Ponemon INSTITUTE

Third Annual Benchmark Study on Patient Privacy & Data Security

Sponsored by ID Experts

Independently conducted by Ponemon Institute LLC

Publication Date: December 2012

Third Annual Benchmark Study on Patient Privacy & Data Security

Presented by Ponemon Institute, December 2012

Part 1. Introduction

Healthcare organizations seem to face an uphill battle in their efforts to stop and reduce the loss or theft of protected health information (PHI) or patient information. As is revealed in the *Third Annual Benchmark Study on Patient Privacy and Data Security,* many healthcare organizations struggle with a lack of technologies, resources and trained personnel to deal with privacy and data security risks.

The consequence of not having adequate funding, solutions and expertise in place is clear. Since first conducting this study in 2010 the percentage of healthcare organizations reporting a data breach has increased and not declined. Further, there are more reports of multiple breaches and only 40 percent of organizations in this study have confidence that they are able to prevent or quickly detect all patient data loss or theft.

Since 2010 the threats to healthcare organizations have become increasingly more difficult to control. Technologies that promise greater productivity and convenience such as mobile devices, file-sharing applications and cloud-based services are difficult to secure. Employee mistakes and negligence also continue to be a significant cause of data breach incidents. Another worry presented in this research is that sophisticated and stealthy attacks by criminals have been steadily increasing since 2010.

The price tag for dealing with these breaches can be staggering. While the cost can range from $10,000 to more than $1 million, we calculate that the average cost for the organizations represented in this benchmark study is $2.4 million over a two-year period. This is up slightly from $2.2 million in 2011 and $2.1 million in 2010.

The types of healthcare organizations participating in the study are hospitals or clinics that are part of a healthcare network (46 percent), integrated delivery systems (36 percent) and standalone hospital or clinic (18 percent). This year 80 healthcare organizations participated in this benchmark research and 324 interviews were conducted[1]. Respondents interviewed work in all areas of the organization: security, administrative, privacy, compliance, finance and clinical.

Key Research Findings:

More healthcare organizations are having several breaches. Ninety-four percent of healthcare organizations in this study have had at least one data breach in the past two years. However, 45 percent report that they have had more than five incidents. In 2010, only 29 percent reported that their organization had more than 5. This suggests the importance of determining the cause of the breach and what steps need to be taken to address areas potentially vulnerable to future incidents.

Data breaches can have severe economic consequences. The economic impact of one or more data breaches for healthcare organizations in this study ranges from less than $10,000 to more than $1 million over a two-year period. Based on the ranges reported by respondents, we calculated that the average economic impact of data breaches over the past two years for the healthcare organizations represented in this study is $2.4 million. This is an increase of almost $400,000 since the study was first conducted in 2010. As this finding demonstrates, the average annual cost to the healthcare industry could potentially be as high as almost $7 billion.[2] Data

[1] Benchmark research differs from survey research. The unit of analysis in benchmark research is the organization and in survey research it is the individual.

[2] This is based on multiplying $1,195,135 x 5,754 (average economic impact for a healthcare organization over a one-year period x the total number of registered US hospitals per the AHA).

breaches costing more than $500,000 have increased from 48 percent of healthcare organizations in 2010 to 57 percent of respondents in this year's study.

I**nsider negligence continues to be at the root of the data breach.** The primary cause of breaches in this study is a lost or stolen computing device (46 percent), which can be attributed in many cases to employee carelessness. This is followed by employee mistakes or unintentional actions (42 percent), and third-party snafus (42 percent). A major challenge for IT security is the increase in criminal attacks, which has seen an increase from 20 percent in 2010 to 33 percent this year.

Respondents acknowledge the harms to patients if their records are lost or stolen. The types of patient data lost or stolen most often are medical files and billing and insurance records, as discussed above. Seventy percent of respondents say there is an increased risk that personal health facts will be disclosed if the records are stolen or lost. This is followed by the risk of financial identity theft and medical identity theft (61 percent and 59 percent, respectively).

Medical identity theft occurs and can affect patient treatment. Fifty-two percent of organizations report that their healthcare organizations had one or more incidents of medical identity theft. While only 18 percent say the theft was a result of a data breach, 32 percent are unsure. This uncertainty is due in part to the finding that only one-third say they have sufficient controls in place to detect medical identity theft.

Employee records are also at risk. Respondents are more confident that patient billing information and medical records will not be susceptible to data loss or theft. In 2011, 39 percent of respondents said patient-billing information was vulnerable. This year the frequency of response declined to 29 percent. Similarly, the susceptibility of patient medical records declined from 25 percent of respondents in 2011 to 15 percent of respondents who believe this information is most at risk. In contrast, a much higher percentage of respondents in this year's study believe employee records have become the most susceptible to data loss or theft than last year (an increase from 9 percent to 21 percent).

Trends in mobility and employee owned devices put patient data at risk. Eighty-one percent of organizations permit employees and medical staff to use their own mobile devices such as smartphones or tablets to connect to their networks or enterprise systems such as email. On average, 51 percent of employees are bringing their own devices to the healthcare facility.

Unsecured medical devices are vulnerable to hackers. Medical devices containing sensitive patient information such as wireless heart pumps, mammogram imaging and insulin pumps often use commercial PCs and have wireless connections that make them vulnerable to cyber attacks. According to the healthcare organizations in this study, 69 percent of organizations do not secure medical devices. This finding may reflect the possibility that they believe it is the responsibility of the vendor—not the healthcare provider--to protect these devices.

Healthcare organizations embrace the cloud. Sixty-two percent of organizations make moderate or heavy use of cloud services. Only 9 percent do not use cloud services. However, 47 percent are not confident that information in the cloud is secure and 23 percent are only somewhat confident.

Concerns about the security of Health Information Exchanges (HIE) are keeping organizations from joining. Only 28 percent of organizations say their organization is a member and another 17 percent say they will become a member. More than one-third (35 percent) say they do not plan to become a member of HIE. The primary reason could be that 66 percent of respondents say they are only somewhat confident (30 percent) or not confident (36 percent) in the security and privacy of patient data on HIEs.

Confidence in the ability to prevent and detect a data breach improves but still has far to go. In 2010, only 31 percent of organizations said they had confidence in preventing and detecting all patient data loss or theft in their organization. This percentage has been steadily climbing and it is now at 40 percent. What has improved is that organizations are relying less on an "ad hoc" process and more on policies and procedures and a combination of manual procedures and security technologies.

Compliance encourages improvements in privacy and data security. Thirty-six percent of respondents strongly agree and agree that recent Office of Civil Rights (OCR) HHS HIPPA/HITECH audits and fines have affected changes in their organization's patient data privacy and security programs. Sixty-eight percent of organizations conduct and document post data breach incident risk assessments as mandated by the HITECH Act, an increase from 61 percent last year.

Employee training is the most common activity but does not seem to be effective in reducing insider negligence. The primary activity conducted by healthcare organizations is to comply with annual or periodic HIPAA privacy and security awareness training of all staff. This is followed by 49 percent who vet and monitor third parties, including business associates. Annual security risk assessments are done by less than half (48 percent) of organizations. The activity performed the least is a periodic privacy risk assessment. While performed the least, privacy risk assessments that evaluate privacy controls and policy may be best able to reduce the frequency of data breaches unintentionally caused by employees.

Barriers to achieving a stronger defense against data breaches continue to be a shortage of technologies, funding and expertise. Fifty-two percent of respondents agree that they have sufficient policies and procedures to prevent or quickly detect unauthorized patient data access, loss or theft. This increased from 41 percent in 2010 and can be attributed to the need for compliance with regulations. However, only 27 percent say they have sufficient resources and 34 percent say they have a sufficient security budget. Technologies and personnel are adequate according to 40 percent and 45 percent of respondents.

The following are some of the top findings of the study. They are discussed in more detail with other results in Part 2 of this report.

- Ninety-four percent of organizations in our study have had at least one data breach in the past two years. The average number for each participating organization is 4 data breach incidents in the past two years.

- The average economic impact of a data breach over the past two years for the healthcare organizations represented in this study is $2.4 million. This is an increase of almost $400,000 since the study was first conducted in 2010.

- The average number of lost or stolen records per breach is 2,769. The types of patient data lost or stolen most often are medical files and billing and insurance records.

- The top three causes for a data breach are: lost or stolen computing devices, employee mistakes and third-party snafus.

- Fifty-two percent discovered the data breach as a result of an audit or assessment followed by employees detecting the breach (47 percent).

- More than half (54 percent) of organizations have little or no confidence that their organization has the ability to detect all patient data loss or theft.

- Eighty-one percent permit employees and medical staff to use their own mobile devices such as smartphones or tablets to connect to their organization's networks or enterprise systems. However, 54 percent of respondents say they are not confident that these personally owned mobile devices are secure.

- Ninety-one percent of hospitals surveyed are using cloud-based services, yet 47percent lack confidence in the ability to keep data secure in the cloud.

- Despite recent attacks on medical devices, 69 percent of respondents say their organization's IT security and/or data protection activities do not include the security of FDA-approved medical devices.

Part 2. Key findings

In this report, we have organized the most salient research results according to the following four topics:

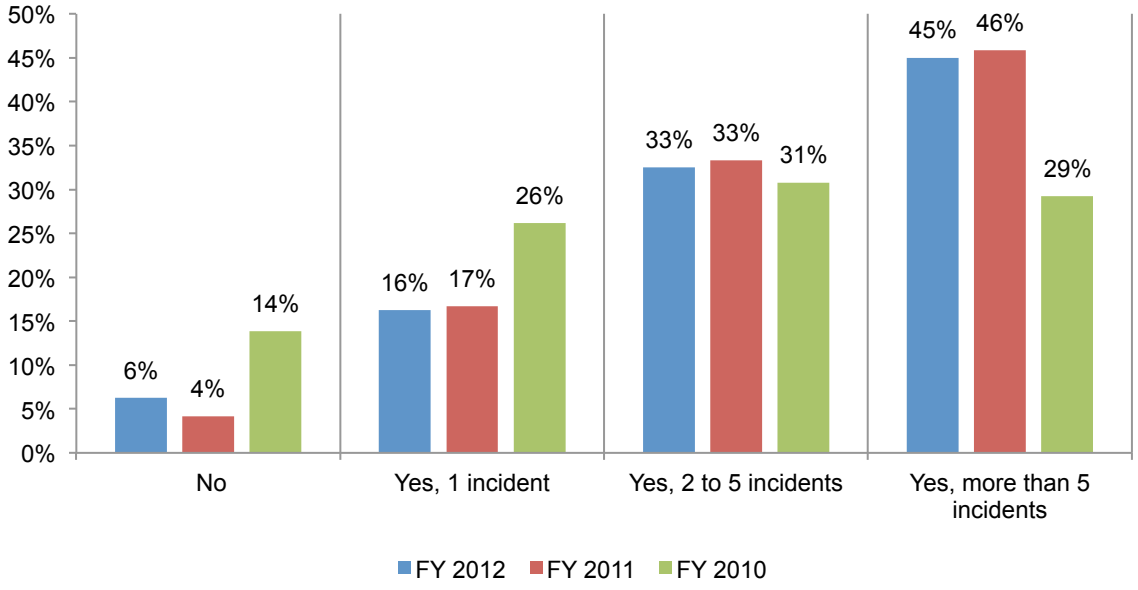
- Healthcare organizations have multiple breaches.
- Data breaches put patients and their information at risk for disclosure and financial and medical identity theft.
- Technology trends threaten healthcare's ability to protect patient information.
- Healthcare organizations take steps to prevent breaches but many still lack resources.

The complete audited findings of this study are presented in the appendix of this report.

