies, which are both currently used by less than 20 percent of respondents' organizations do not have high levels of projected future use, at 11 and 16 percent respectively.

The number of respondents reporting that they would purchase additional technology that was not already in use is shown by organization type in the table below; the * indicates a statistically significant relationship.

Security Tool	Hospital Use	Medical Practice Use
Audit Logs	48.10%	52.60%
Biometric Technologies	15.20%	13.30%
Data Encryption (Storage)	47.50%	39.50%
Data Encryption (Transmission)	54.00%	39.40%
Data Loss Prevention	30.90%	20.80%
Disaster Recovery	72.70%	63.60%
eDiscovery*	24.50%	6.50%
Electronic Signature	47.90%	42.90%
Email Encryption	63.60%	48.80%
Firewalls*	20.00%	33.30%
Intrusion Prevention	43.80%	36.10%
Mobile Device Encryption*	53.20%	33.30%
Network Encryption	25.00%	21.60%
Off-Site Electronic Data Storage	31.30%	24.00%
Public Key Infrastructure	12.80%	6.80%
Single Sign On*	46.50%	15.70%
Two-Factor Authentication	26.80%	20.80%
User Access Controls	40.00%	28.60%
Wireless Security Protocols	38.20%	27.30%

For the first time this year, the survey specifically addressed additional information in the area of encryption. Nearly 85 percent of respondents indicated that their organization uses at least one of the encryption technologies tracked in this research. These respondents were asked to identify on what types of devices this technology was deployed.

Nearly half of respondents (42 percent) reported that none of the data on their desktop computers was encrypted. In comparison, only 16 percent of respondents reported that none of the data on their laptop computers was encrypted. Indeed more than half of respondents reported that at least 75 percent of the data housed on laptop computers is encrypted. A high percent of respondents (45 percent) also reported that at least 75 percent of the data on their back-up tapes was encrypted.

9. Patient Identity

Half of respondents indicated that they validate patient identity by both requiring a government/facility-issued ID and checking the ID against information in the master patient index. A similar percent reported that they have a formal process for reconciling duplicate records in their master patient index.

Only two percent of respondents did not report a specific method by which their organization proves that the person at the point of care is who they say they are. Slightly more than half of the respondents (52 percent) indicated that they require a valid government/facility-issued photo ID that is then checked against demographic information in the master person index (MPI). Another quarter (22 percent) reported that they use only a government/facility-issued photo ID. However, respondents at

hospitals were more likely to report that they required a valid government/facility-issued photo ID *and* that they checked this information against demographic information in an MPI than were those working at a medical practice (56 percent compared to 48 percent).

Eight percent reported that their sole means of validating data is to check the data provided by the patient against information in the MPI. Four percent of respondents reported that they use physician and/or clinical attributes such as a tattoo or dental records to validate patient identities. The remaining respondents reported other measures or were not sure of the method used to validate patient identity.

For subsequent visits, respondents were most likely to report that they would assign and use unique identifiers; this was selected by 46 percent of respondents. However, only 15 percent of respondents noted that their organization offers a facility issued identification card, and only three percent noted that their organization created a facility issued smart card with processing capability. In addition, about four percent of respondents noted that they scanned a photo of the patient into their system and used that for future reference. Two percent of respondents reported that they used either a finger print or palm scan for identification. None of the respondents reported using iris scan or retinal scan technology for identification purposes. Seventeen percent were not sure how this was accomplished.

Respondents were also asked to identify how duplicate records were identified in the master person index. More than half of respondents (56 percent) reported that they had a formal reconciliation process with their staff. Another quarter (27 percent) reported that the process was an informal manual process. Approximately 10 percent were not sure how this was accomplished. Five percent reported that they did not have a process for managing duplicate records. Two percent of the respondents noted that they do not have an MPI. Those working for a medical practice were more likely to report using an informal manual process than were those working for a hospital (32 percent compared to 25 percent).

Finally, respondents were asked to identify some of the capabilities of their electronic health record (EHR) with regard to storage of identification data. A high percentage of respondents (83 percent) indicated that they enable alphanumeric storage of demographic information, such as name, address, phone, date of birth, gender or social security number. Approximately 59 percent of respondents indicated that their EHR can store analog, scanned or digital photos. Respondents were less likely to report that their EMR could store alphanumeric digital representations such as smart card identifiers (16 percent). Nine percent of respondents reported that they don't have an EHR.

None of the questions in this section were asked in the 2009 research.

10. Security Breaches and Medical Identity Theft

While nearly all respondents reported that their organization actively works to determine the cause/origin of a security breach, only two-thirds of respondents reported that their organization has formal policies/procedures in place related to addressing a security breach. One-third 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. About two-

thirds of respondents reported that their organization does have this type of plan in place. Another quarter (27 percent) are currently developing these policies and procedures. Only one percent reported that they did not have this type of plan and had no plan to do this in the future. In comparison, last year only about half of respondents reported that their organization has a plan in place for responding to threats or incidents relating to a security breach and six percent said that their organization has no plan in place and does not intend to develop a plan.

Consistent with the data from last year, 93 percent of respondents indicated that their organization actively works to determine the cause/origin of a security breach.

Approximately one-third of respondents (31 percent) reported that their organization has had at least one known case of medical identity theft at their organization. This is nearly identical to the data from 2009, when 32 percent of respondents reported that a case of medical identity theft had taken place at their organization. Those working for a medical practice were much less likely to report that a security breach occurred at their organization (17 percent), when compared to those working for a hospital organization (38 percent).

For the purposes of this research, medical identity theft was identified as “the use of an individual’s identity-specific information such as name, date of birth, social security number, insurance information, etc. without the individuals’ 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 standing is corrupted, potentially impacting patient care”.