1. Healthcare organizations have multiple breaches.

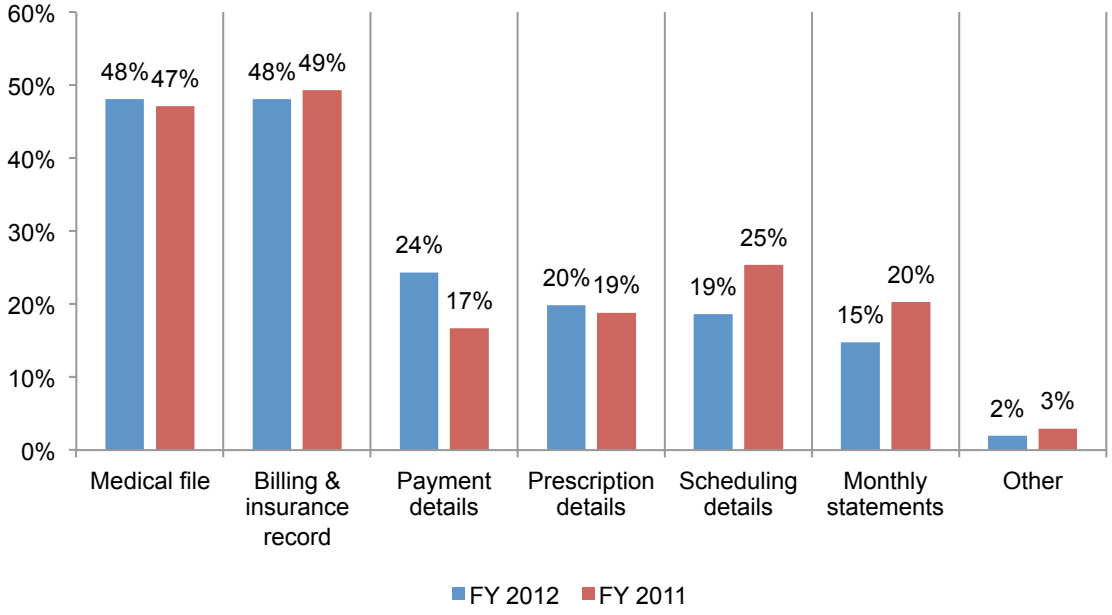
More healthcare organizations are having several breaches. According to Figure 1, 94 percent of healthcare organizations in this study have had at least one data breach in the past two years. However, 45 percent report that they have had more than five incidents. In 2010, only 29 percent reported that their organization had more than 5. This suggests the importance of determining the cause of the breach and what steps need to be taken to address areas potentially vulnerable to future incidents.

Figure 1. Experienced a data breach involving the loss of patient data in the past two years



It is not surprising that data breaches are most likely to involve healthcare records with the kind of sensitive and valuable information that appeals to identity thieves. According to the findings presented in Figure 2, medical files and billing and insurance records are the most likely to be lost or stolen. This is consistent with the findings from 2011. It is interesting to note that payment details as a type of data that is lost or stolen increased significantly from 17 percent to 24 percent.

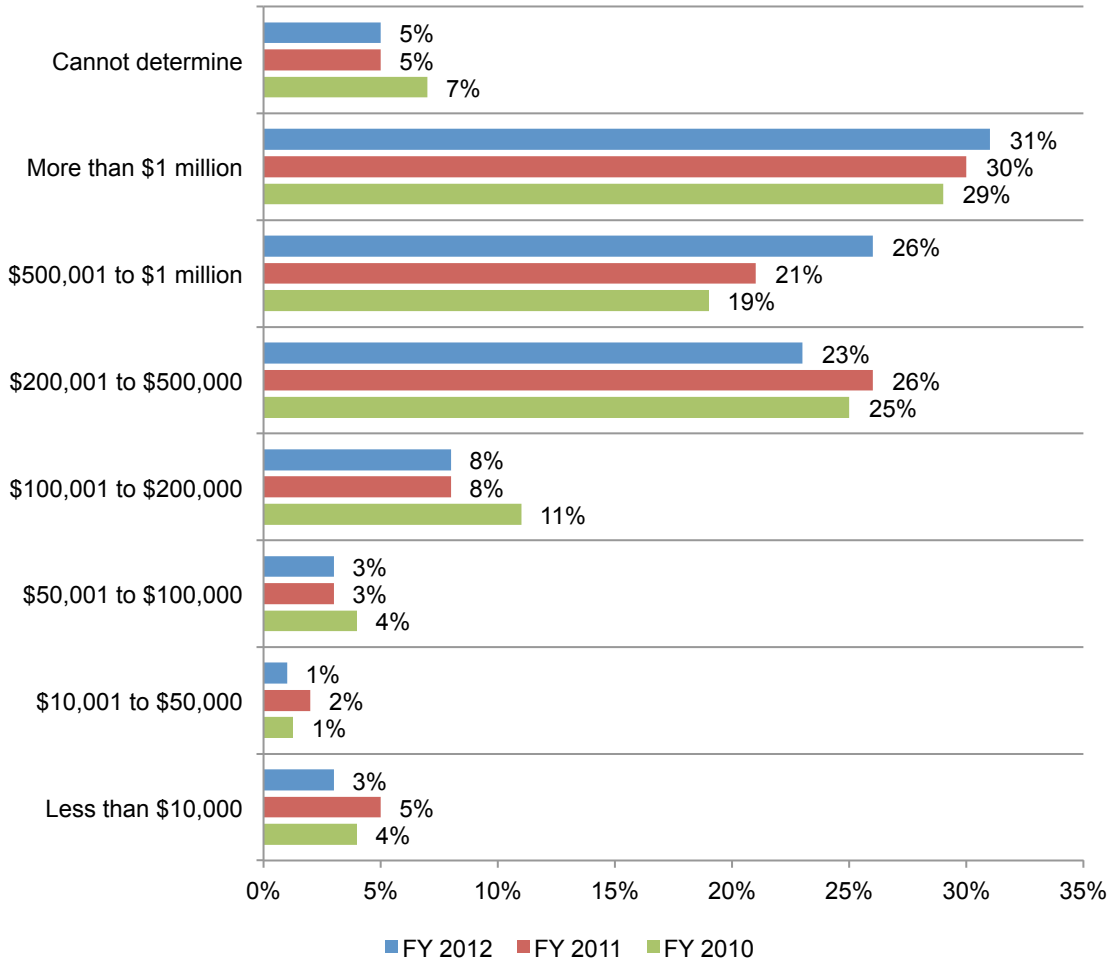
Figure 2. Type of data that was lost or stolen
More than one choice permitted



Data breaches can have severe economic consequences. Figure 3 reveals that the economic impact of one or more data breaches for healthcare organizations in this study ranges from less than $10,000 to more than $1 million over a two-year period.

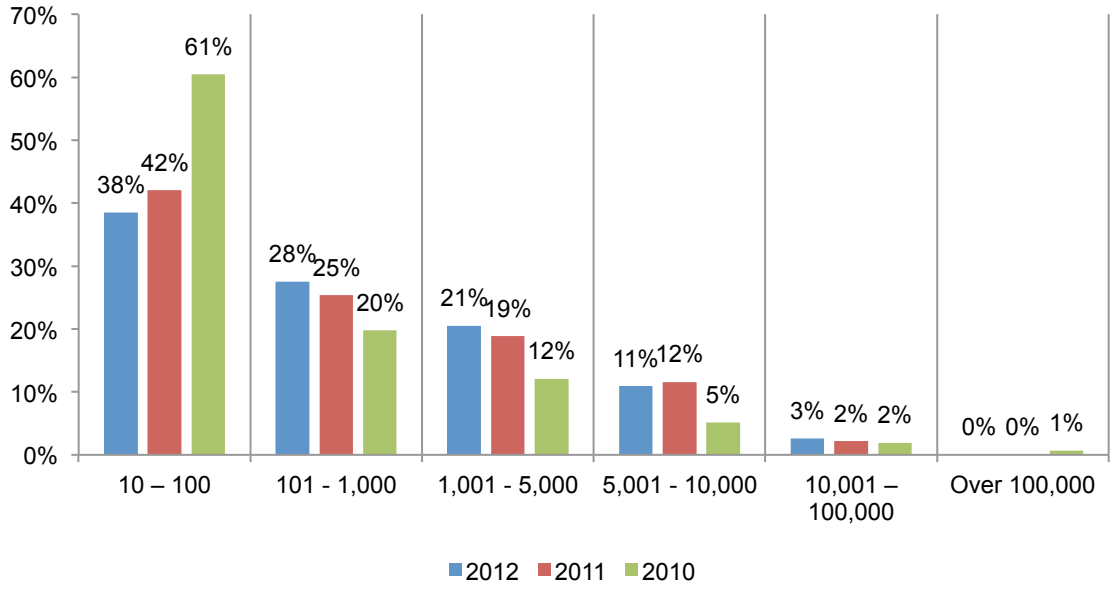
Based on the ranges reported by respondents, the average economic impact of data breaches over the past two years for the healthcare organizations represented in this study is $2.4 million. This is an increase of almost $400,000 since the study was first conducted in 2010. As this finding demonstrates, the average cost to the healthcare industry could potentially be as high as $7 billion annually. The figure also shows that data breaches costing more than $500,000 have increased from 48 percent of healthcare organizations in 2010 to 57 percent of respondents in this year's study.

Figure 3. Economic impact of data breach incidents experienced over the past two years



According to the organizations in this study, the average number of lost or stolen records per breach was 2,769 (Figure 4). Other research conducted by Ponemon Institute has found the average cost per one lost or stolen record is $194. Based on the average number of lost or stolen records in this study, only one data breach could have an economic impact of about $537,186.[3]

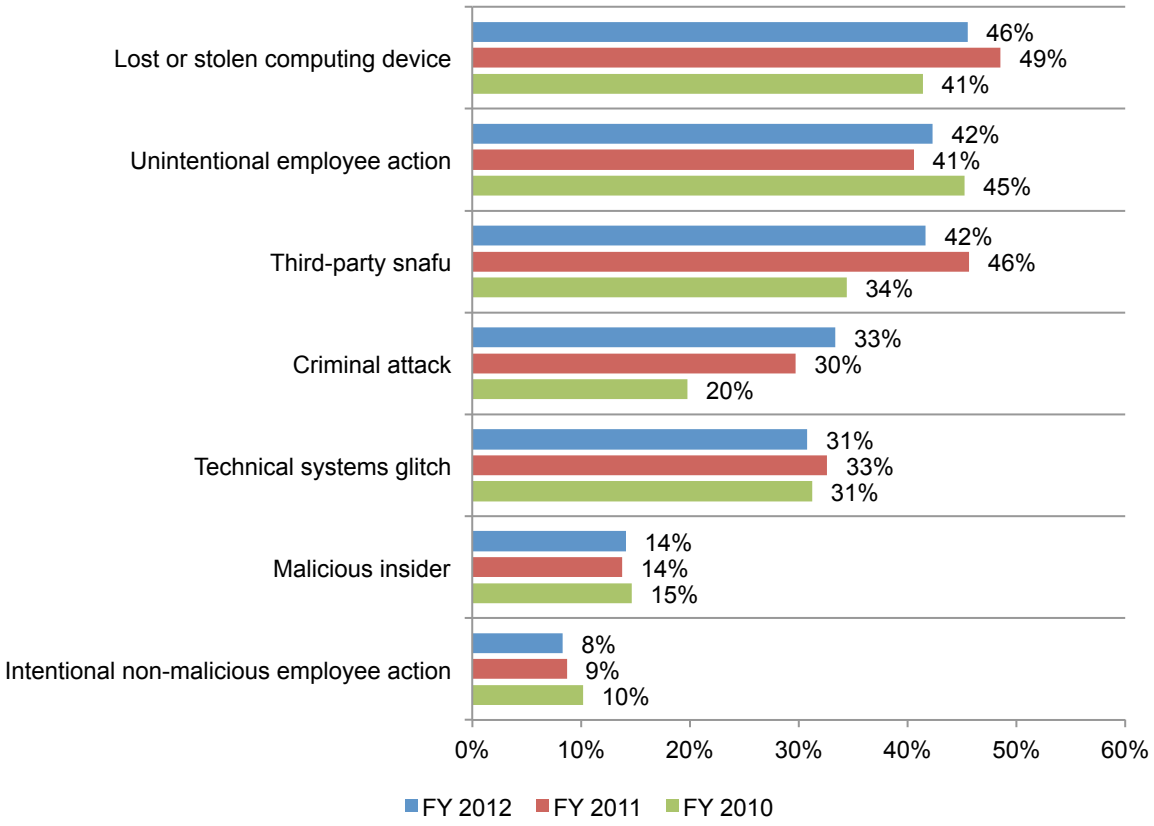
Figure 4. Number of compromised records



[3] See *2011 Cost of a Data Breach*, conducted by Ponemon Institute and sponsored by Symantec, March 2012

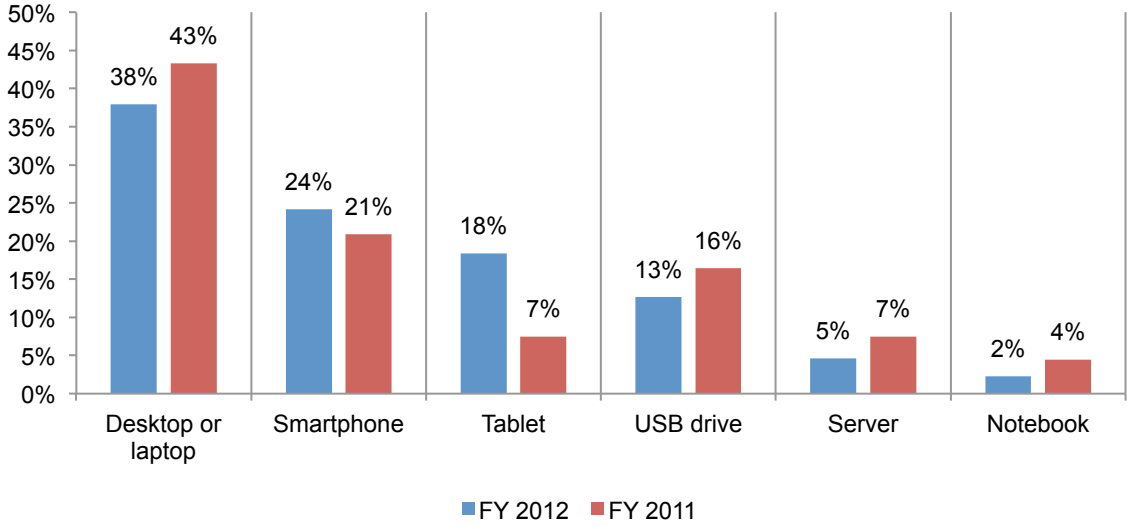
Insider negligence continues to be at the root of the data breach. According to Figure 5, the primary cause of breaches in this study is a lost or stolen computing device (46 percent), which can be attributed in many cases to employee carelessness. This is followed by employee mistakes or unintentional actions (42 percent), and third-party snafus (42 percent). A major challenge for IT security is the increase in criminal attacks, which has increased from 20 percent in 2010 to 33 percent this year.

Figure 5. Nature of the incident
More than one choice permitted



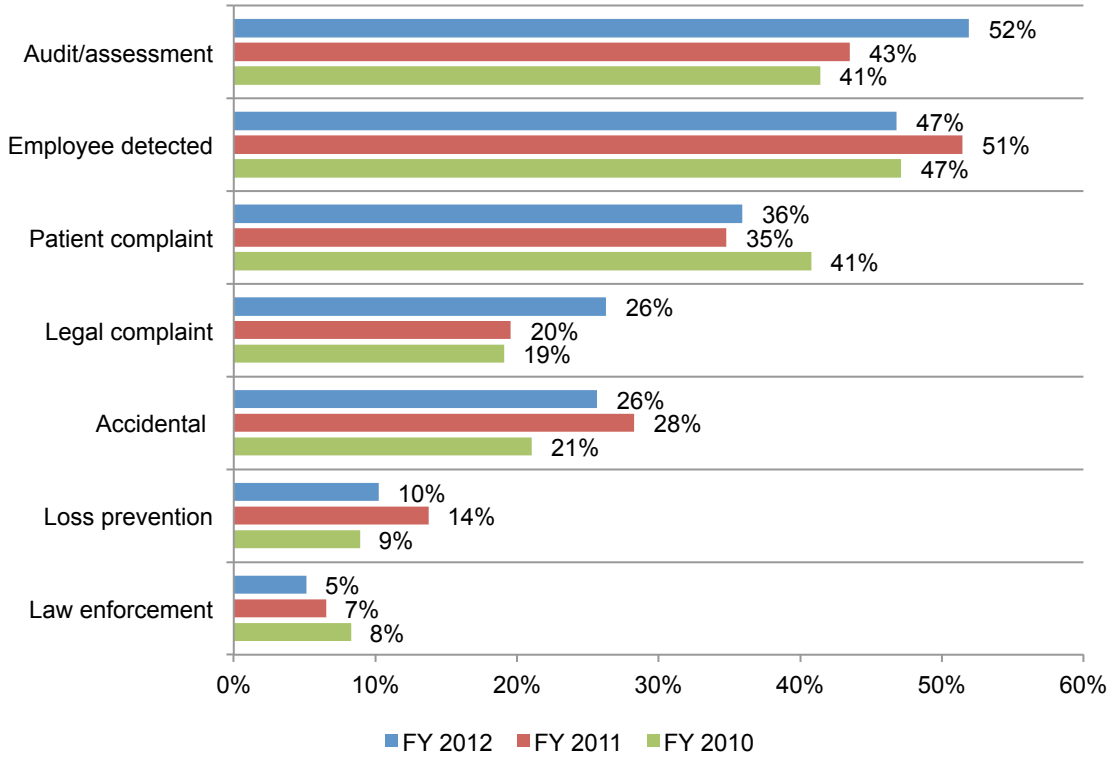
Desktops are still the device most often compromised or stolen but this has declined since last year, as shown in Figure 6. Lost or compromised smartphones and tablets have increased. As shown, tablets have become more vulnerable to loss or theft.

Figure 6. Type of device compromised or stolen



For the first time, according to Figure 7, respondents say the breach was most likely discovered through an audit or an assessment (52 percent) followed by employees detecting the breach (47 percent) and patient complaints (36 percent). Legal complaints as an indicator of a data breach have increased sharply since 2010 and 2011.

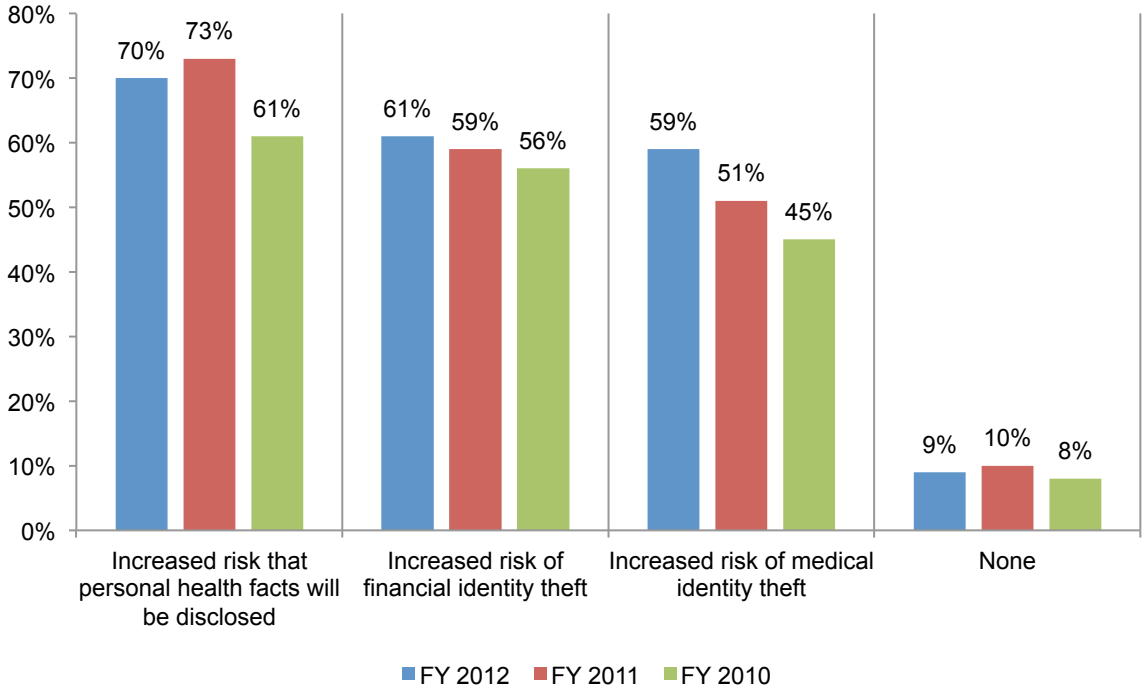
Figure 7. How the data breach was discovered



2. Data breaches put patients and their information at risk for disclosure and financial and medical identity theft.

Respondents acknowledge the harms to patients if their records are lost or stolen. The types of patient data lost or stolen most often are medical files and billing and insurance records, as discussed above. Seventy percent of respondents say there is an increased risk that personal health facts will be disclosed if the records are stolen or lost. This is followed by the risk of financial identity theft and medical identity theft (61 percent and 59 percent, respectively), as shown in Figure 8.

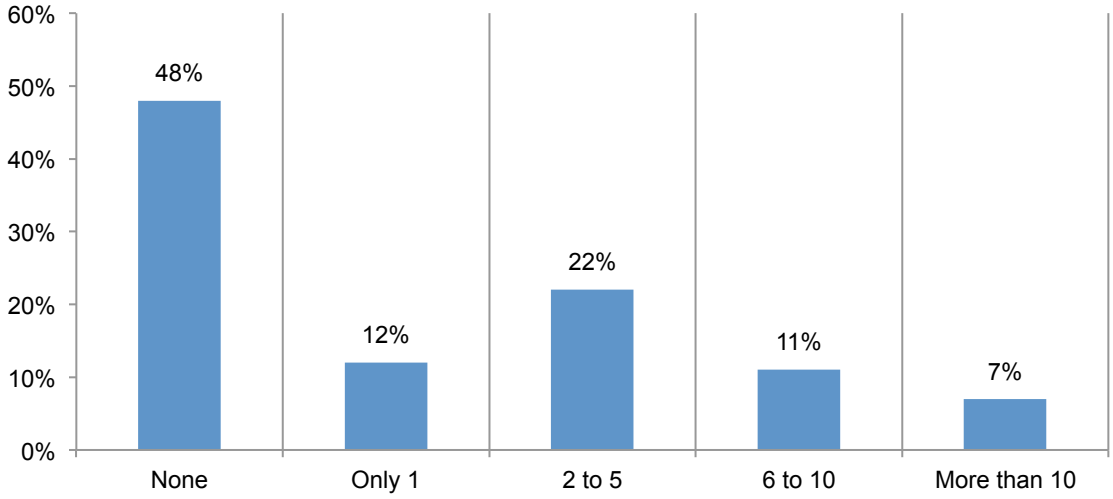
Figure 8. Harms patients suffer if their records are lost or stolen
More than one choice permitted



While there is agreement that patients are at greater risk of financial identity theft if their records are lost or stolen, 65 percent of respondents say their organizations do not offer credit monitoring or other protection services.

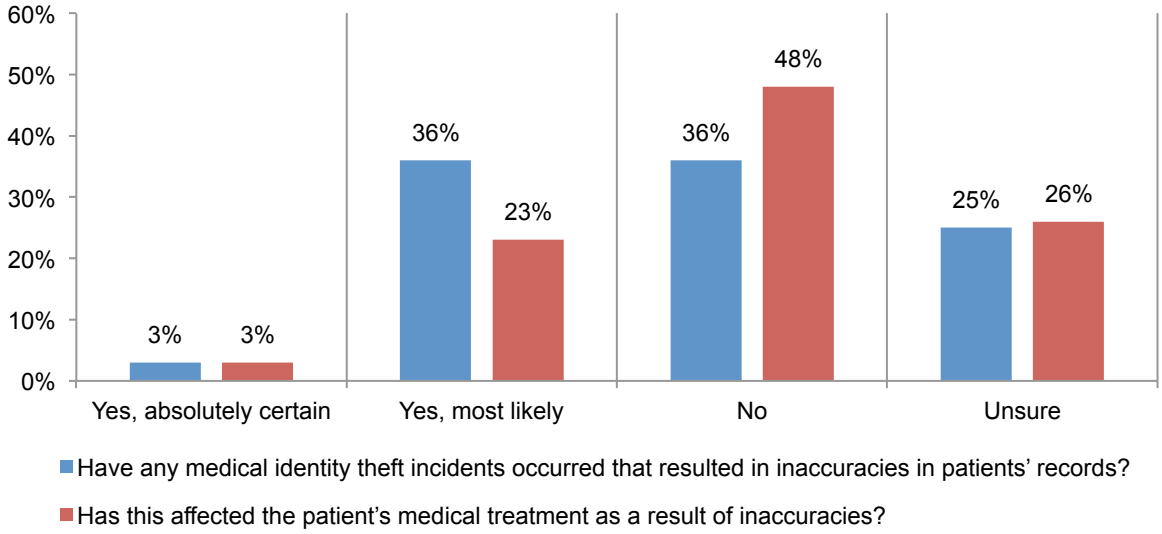
Medical identity theft occurs and can affect patient treatment. As shown in Figure 9, 52 percent of organizations report that their healthcare organizations had one or more incidents of medical identity theft. While only 18 percent say the theft was a result of a data breach, 32 percent are unsure. This uncertainty is due in part to the finding that only one-third say they have sufficient controls in place to detect medical identity theft.