11. Conclusion

In order to qualify for meaningful use incentives CMS identified a core set of 14 meaningful use objectives in which eligible hospitals (EH) and 15 core meaningful use objectives in which eligible professionals (EP) need to focus to qualify for incentive funds provided through the new CMS Medicare and Medicaid incentive program. Additionally, EHs and EPs must also focus on five of 10 menu set objectives to qualify for incentive funds.

The area of risk analysis is one that organizations must ensure that they are taking into consideration. Without undergoing this process and then using the outcomes to change use of controls and modifications within policies and procedures, organizations will not qualify for the meaningful use incentives. At present, one-quarter of the sample population would not qualify for meaningful use as a result of this area.

The results also show that medical practices are not as advanced in many of the areas for security data, when compared to hospitals. For instance, they are less likely to report conducting a formal risk analysis, they are less likely to have many of the security tools in place and they are less likely to analyze data from their audit logs. One issue that may explain this is a potential lack of IT staff at medical practices, leaving the security function to others who simply do not have the expertise and background to negotiate the complex issues surrounding the privacy and security of data. One approach to bridging this gap may be the use of external resources, such as consultants. Indeed, the respondents representing medical practices in this study were much more likely to report that they relied on external resources when compared to those working for a hospital.

In addition to meeting the meaningful use requirements, establishing a robust environment is crucial as organizations share information outside of their organizations. Respondents were more likely in this year's study than they were in the past to report that they shared electronically stored data with patients, surrogates and designated others. Furthermore, 79 percent of respondents reported that they would share information with outside organizations in the future. Thus, organizations need to ensure that they are properly securing data that is being transmitted outside of the organization. At this time, respondents were not likely to report that they added security tools to for the purpose of sharing data outside their organizations. At the same time, use of tools such as data encryption in transmission and e-mail encryption are used by less than two-thirds of respondents.

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 have offices in Chicago, Washington, DC, Brussels, Singapore, Leipzig, and other locations across the United States. HIMSS represents more than 30,000 individual members, of which two thirds work in healthcare provider, governmental and not-for-profit organizations. HIMSS also includes over 470 corporate members and more than 85 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, and research initiatives 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. About Intel

Connecting people and information for a healthier tomorrow: Intel products, solutions and technologies are enabling healthcare organizations to develop new models of care delivery to better meet the needs of patients and their clinical teams while improving the quality and efficiency of delivering care. www.intel.com/healthcare

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 3rd Annual HIMSS Security Survey, sponsored by Intel.

15. For More Information, Contact:

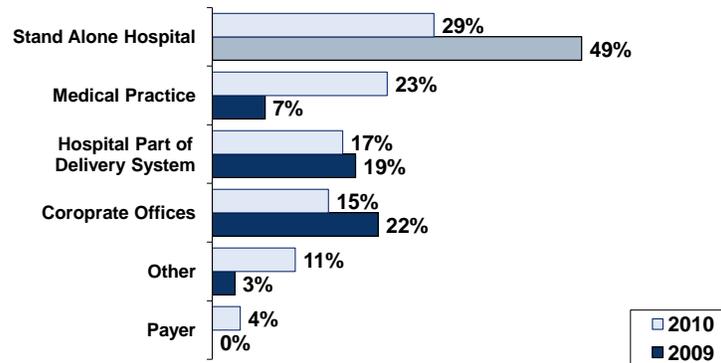
Joyce Lofstrom
Senior Manager, Corporate
Communications
HIMSS
230 E. Ohio St., #500
Chicago, IL 60611
312-915-9237
jlofstrom@himss.org

Jared Quoyeser, MHA, MBA
Director, Americas Healthcare Industry
Management
Intel
1900 Prairie City Road
Folsom, CA 95630
916-356-5866

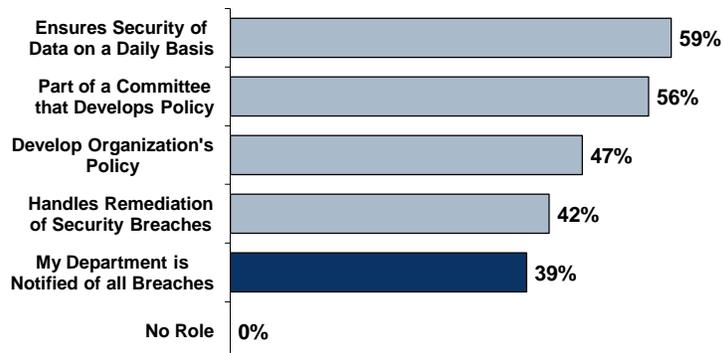
Appendix



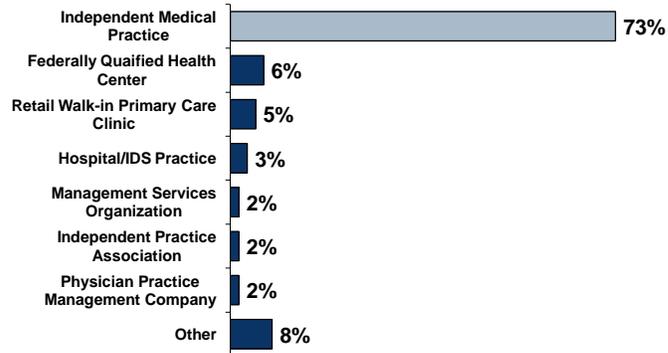
Participant Profile – Organization Type



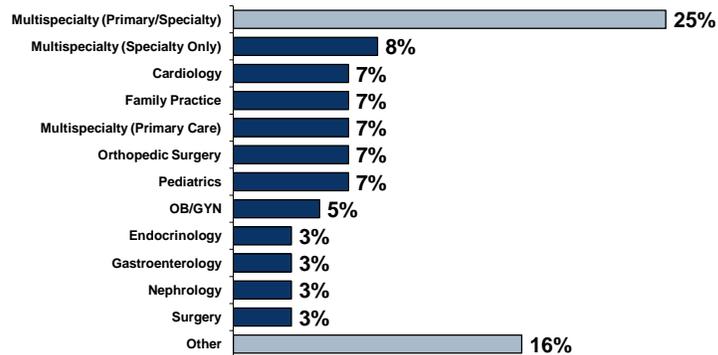
Level of Participation in Maintaining Privacy & Security