Figure 9. Number of identity theft incidents experienced over the past 12 months



The affect of medical identity theft could prove to be fatal as revealed in Figure 10. Thirty-nine percent (3 percent + 36 percent) of those healthcare organizations that experienced medical identity theft in their organizations say it resulted in inaccuracies in the patient's medical record and 26 percent (3 percent + 23 percent) say it affected the patient's medical treatment.

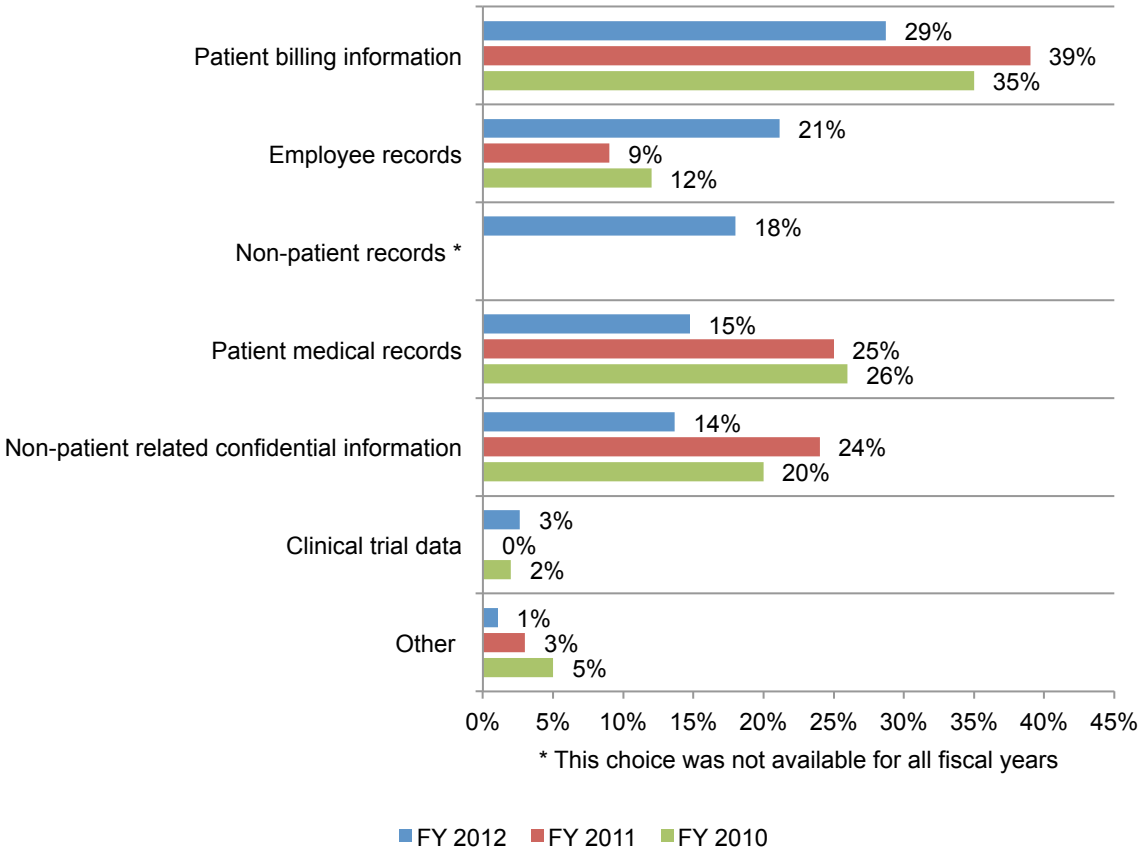
Figure 10. Consequences of medical identity theft on patient records



Employee records are also at risk. Figure 11 reveals that respondents are more confident that patient billing information and medical records will not be susceptible to data loss or theft. In 2011, 39 percent of respondents said patient-billing information was vulnerable. This year the frequency of response declined to 29 percent.

Similarly, the susceptibility of patient medical records declined from 25 percent of respondents in 2011 to 15 percent of respondents who believe this information is most at risk. In contrast, a much higher percentage of respondents in this year's study believe employee records have become the most susceptible to data loss or theft than last year (an increase from 9 percent to 21 percent).

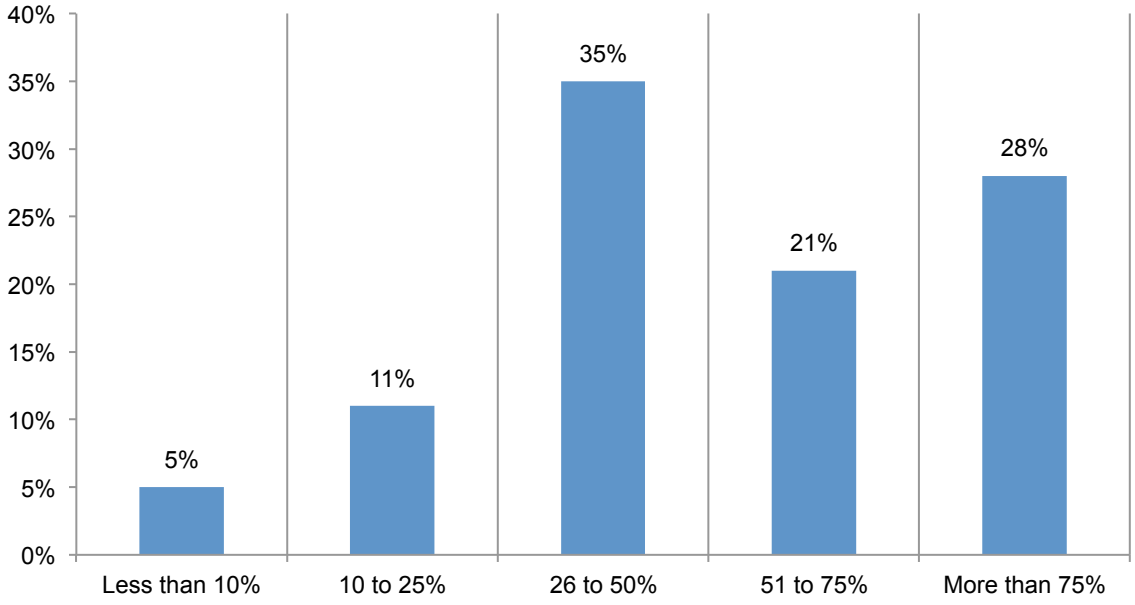
Figure 11. Type of data most susceptible to data loss or theft



3. Technology trends threaten healthcare's ability to protect patient information.

Trends in mobility and employee owned devices put patient data at risk. Eighty-one percent of organizations permit employees and medical staff to use their own mobile devices such as smartphones or tablets to connect to their networks or enterprise systems such as email. Figure 12 shows the percentage of employees allowed to use their personal devices in the workplace. On average, 51 percent of employees are bringing their own devices to the healthcare facility.

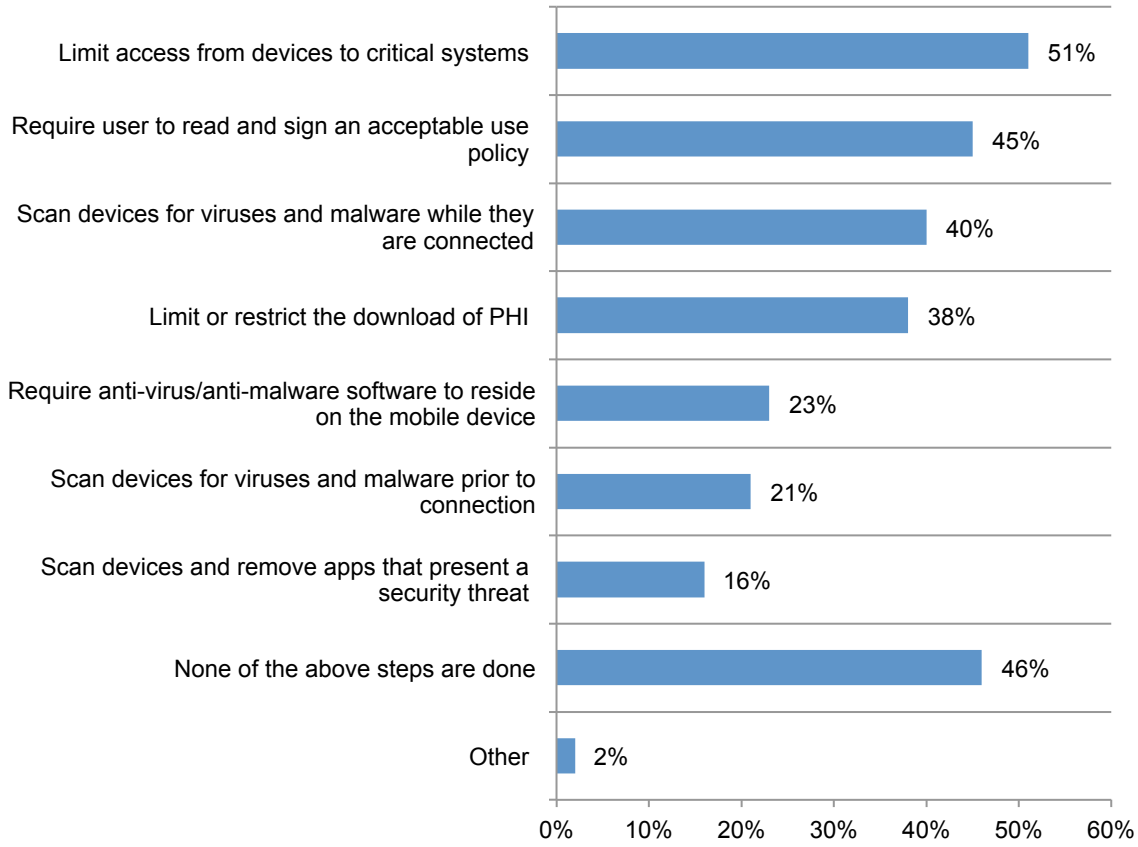
Figure 12. Personally owned mobile device use in the workplace



However, respondents say their organizations are allowing BYOD despite a lack of confidence that they can make sure these devices are secure. According to the findings, 54 percent are not confident and only 9 percent are very confident they are secure.

Steps taken to protect their networks and systems are shown in Figure 13. They are: limiting access from devices to critical systems, including those that connect to PHI, requiring users to read and sign an acceptable use policy prior to connection and scanning devices for viruses and malware while they are connected. However, 46 percent of respondents admit that they do not take these or other precautions listed in the figure.