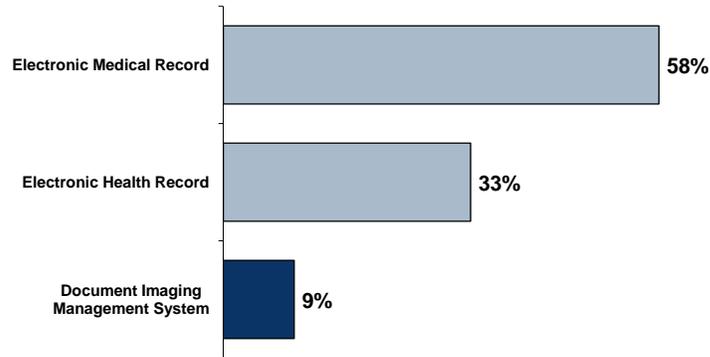
Participant Profile – Type of Medical Practice



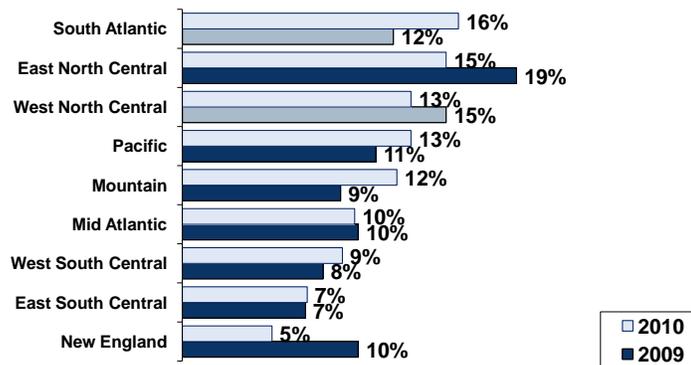
Participant Profile – Medical Practice Specialty



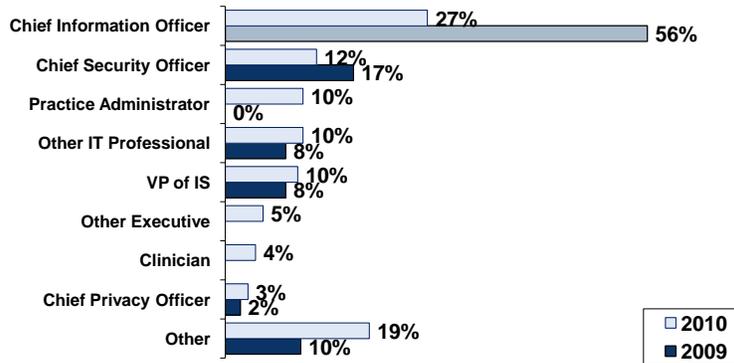
Participant Profile – Method of Storing Data at Medical Practices



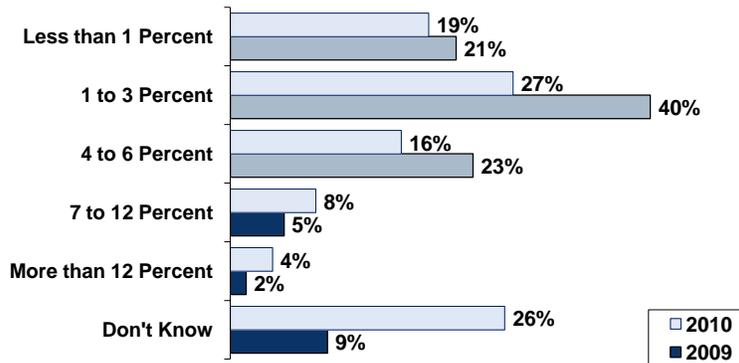
Participant Profile – Region



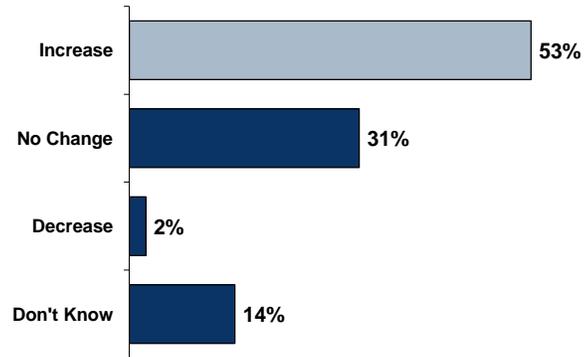
Participant Profile – Title



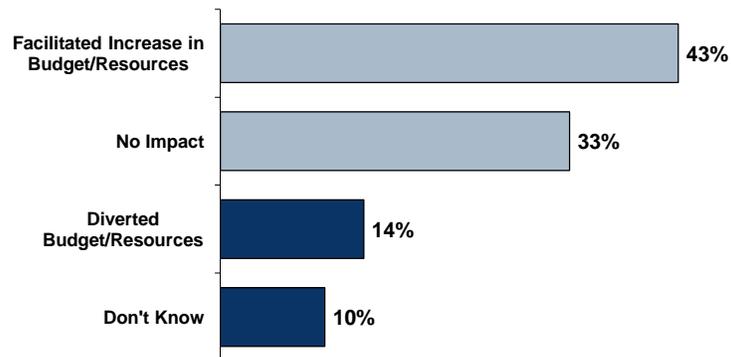
Percent of IT Budget Dedicated to Information Security