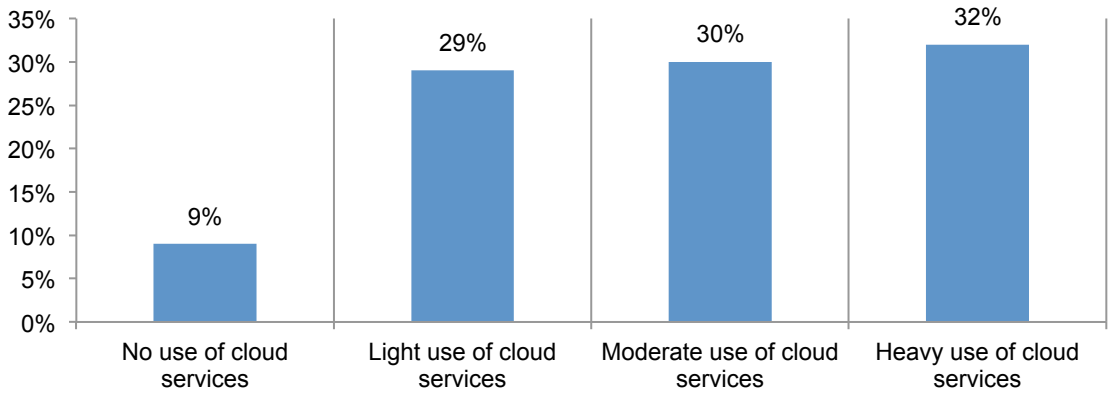
Figure 13. Measures to ensure devices are secure enough to connect to the network
More than one response permitted



Unsecured medical devices are vulnerable to hackers. Medical devices containing sensitive patient information such as wireless heart pumps, mammogram imaging and insulin pumps often use commercial PCs and have wireless connections that make them vulnerable to cyber attacks. According to the healthcare organizations in this study, 69 percent of organizations do not secure medical devices. This finding may reflect the possibility that they believe it is the responsibility of the vendor—not the healthcare provider--to protect these devices.

Healthcare organizations embrace the cloud. According to Figure 14, 62 percent say their organizations make moderate or heavy use of cloud services. Only 9 percent say they do not use cloud services. However, 47 percent of respondents say are not confident that information in the cloud is secure and 23 percent are only somewhat confident.

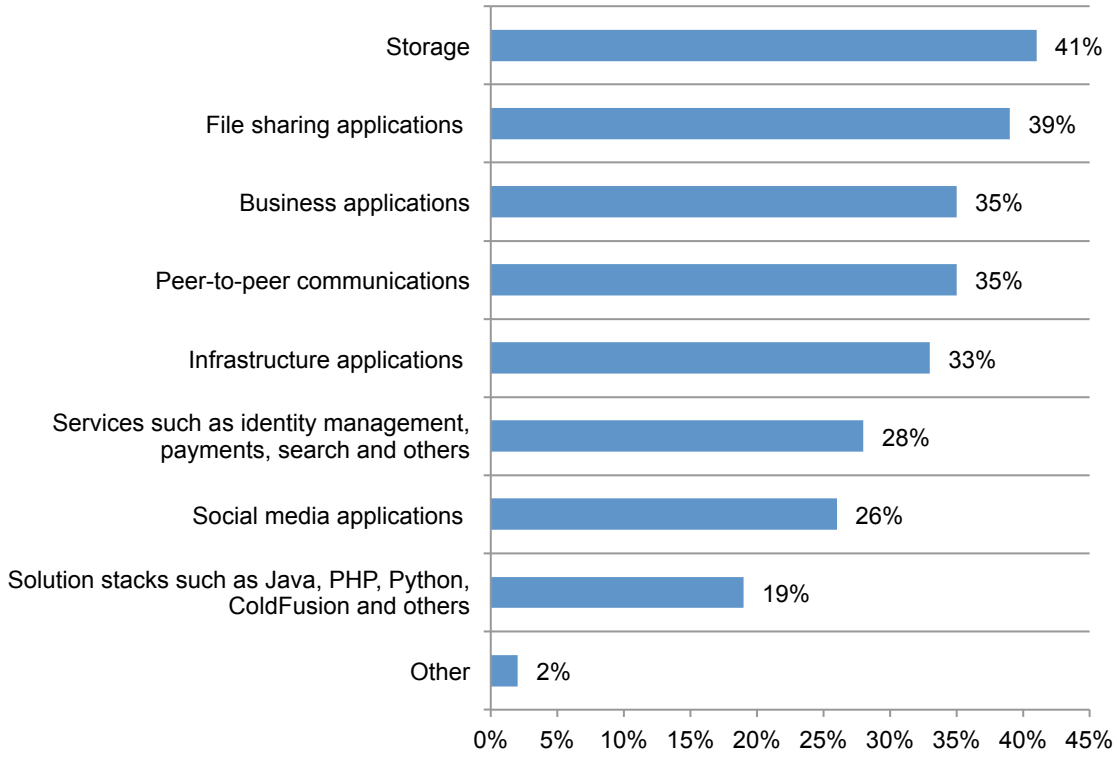
Figure 14. Use of cloud services



Figures 15 and 16 reveal the applications and types of information processed and stored in the cloud. Based on what patient information is in the cloud it is important that organizations ensure cloud computing services meet their security standards.

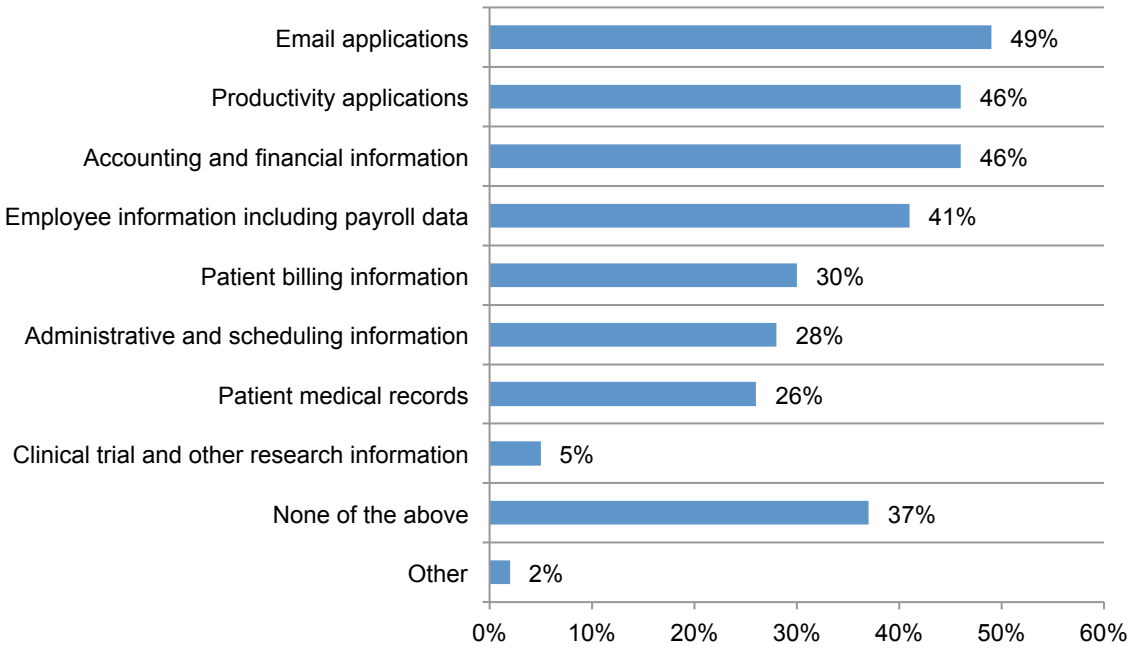
As shown in Figure 15, the applications or services most used are storage, file-sharing applications, business applications, peer-to-peer communications.

Figure 15. Cloud applications or services in use
More than one response permitted



The types of information most often processed or stored in the cloud are email applications, productivity applications, accounting information and employee information such as payroll data (Figure 16). Also processed or stored in the cloud, but not as often, are patient medical records and billing information.

Figure 16. Types of information processed and/or stored in the cloud
More than one response permitted

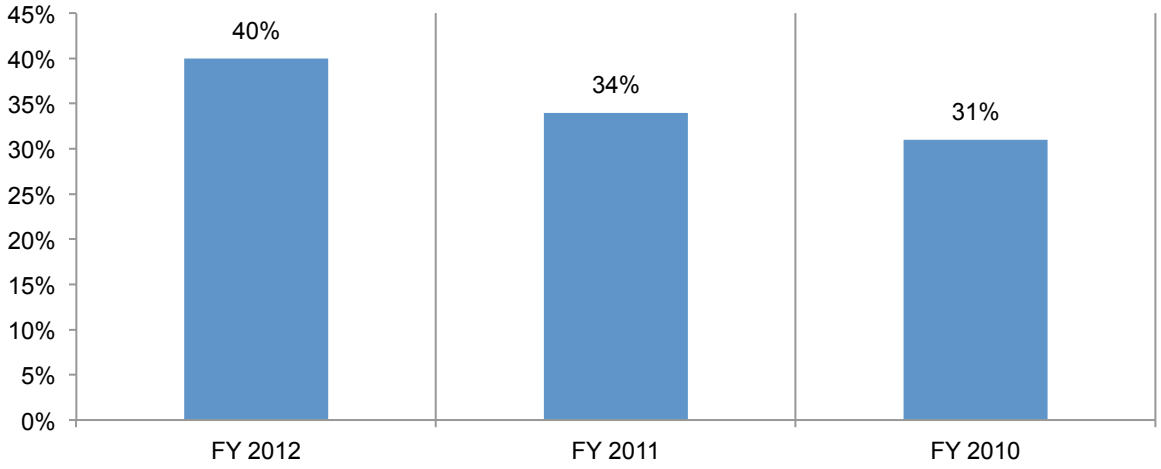


Concerns about the security of Health Information Exchanges (HIE) are keeping organizations from joining. Only 28 percent of organizations say their organization is a member and another 17 percent say they will become a member. More than one-third (35 percent) say they do not plan to become a member of HIE. The primary reason could be that 66 percent of respondents say they are only somewhat confident (30 percent) or not confident (36 percent) in the security and privacy of patient data share on HIEs.

4. Healthcare organizations take steps to prevent breaches but many still lack resources.

Confidence in the ability to prevent and detect a data breach improves but still has far to go. In 2010, only 31 percent of organizations said they had confidence in preventing and detecting patient data loss or theft in their organization. This percentage has been steadily climbing and it is now at 40 percent, as shown in Figure 17. What has improved is that organizations are relying less on an "ad hoc" process and more on policies and procedures and a combination of manual procedures and security technologies.

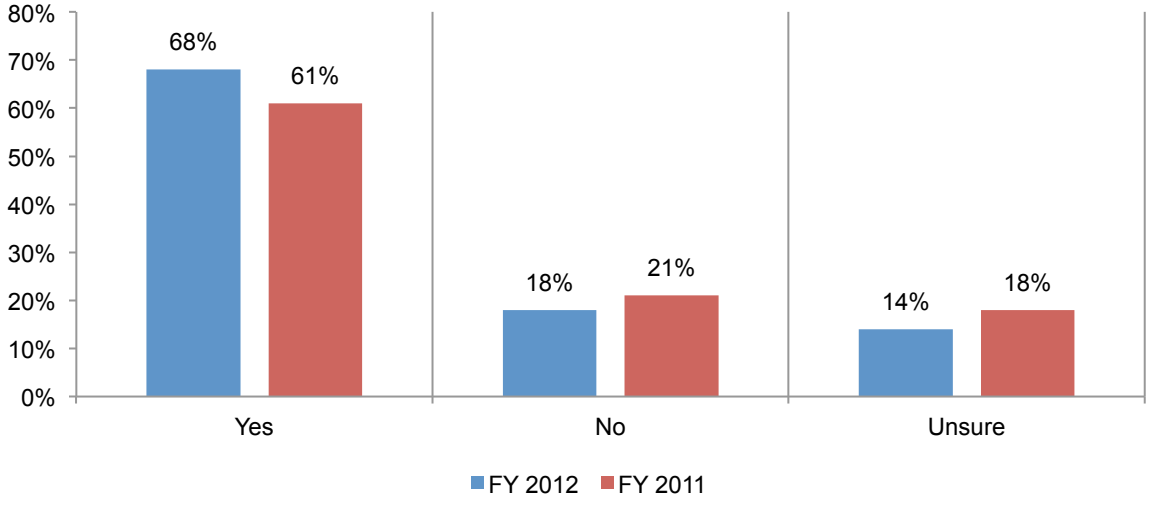
Figure 17. Ability to prevent or detect patient data loss
Very confident and confident response combined



Compliance encourages improvements in privacy and data security. Thirty-six percent of respondents strongly agree and agree that recent Office of Civil Rights (OCR) HHS HIPPA/HITECH audits and fines have affected changes in their organization's patient data privacy and security programs.