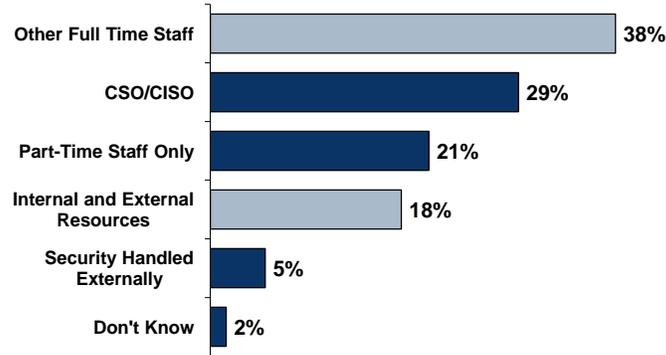
Change in Percent of IT Budget Dedicated to Information Security



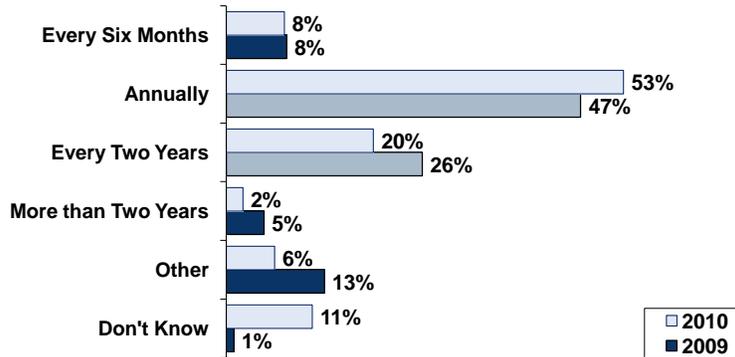
Impact of Federal Initiatives on Federal Budget



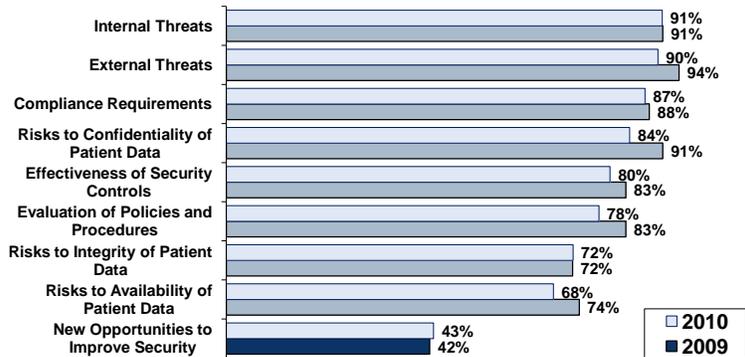
Personnel Responsible for Securing Environment



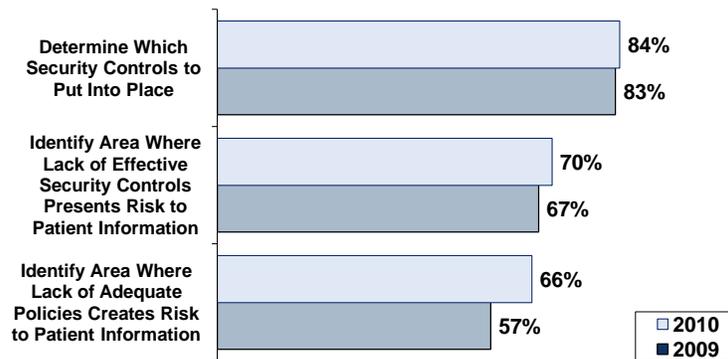
Frequency of Conducting a Formal Risk Analysis



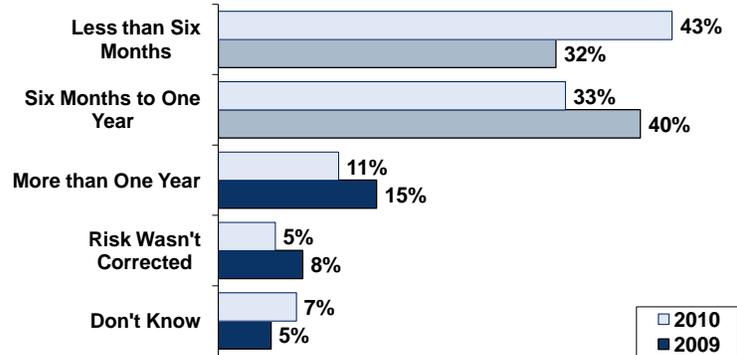
Components of a Formal Risk Analysis



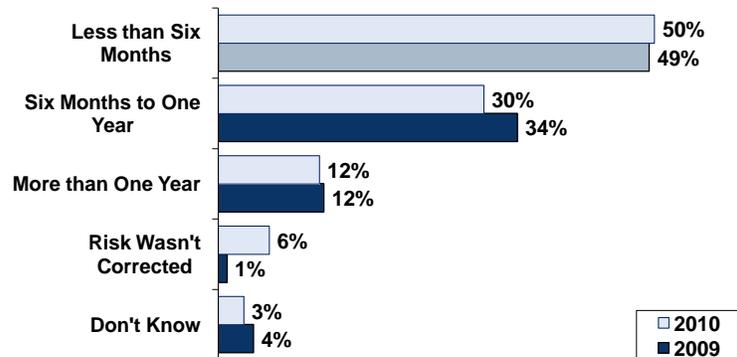
Use for Risk Analysis Data



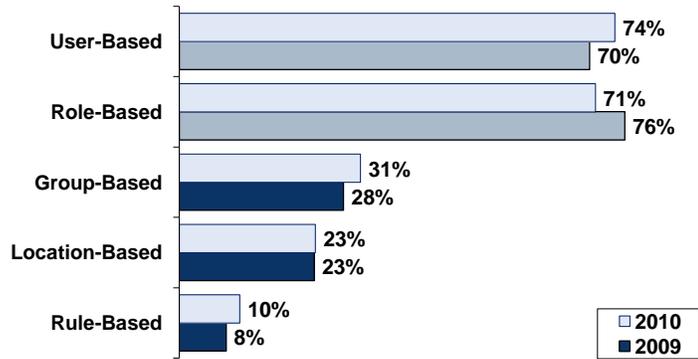
Length of Time Required to Correct a Deficiency by Revising Security Controls



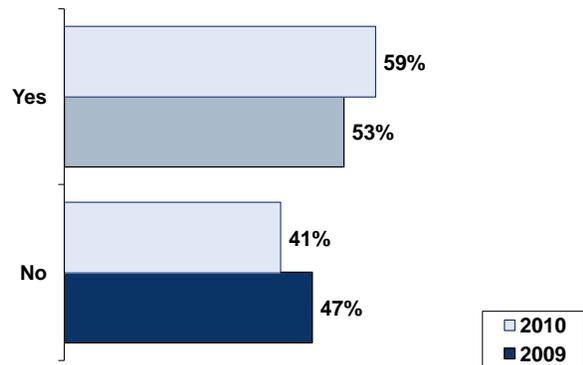
Length of Time Required to Correct a Deficiency by Revising Policies/Procedures



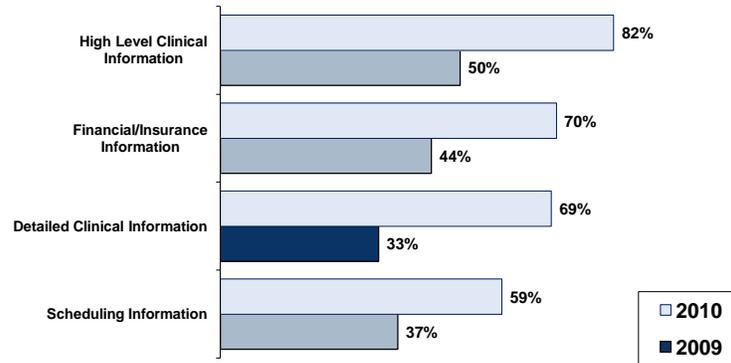
Method for Controlling Organizational Access to Patient Information



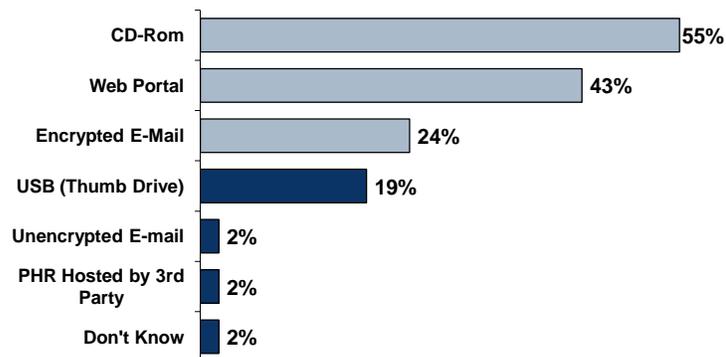
Access to Electronic Information By Patients, Surrogates or Designated Others



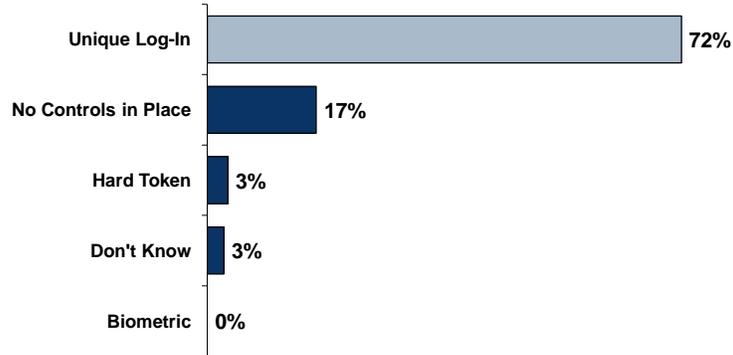
Types of Data Patients, Surrogates and Designated Others Can Access



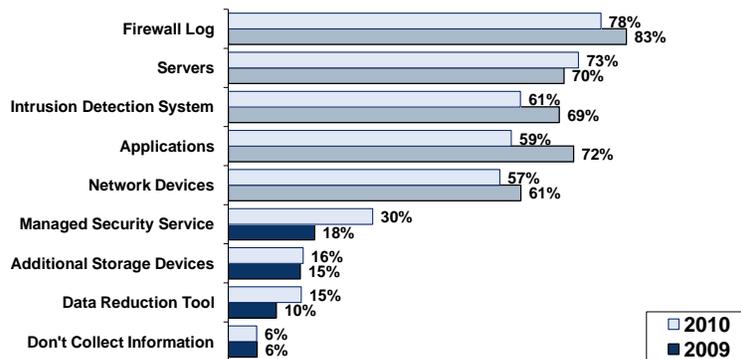
Means by Which Organizations Provide Electronic Information to Patients



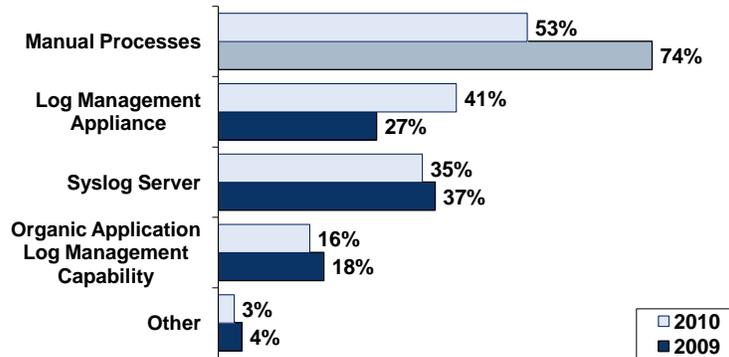
Method of Controlling Access to Health Websites/Web Portals Offered to Patients