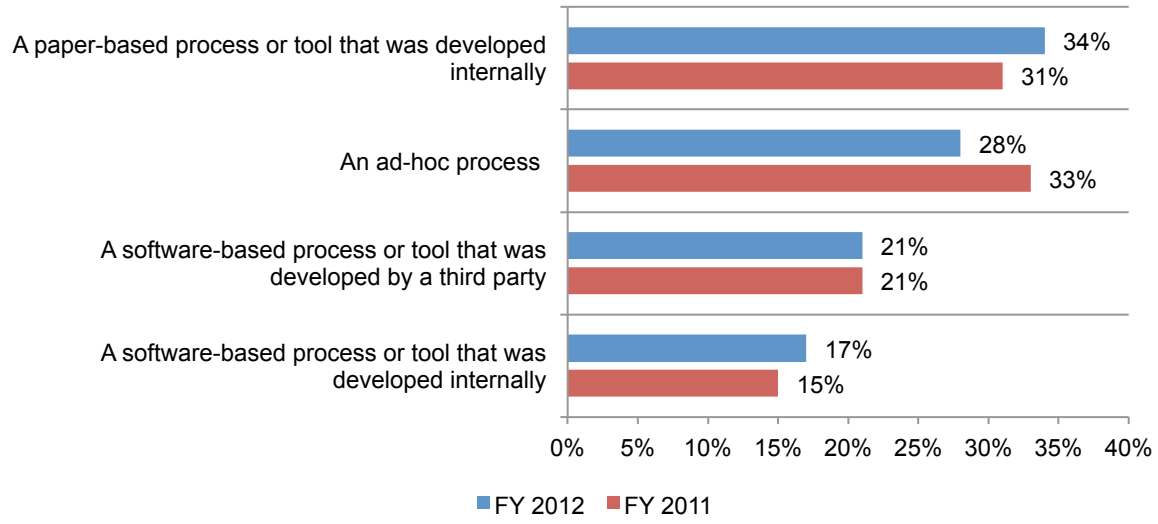
According to Figure 18, 68 percent of organizations conduct and document post data breach incident risk assessments as mandated by the HITECH Act, an increase from 61 percent last year.

Figure 18. Post data breach risk assessments are conducted and documented



As mentioned previously, most data breaches are discovered through the process of conducting an audit or assessment (Figure 19). Further, more organizations are using a paper-based process or software-based process or tool that was developed internally (34 percent and 17 percent, respectively).

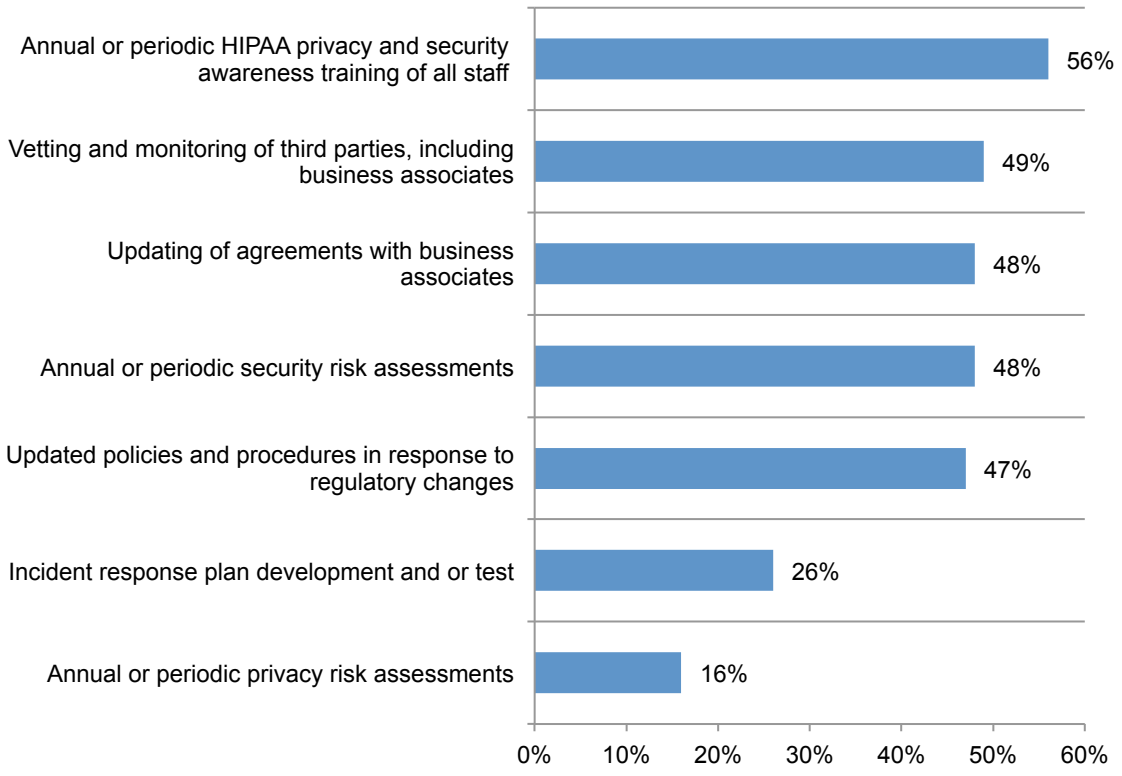
Figure 19. Risk assessment methods



Employee training is the most common activity but does not seem to be effective in reducing insider negligence. Figure 20 reveals that the primary activity conducted by healthcare organizations is to comply with annual or periodic HIPAA privacy and security awareness training of all staff, as reported by 56 percent of the organizations. How effective is the training when employee negligence and mistakes rank second in the root causes of a data breach? This is followed by 49 percent who vet and monitor third parties, including business associates.

Annual or security risk assessments are done by less than half (48 percent) of organizations. The activity performed the least is a periodic privacy risk assessment. While performed the least, privacy risk assessments that evaluate privacy controls and policy may be best able to reduce the frequency of data breaches unintentionally caused by employees.

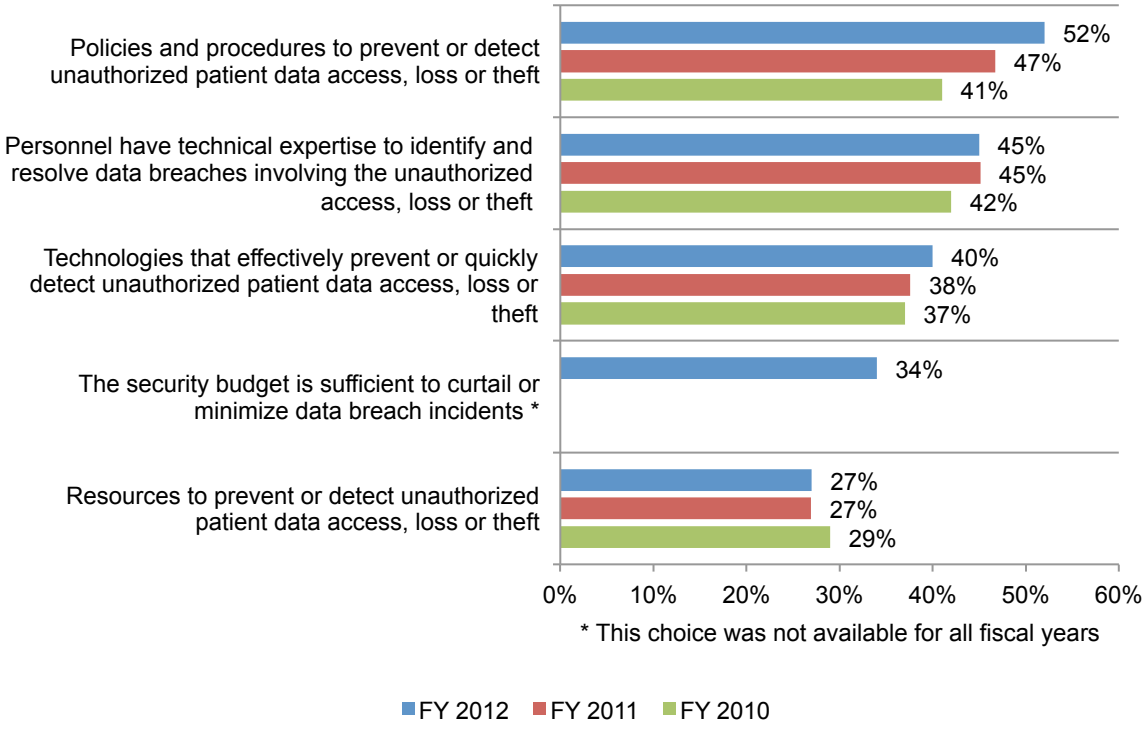
Figure 20. Data protection practices
More than one response permitted



Barriers to achieving a stronger defense against data breaches continue to be a shortage of technologies, funding and expertise. According to Figure 21, 52 percent of respondents agree that they have sufficient policies and procedures to prevent or quickly detect unauthorized patient data access, loss or theft. This increased from 41 percent in 2010 and can be attributed to the need for compliance with regulations.

However, only 27 percent say they have sufficient resources and 34 percent say they have a sufficient security budget. Technologies and personnel are adequate according to 40 percent and 45 percent of respondents.

Figure 21. Attributions about patient data security
Strongly agree and agree response combined



Part 3. Implications and recommendations

Healthcare organizations need to strengthen their privacy and security posture if they are to reduce the number of data breaches occurring in their organizations. The findings suggest a low level of confidence in the ability to safeguard healthcare organizations from the mobility and BYOD risks as well as in being able to detect data breaches and medical identity theft. The following is a list of recommendations:

- Make the business case for investing in people, process and technologies based on the economic impact to healthcare organizations participating in this benchmark research. Consider elevating the chief privacy and security role from the hierarchical organization to one that reports directly to the board of directors.

- Conduct a privacy and security risk assessment annually to understand what practices may be putting your organization at risk. Storing large amounts of confidential data or failing to institute appropriate safeguards limiting access to PHI can expose healthcare organizations to unnecessary risks.

- Create a comprehensive mobile device policy (including detailed guidelines) for all employees and contractors. The policy should address the risks and the security procedures that should be followed. Reinforce your mobile device policy with employee education on the importance of safeguarding their mobile devices and how to avoid risky behaviors.

- Before deploying cloud applications and services, ensure the appropriate security requirements are in place. Depending upon how you are using the cloud, your cloud provider may be considered a business associate under HIPAA. Be sure to evaluate your relationship with your cloud provider and sign a business associate agreement if appropriate.

- Ensure electronic health records (EHR) and HIE plans include rigorous privacy and security analysis and that key privacy and security personnel are actively involved in the implementation teams.

A stronger security posture will lead to greater confidence that patients' confidential and sensitive information is protected and costly financial and medical identity theft incidents will be prevented. Most important, limiting the financial consequences of a data breach can mean that more resources will be spent on the delivery of quality healthcare services.

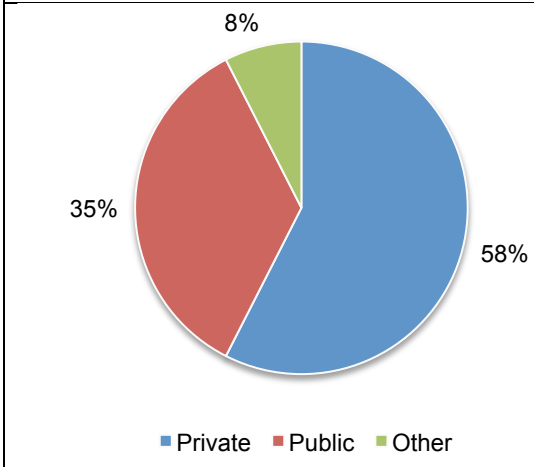
Part 3. Benchmark Methods

Table 1 summarizes the response completed over a three-month period concluding in November 2012. A total of 499 health care organizations were selected for participation and contacted by the researcher. Ninety-two organizations agreed to complete the benchmark survey; however, 81 completed the benchmark instrument. One benchmarked organization was deemed incomplete and, hence, removed from the sample. A final sample of 80 organizations was used in our analysis, which is a net increase of eight organizations from our 2011 study.

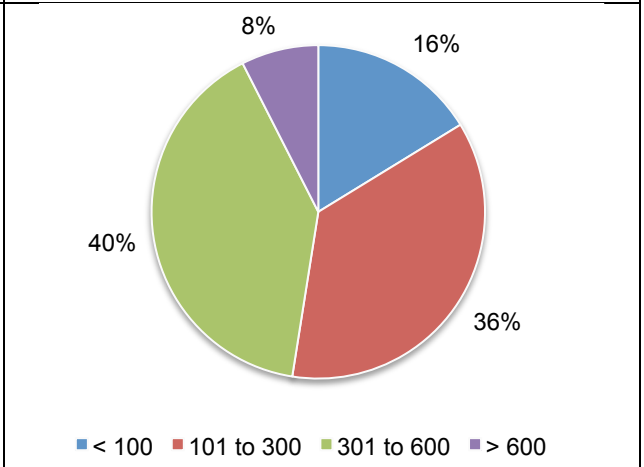
Table 1. Benchmark sampling response	FY 2012	FY 2011	FY 2010
Total healthcare organizations contacts made	499	511	457
Total healthcare organizations recruited	92	98	99
Total healthcare organizations participating	81	75	67
Total healthcare organizations providing incomplete responses	1	3	2
Final benchmark sample	80	72	65

Pie Chart 1 reports the type of healthcare providers that participated in this research, with 58 percent represented private organizations. Pie Chart 2 shows the size of organizations with respect to the number of patient beds. Forty percent of participating healthcare providers have a 301 to 600-bed capacity, while 36 percent have 101 to 300 beds.

Pie Chart 1. Type of health care provider

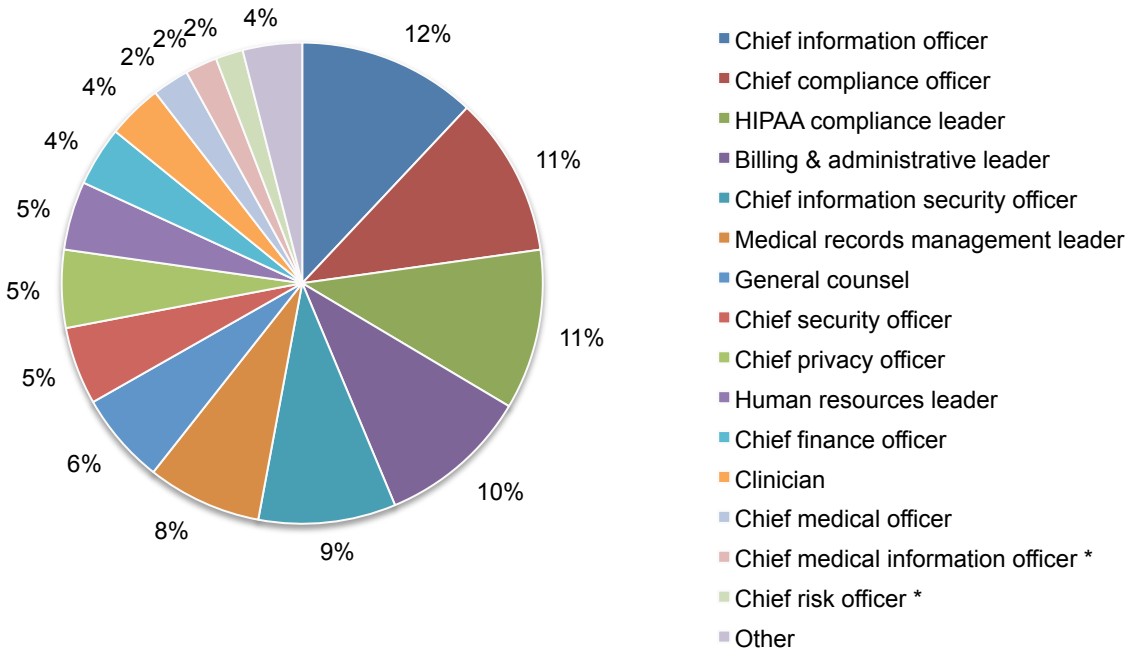


Pie Chart 2. The number of patient beds (size)



According to Pie Chart 3, the primary roles of respondents or their supervisors interviewed in this study are chief information officer (12 percent) chief compliance officer (11 percent) and HIPAA compliance leader (11 percent).

Pie Chart 3. What best describes your role or the role of your supervisor?



* This response was not available for all fiscal years

Part 4. Limitations

The presented findings are based on self-reported benchmark survey returns. Usable returns from 80 organizations – or about 16 percent of those organizations initially contacted – were collected and used in the above-mentioned analysis. It is always possible those organizations that chose not to participate are substantially different in terms of data protection and compliance activities.

Because our sampling frame is a proprietary list of organizations known to the researcher, the quality of our results is influenced by the accuracy of contact information and the degree to which the list is representative of the population of all covered entities and business associates in the United States. While it is our belief that our sample is representative, we do acknowledge that results may be biased in two important respects:

- Survey results are skewed to larger-sized healthcare organizations, excluding the plethora of very small provider organizations including local clinics and medical practitioners.
- Our contact methods targeted individuals who are presently in the data protection, security, privacy or compliance fields. Hence, it is possible that contacting other individuals in these same organizations would have resulted in different findings.

To keep the survey concise and focused, we omitted other normatively important variables from the analyses. Omitted variables might explain survey findings, especially differences between covered entities and business associates as well as organizational size.

The quality of survey research is based on the integrity of confidential responses received from respondents. While certain checks and balances have been incorporated into our survey methods, there is always the possibility that certain respondents did not provide accurate or complete responses to our benchmark instrument.

We fully acknowledge that our sample size is small and, hence, the ability to generalize findings about organizational size, organizational type, and program maturity is limited. Great care should be exercised before attempting to generalize these findings to the population of all health care providers.

Finally, we compare the 2012 results to benchmark studies completed in 2011 and 2010. While these three samples were approximately matched based on organizational size, type and regional location, we can only infer trends from between-sample differences.

Appendix: Detailed Results

The following tables provide the frequency and percentage frequency of all benchmark survey questions completed by 80 participating companies. All field research was completed over a three-month period concluding in November 2012

Benchmark sampling response	FY 2012	FY 2011	FY 2010
Total healthcare organizations contacts made	499	511	457
Total healthcare organizations recruited	92	98	99
Total healthcare organizations participating	81	75	67
Total healthcare organizations providing incomplete responses	1	3	2
Final benchmark sample	80	72	65

Part 1: Organizational characteristics			
Q1a. What best describes your organization:	FY 2012	FY 2011	FY 2010
Public healthcare provider	35%	32%	35%
Private healthcare provider	58%	57%	54%
Other	8%	11%	11%
Total	100%	100%	100%

Q1b. How many patient beds (capacity) does your organization have?	FY 2012	FY 2011	FY 2010
Less than 100	16%	17%	18%
101 to 300	36%	35%	32%
301 to 600	40%	42%	45%
More than 600	8%	7%	5%
Total	100%	100%	100%

Q1c. What best describes your organization's operating structure?	FY 2012	FY 2011	FY 2010
Integrated Delivery System	36%	36%	35%
Hospital or clinic that is part of a healthcare network	46%	47%	46%
Standalone hospital	14%	17%	17%
Standalone Clinic	4%		
Other	0%	0%	2%
Total	100%	100%	100%

Q1d. Please indicate the region of the United States where you are located.	FY 2012	FY 2011	FY 2010
Northeast	21%	22%	23%
Mid-Atlantic	20%	21%	20%
Midwest	16%	15%	15%
Southeast	11%	13%	12%
Southwest	13%	13%	14%
Pacific-West	19%	17%	15%
Total	100%	100%	100%

Q1e. What best describes your role or the role of your supervisor?	FY 2012	FY 2011	FY 2010
Chief security officer	5%	5%	7%
Chief information security officer	9%	10%	9%
Chief information officer	12%	11%	6%
Chief privacy officer	5%	6%	4%
Chief compliance officer	11%	11%	11%
Chief medical officer	2%	3%	1%
Chief clinical officer	1%	1%	0%
Chief risk officer (2012)	2%		
Chief medical information officer (2012)	2%		
Chief finance officer	4%	4%	6%
Chief development officer	1%	2%	2%
General counsel	6%	5%	6%
HIPAA compliance leader	11%	11%	12%
Clinician	4%	3%	1%
Billing & administrative leader	10%	12%	15%
Medical records management leader	8%	11%	13%
Human resources leader	5%	5%	5%
Other	2%	1%	1%
Total	100%	100%	100%
Total number of individual interviews	324	300	211
Average number of interviews per HC organization	4.05	4.17	3.25

Q1f. What best describes your department?	FY 2012	FY 2011	FY 2010
Compliance	94%	100%	91%
Privacy	34%	39%	48%
Information technology (IT)	79%	76%	45%
Legal	21%	21%	20%
Finance	16%	15%	20%
Marketing and communications	6%	8%	6%
Medical informatics	24%	24%	17%
Medical staff	19%	18%	15%
Patient services	48%	47%	38%
Records management	23%	14%	9%
Risk management	6%	15%	9%
Development (foundation)	6%	11%	8%
Planning	10%	4%	6%
Human resources	14%	19%	20%
Other	6%	4%	0%
Total	405%	417%	352%

	Strongly agree and Agree response combined		
Part 2. Attributions. Please rate your opinion about the statements contained next to each statement using the scale provided.	FY 2012	FY 2011	FY 2010
Q2. My organization has sufficient policies and procedures that effectively prevent or quickly detect unauthorized patient data access, loss or theft.	52%	47%	41%
Q3. My organization has sufficient technologies that effectively prevent or quickly detect unauthorized patient data access, loss or theft.	40%	38%	37%
Q4. My organization has sufficient resources to prevent or quickly detect unauthorized patient data access, loss or theft.	27%	27%	29%
Q5. My organization has personnel who have sufficient technical expertise to be able to identify and resolve data breaches involving the unauthorized access, loss or theft of patient data.	45%	45%	42%
Q6. Our organization's security budget is sufficient to curtail or minimize data breach incidents.	34%		
Q7. My organization has personnel who are knowledgeable about HITECH and states' data breach notification laws.	44%		
Q8. Recent Office of Civil Rights (OCR) HHS HIPPA/HITECH audits and fines have affected changes in my organization's patient data privacy and security programs.	36%		

Part 3: Privacy Incidents & Data Breach			
Q9. Has your department suffered a data breach involving the loss or theft of patient data in the past two years as defined above?	2012 Pct%	2011 Pct%	2010 Pct%
No	6%	4%	14%
Yes, 1 incident	16%	17%	26%
Yes, 2 to 5 incidents	33%	33%	31%
Yes, more than 5 incidents	45%	46%	29%
Total	100%	100%	100%
Extrapolated average number of data breaches for the benchmark sample	4.00	4.08	3.09
Extrapolated total number of data breaches for the benchmark sample	320	294	201

Q10. How confident are you that your organization has the ability to detect all patient data loss or theft?	2012 Pct%	2011 Pct%	2010 Pct%
Very confident	13%	12%	11%
Confident	33%	31%	31%
Little confidence	31%	33%	35%
No confidence	23%	24%	23%
Total	100%	100%	100%

Q11. Two separate data breach incidents over the past two years.	FY 2012	FY 2011	FY 2010
Number of incidents reported	320	294	201
Number of observed incidents used in the analysis of Q11	156	138	157

11a. Approximate number of compromised records	FY 2012	FY 2011	FY 2010
10 – 100	38%	42%	61%
101 - 1,000	28%	25%	20%
1,001 - 5,000	21%	19%	12%
5,001 - 10,000	11%	12%	5%
10,001 – 100,000	3%	2%	2%
Over 100,000	0%	0%	1%
Total	100%	100%	100%
Extroplated average number of lost or stolen records over two years	2,769	2,575	1,769

11b. Nature of the incident	FY 2012	FY 2011	FY 2010
Unintentional employee action	42%	41%	45%
Intentional non-malicious employee action	8%	9%	10%
Technical systems glitch	31%	33%	31%
Criminal attack	33%	30%	20%
Malicious insider	14%	14%	15%
Third-party snafu	42%	46%	34%
Lost or stolen computing device	46%	49%	41%
Total	216%	220%	197%
*More than one selection is permitted			