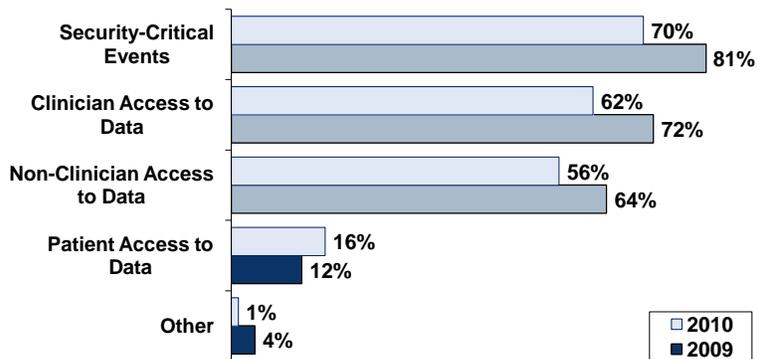
Types of Systems from Which Data is Collected and Analyzed



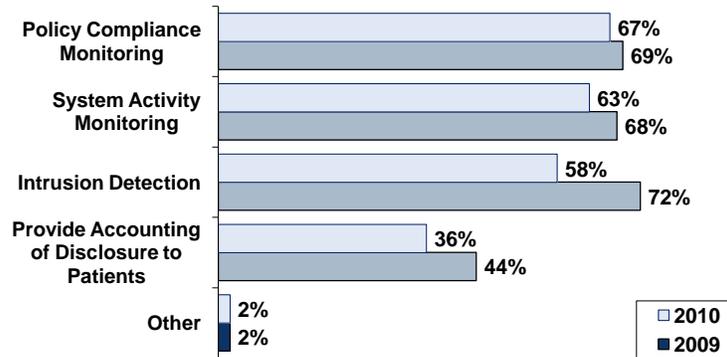
Methods for Analyzing Log Information



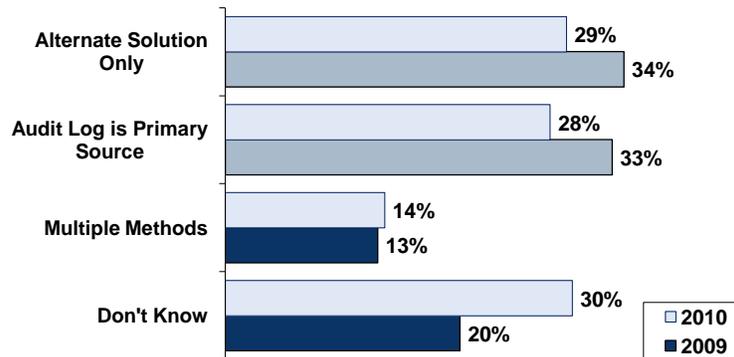
Events Captured by Audit Logs



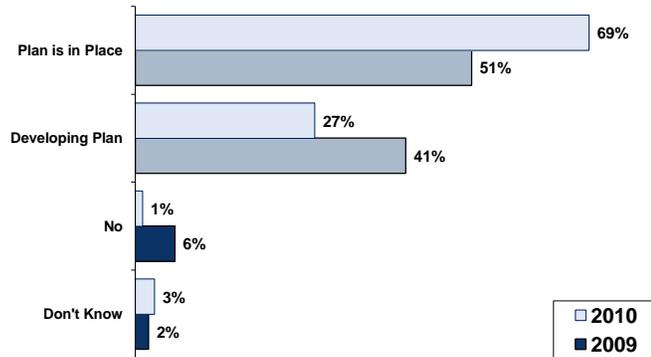
Use of Audit Log Data



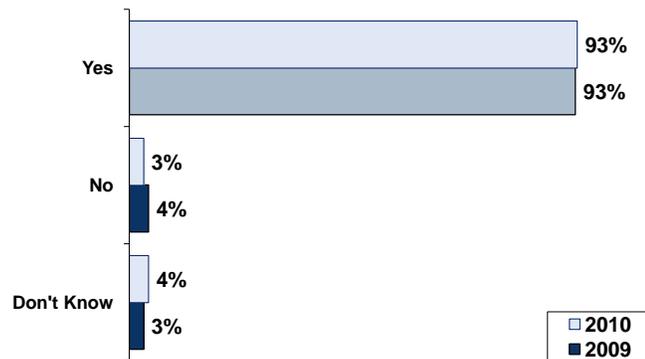
Means by Which Accounting of Disclosure is Made Available to Patients



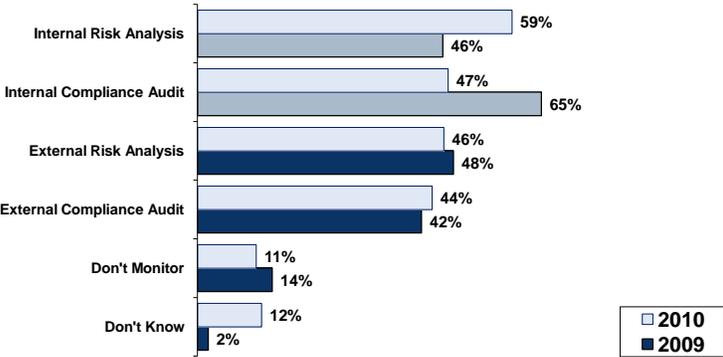
Plan in Place to Respond to Threats or Security Breaches