11c. Type of device compromised or stolen	FY 2012	FY 2011
None		
Desktop or laptop	38%	43%
Smartphone	24%	21%
Tablet	18%	7%
Notebook	2%	4%
Server	5%	7%
USB drive	13%	16%
Total	100%	100%

11d. Type of patient data lost or stolen	FY 2012	FY 2011
Medical file	48%	47%
Billing and insurance record	48%	49%
Scheduling details	19%	25%
Prescription details	20%	19%
Payment details	24%	17%
Monthly statements	15%	20%
Other	2%	3%
Total	176%	180%
*More than one selection is permitted		

11e. How the data breach was discovered	FY 2012	FY 2011	FY 2010
Accidental	26%	28%	21%
Loss prevention	10%	14%	9%
Patient complaint	36%	35%	41%
Law enforcement	5%	7%	8%
Legal complaint	26%	20%	19%
Employee detected	47%	51%	47%
Audit/assessment	52%	43%	41%
Total	202%	198%	187%
*More than one selection is permitted			

11f. Offer of protection services	FY 2012	FY 2011
None offered	65%	65%
Credit monitoring	22%	19%
Other identity monitoring	4%	6%
Insurance	1%	1%
Identity restoration	7%	9%
Other	0%	0%
Total	100%	100%
*More than one selection is permitted		

Q12. In your opinion (best guess), what best describes the lifetime economic value, on average, of one patient or customer to your organization?	FY 2012	FY 2011	FY 2010
Less than $10,000	9%	10%	12%
$10,001 to $50,000	32%	31%	29%
$50,001 to $100,000	24%	23%	21%
$100,001 to $200,000	12%	10%	13%
$200,001 to $500,000	7%	4%	5%
$500,001 to $1 million	3%	3%	3%
More than $1 million	2%	3%	2%
Cannot determine	11%	16%	15%
Total	100%	100%	100%
Average lifetime value of one lost patient (customer)	$111,810	$113,400	$107,580

Q13. In your opinion (best guess), what best describes the economic impact of data breach incidents experience by your organization over the past two years?	FY 2012	FY 2011	FY 2010
Less than $10,000	3%	5%	4%
$10,001 to $50,000	1%	2%	1%
$50,001 to $100,000	3%	3%	4%
$100,001 to $200,000	8%	8%	11%
$200,001 to $500,000	23%	26%	25%
$500,001 to $1 million	26%	21%	19%
More than $1 million	31%	30%	29%
Cannot determine	5%	5%	7%
Total	100%	100%	100%
Average economic impact of data breach over the past two years	$2,390,270	$2,243,700	$2,060,174

Q14. Does your EHR (electronic healthcare records) system allow your organization to comply with the HHS mandated requirements to protect patient privacy?	FY 2012
Yes	22%
Partially	29%
No	19%
We don't use EHRs	30%
Total	100%

Q15. Is your organization a member of a Health Information Exchange (HIE), defined as the mobilization of healthcare information electronically across organizations within a region, community or hospital system?	FY 2012
Yes	28%
We will become a member	17%
We are considering membership	20%
No, we do not plan to become a member of HIE	35%
Total	100%

Q16. What is your level of confidence as to the security and privacy of patient data shared on Health Information Exchanges?	FY 2012
Very confident	17%
Confident	17%
Somewhat confident	30%
Not confident	36%
Total	100%

Q17a. Does your organization permit employees and medical staff to use their own mobile devices such as smartphones or tablets to connect to your organization's networks or enterprise systems (such as email)?	FY 2012
Yes	81%
No	19%
Total	100%

Q17b. If yes, approximately what percentage of your organization's employees (including part-time and contract employees) use their personallly owned mobile device such as a smartphone or tablet?	FY 2012
Less than 10%	5%
10 to 25%	11%
26 to 50%	35%
51 to 75%	21%
More than 75%	28%
Total	100%
Extrapolated value	51%

Q17c. If yes, how does your organization ensure these personally owned mobile devices are secure enough to connect to your organization’s network or enterprise systems? Please select all that apply.	FY 2012
Scan devices for viruses and malware prior to connection	21%
Scan devices and remove all mobile apps that present a security threat prior to connection	16%
Scan devices for viruses and malware while they are connected	40%
Require anti-virus/anti-malware software to reside on the mobile device prior to connection	23%
Require user to read and sign an acceptable use policy prior to connection	45%
Limit access from devices to critical systems including those that connect to PHI	51%
Limit or restrict the download of PHI onto these devices	38%
None of the above steps are done	46%
Other (please specify)	2%
Total	282%

Q17d. If yes, what is your level of confidence as to the security of the personally-owned mobile devices used in your organization?	FY 2012
Very confident	9%
Confident	16%
Somewhat confident	21%
Not confident	54%
Total	100%

18a. Does your organization use social media to engage with patients?	FY 2012
Yes	42%
No	58%
Total	100%

18b. If yes, what is your level of confidence that the patient data shared on your organization's social media forums is secure?	FY 2012
Very confident	10%
Confident	17%
Somewhat confident	23%
Not confident	50%
Total	100%

Q19. Does the scope of your organization's IT security and/or data protection activities include the security of FDA-approved medical devices such as those attached or not attached to the patient (such as insulin pumps or medical imaging equipment)?	FY 2012
Yes	31%
No	69%
Total	100%

Cloud services refer to distributed computing solutions that can be owned by third-parties on data center locations outside the end-user company's IT infrastructure. Consumers of cloud computing services purchase capacity on-demand and are not concerned with the underlying technologies used to increase computing capacity.

Q20. What best describes your organization's use of cloud services?	FY 2012
No use of cloud services (skip to Q25)	9%
Light use of cloud services	29%
Moderate use of cloud services	30%
Heavy use of cloud services	32%
Total	100%

Q21. What cloud applications or services does your organization presently use? Please select all that apply.	FY 2012
Peer-to-peer communications (such as Skype)	35%
Social media applications (such as Facebook, YouTube, Twitter, etc.)	26%
File sharing applications such as DropBox, Box.net and others	39%
Business applications (such as Google Docs, webmail, etc.)	35%
Infrastructure applications (online backup, security, archiving, etc.)	33%
Services such as identity management, payments, search and others	28%
Solution stacks such as Java, PHP, Python, ColdFusion and others	19%
Storage	41%
Other (please specify)	2%
Total	258%

Q22. What types of information does your organization process and/or store in the cloud environment? Please check all that apply	FY 2012
Patient medical records	26%
Patient billing information	30%
Clinical trial and other research information	5%
Employee information including payroll data	41%
Administrative and scheduling information	28%
Accounting and financial information	46%
Email applications	49%
Productivity applications	46%
None of the above	37%
Other (please specify)	2%
Total	310%

Q23. What types of information does your organization consider **too sensitive** to be processed and/or stored in the cloud environment? Please check all that apply.	FY 2012
Patient medical records	56%
Patient billing information	51%
Clinical trial and other research information	37%
Employee information including payroll data	34%
Administrative and scheduling information	29%
Accounting and financial information	33%
Email applications	15%
Productivity applications	18%
None of the above	35%
Other (please specify)	2%
Total	310%

Q24. How confident are you that information in the cloud is secure?	FY 2012
Very confident	11%
Confident	19%
Somewhat confident	23%
Not confident	47%
Total	100%

Part 5. IT and Data Protection Practices			
Q25. What type of data is most susceptible to data loss or theft within your department (please select only one)?	FY 2012	FY 2011	FY 2010
Patient billing information	29%	39%	35%
Patient medical records	15%	25%	26%
Clinical trial data	3%	0%	2%
Employee records	21%	9%	12%
Non-patient records	18%		
Non-patient related confidential information	14%	24%	20%
Other (please specify)	1%	3%	5%
Total	100%	100%	100%

Q26. How has the threat of an OCR HIPAA Audit affected changes in your organization (select the top two changes)?	FY 2012
Required an update of our policies and procedures	57%
Conducted employee training	27%
Conducted a risk assessment/risk analysis	60%
Purchased cyber insurance	9%
No changes	47%
Total	200%

Q27. What best describes the process for preventing and detecting data breach incidents in your organization today? Please select one best choice.	FY 2012	FY 2011	FY 2010
An "ad hoc" process	23%	27%	35%
Mostly a process that relies on policies and procedures	28%	29%	23%
Mostly a process that relies on security technologies	20%	21%	16%
A combination of manual procedures and security technologies	24%	19%	20%
None of the above	5%	4%	6%
Total	100%	100%	100%

Q28. How confident are you that your organization has the ability to prevent or quickly detect patient data loss or theft in your organization?	FY 2012	FY 2011	FY 2010
Very confident and confident response combined	40%	34%	31%

Q29. Does your organization perform the following activities (Please check all that apply)?	FY 2012
Annual or periodic privacy risk assessments	16%
Annual or periodic security risk assessments	48%
Incident response plan development and or test	26%
Updated policies and procedures in response to regulatory changes	47%
Annual or periodic HIPAA privacy and security awareness training of all staff	56%
Vetting and monitoring of third parties, including business associates	49%
Updating of agreements with business associates	48%
Total	290%

Post-incident risk assessment The HITECH Act's Breach Notification Rule requires organizations to have a process for performing an incident risk assessment for each privacy incident as described in the Administrative Burden of Proof (45 CFR 164.414) provision of the Act. The level of risk or harm found by the incident risk assessment determines whether a data breach has occurred and therefore must follow the data breach notification requirements under the breach notification rule.

Q30a. Does your organization conduct and document post data breach incident risk assessments as mandated by the HITECH Act?	FY 2012	FY 2011
Yes	68%	61%
No	18%	21%
Unsure	14%	18%
Total	100%	100%

Q30b. If yes, which one of the following choices best describes your process?	FY 2012	FY 2011
An ad-hoc process	28%	33%
A paper-based process or tool that was developed internally	34%	31%
A software-based process or tool that was developed internally	17%	15%
A software-based process or tool that was developed by a third party	21%	21%
Total	100%	100%

Medical identity theft is defined as the theft of a patient's health credential to obtain medical treatment, services and products (devices).

Q31. How many separate medical identity theft incidents did your organization experience over the past 12 months?	FY 2012
None	48%
Only 1	12%
2 to 5	22%
6 to 10	11%
More than 10	7%
Total	100%
Extrapolated value	2.5

Q32. Were any of these medical identity theft incidents the result of a data breach experienced by your organization?	2012 Pct%
Yes, absolutely certain	3%
Yes, most likely	15%
No	50%
Unsure	32%
Total	100%

Q33a. Have any medical identity theft incidents occurred that resulted in inaccuracies in patients' records?	2012 Pct%
Yes, absolutely certain	3%
Yes, most likely	36%
No	36%
Unsure	25%
Total	100%

Q33b. If yes, has this affected the patient's medical treatment as a result of inaccuracies?	2012 Pct%
Yes, absolutely certain	3%
Yes, most likely	23%
No	48%
Unsure	26%
Total	100%

Q34. In your opinion, does your organization have sufficient controls or procedures in place to prevent and/or quickly detect medical identity theft incidents?	2012 Pct%
Yes	33%
No	67%
Total	100%

Q35. In your opinion, what harms do patients actually suffer if their records are lost or stolen?	FY 2012	FY 2011	FY 2010
Increased risk of financial identity theft	61%	59%	56%
Increased risk of medical identity theft	59%	51%	45%
Increased risk that personal health facts will be disclosed	70%	73%	61%
None	9%	10%	8%
Total	199%	193%	170%

Credit monitoring is defined as monitoring of changes to an individual's credit report such as the creation of new credit accounts.

Q36. Do you believe credit monitoring is effective in preventing or detecting medical identity theft?	FY 2012	FY 2011
Yes	18%	28%
No	69%	72%
Unsure	13%	0%
Total	100%	100%

Q37. If you do not believe or are unsure that credit monitoring is effective, do you believe that another solution for the prevention and detection of medical identity theft is needed?	FY 2012	FY 2011
Yes	46%	74%
No	23%	11%
Unsure	31%	15%
Total	100%	100%

.

For more information about this study, please contact Ponemon Institute by sending an email to research@ponemon.org or calling our toll free line at 1.800.887.3118.

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the **Council of American Survey Research Organizations (CASRO)**, we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.