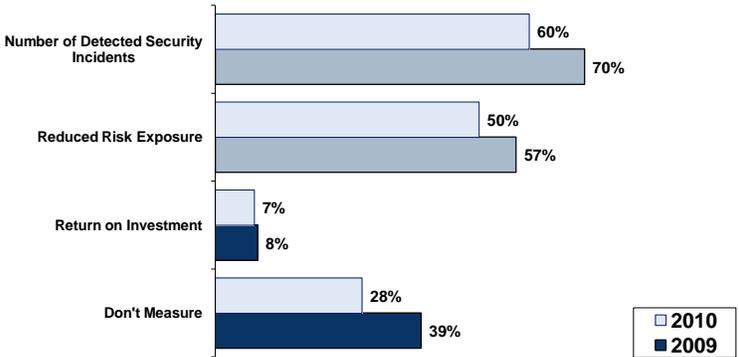
Actively Determine Cause/Origin of a Security Breach



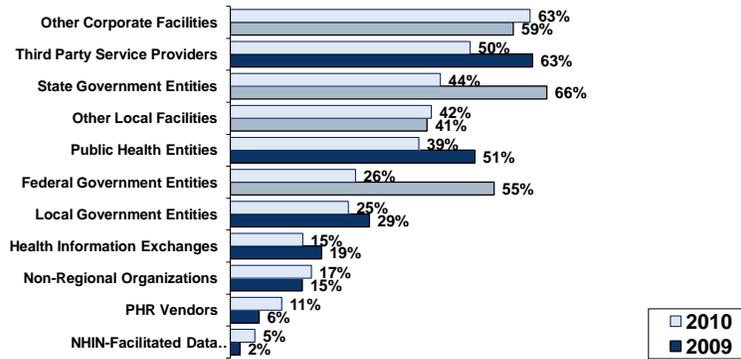
Means for Monitoring Success of Security Controls in Place



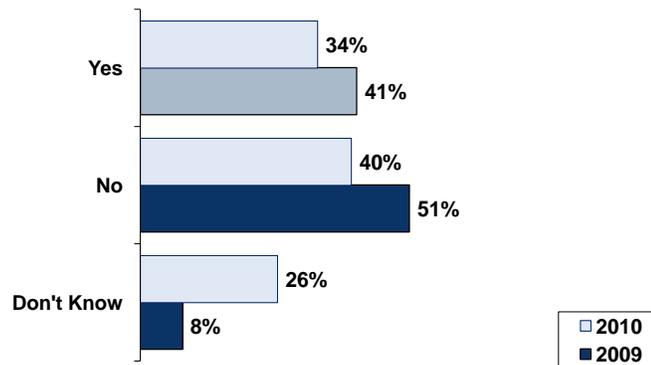
Means for Measuring Success of Security Controls in Place



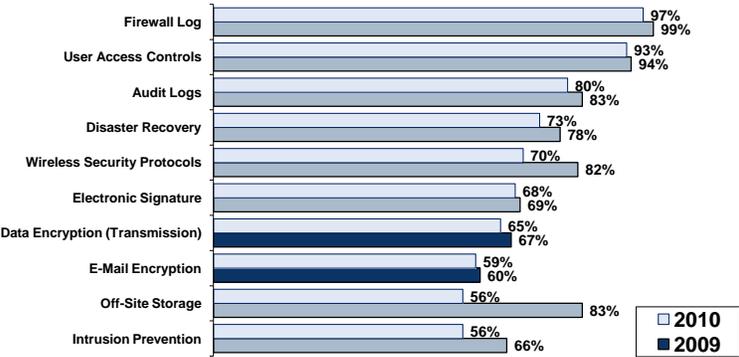
Existing Data Sharing Relationships



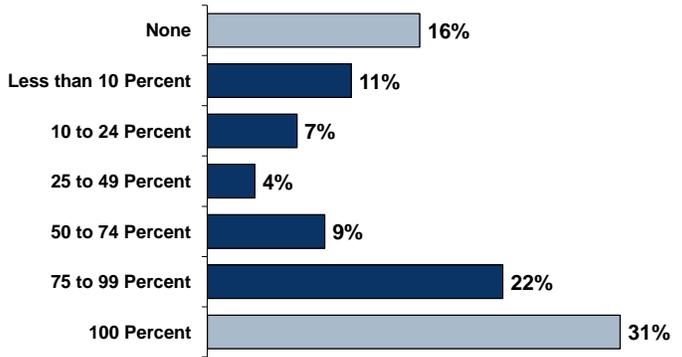
Data Sharing Arrangements Require Use of Additional Security Controls



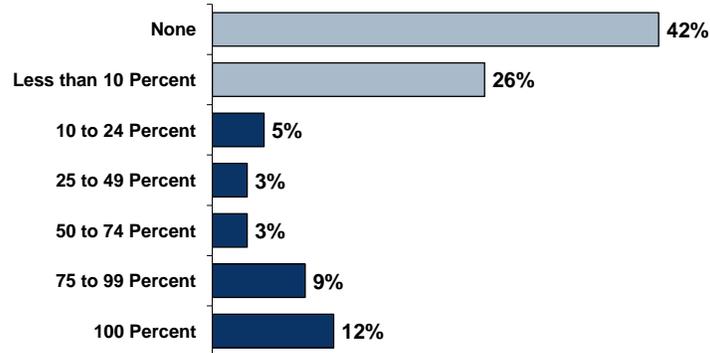
Use of Security Technologies (Top 10 Responses)



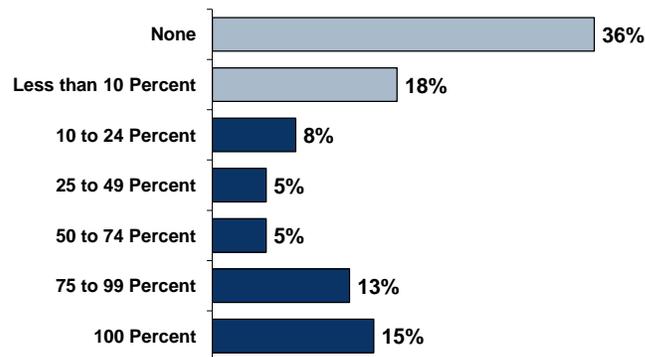
Percent of Data on Laptop Computers that is Encrypted



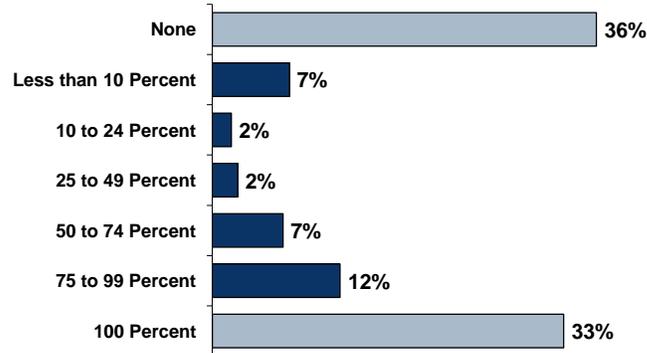
Percent of Data on Desktop Computers that is Encrypted



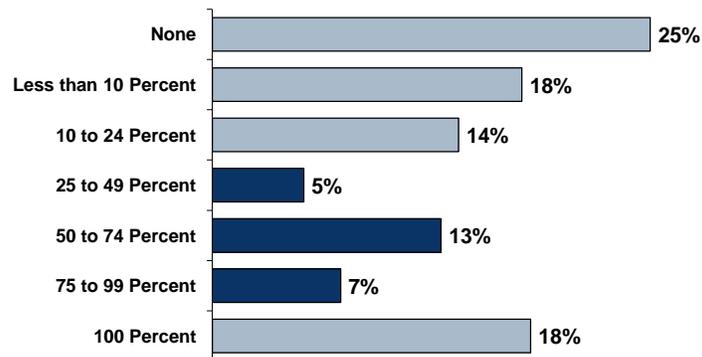
Percent of Data on Servers that is Encrypted



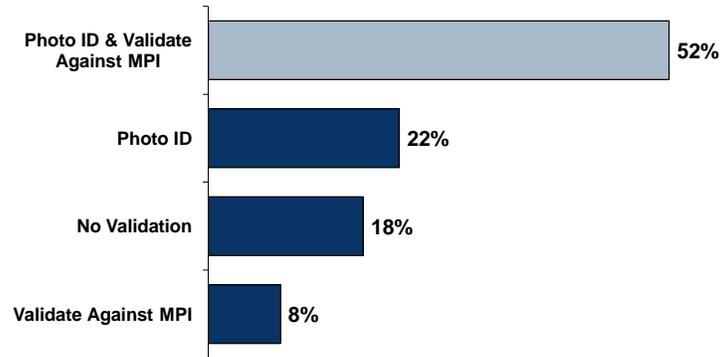
Percent of Data on Back-Up Tapes that is Encrypted



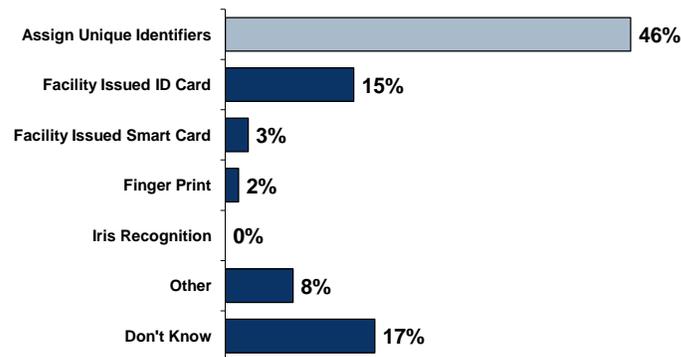
Percent of Data on E-Mail that is Encrypted



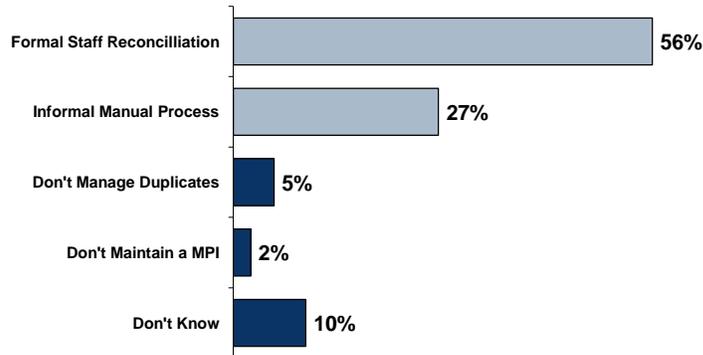
Method of Proving Patients' Identities



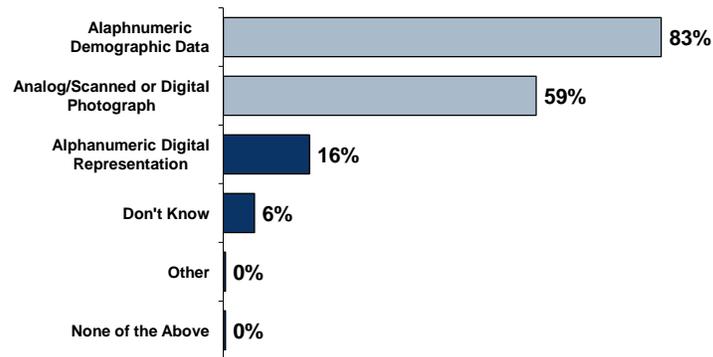
Method for Ongoing Validation at Subsequent Visits



Method for Identifying Duplicates within MPI



Items Stored in Electronic Health Record



Has Organization Had One Case of Medical Identify Threat

