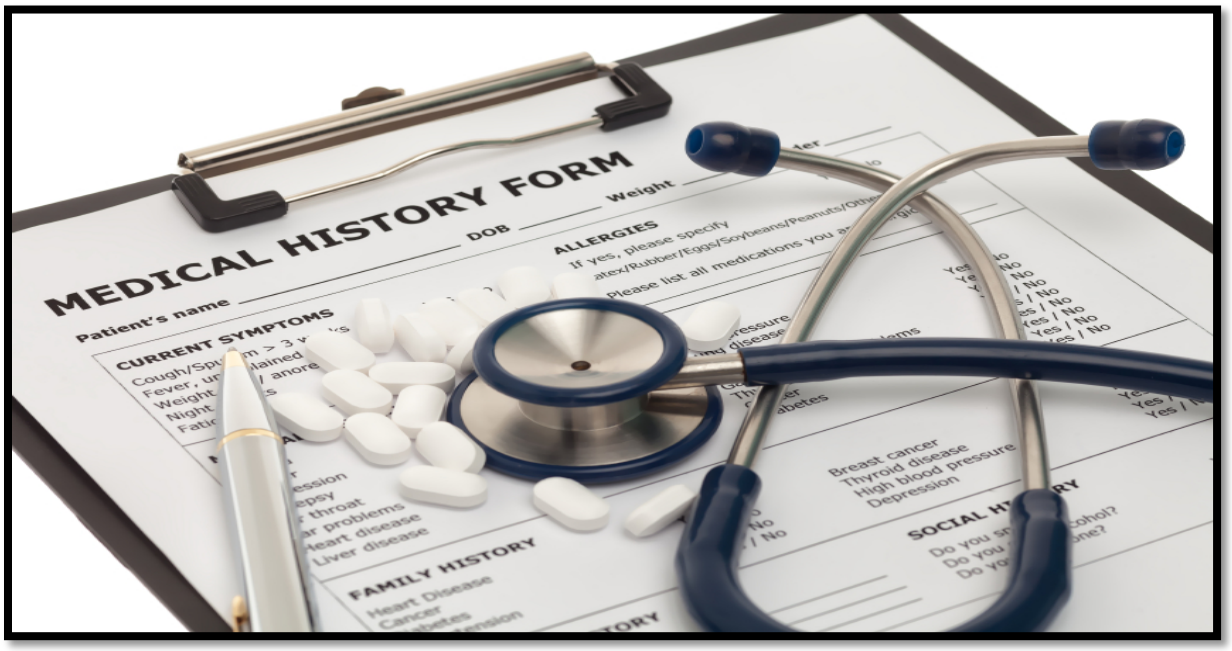
Ponemon INSTITUTE



Fourth Annual Benchmark Study on Patient Privacy & Data Security

Sponsored by ID Experts

Independently conducted by Ponemon Institute LLC

Publication Date: March 2014

Fourth Annual Benchmark Study on Patient Privacy & Data Security

Presented by Ponemon Institute
March 2014

Part 1. Introduction

The *Fourth Annual Study on Patient Privacy & Data Security* reveals new and expanded threats to the security and privacy of patient information in the U.S. healthcare system. The Affordable Care Act (ACA) is seen as a contributing factor because of the documented insecure websites, databases and health information exchanges that are highly vulnerable to insider and outsider threats. While the total number of data breaches has declined slightly over previous years, almost every healthcare organization represented in this research had a data breach. The study also found that healthcare organizations continue to struggle to comply with increasing complex federal and state privacy and security regulations.

Criminal attacks on healthcare systems have risen a startling 100 percent since we first conducted this study four years ago in 2010. Healthcare employees are fueling breach risks by increased use of their personal unsecured devices (smartphones, laptops and tablets). Business Associates—those that have access to PHI and work with healthcare organizations—are not yet in compliance with the HIPAA Final Rule.

Data breaches continue to cost some healthcare organizations millions of dollars every year. While the cost can range from less than $10,000 to more than $1 million, we calculate that the average cost for the organizations represented in this year's benchmark study is approximately $2 million over a two-year period. This is down from $2.4 million in last year's report as well as from the $2.2 million reported in 2011 and $2.1 million in 2010. Based on the experience of the healthcare organizations in this benchmark study, we believe the potential cost to the healthcare industry could be as much as $5.6 billion annually.[1]

The types of healthcare organizations participating in the study are hospitals or clinics that are part of a healthcare network (49 percent), integrated delivery systems (34 percent) and standalone hospital or clinic (17 percent). This year 91 healthcare organizations participated in this benchmark research and 388 interviews were conducted[2]. All organizations in this research are subject to HIPAA as a covered entity. Most respondents interviewed work in compliance, IT, patient services and privacy.

Key Research Findings:

The number of data breaches decrease slightly. Ninety percent of healthcare organizations in this study have had at least one data breach in the past two years. However, 38 percent report that they have had more than five incidents. This is a decline from last year's report when 45 percent of organizations had more than 5. This coupled with an increase in organizations' level of confidence in data breach detections suggests that modest improvements have been made in reducing threats to patient data.

Healthcare organizations improve ability to control data breach costs. 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 $2.0 million. This is a decrease of almost $400,000 or 17 percent since last year.

[1] This is based on multiplying $986,948 (50% of the average two year cost of a data breach experienced by the 91 healthcare organizations in this research) x 5,723 (the total number of registered US hospitals per the AHA).
[2] Benchmark research differs from survey research. The unit of analysis in benchmark research is the organization and in survey research it is the individual.

ACA increases risk to patient privacy and information security. Respondents in 69 percent of organizations represented believe the ACA significantly increases (36 percent) or increases (33 percent) risk to patient privacy and security. The primary concerns are insecure exchange of patient information between healthcare providers and government (75 percent of organizations), patient data on insecure databases (65 percent) and patient registration on insecure websites (63 percent of organizations).

ACO participation increases data breach risks. Fifty-one percent of organizations say they are part of an Accountable Care Organization (ACO) and 66 percent say the risks to patient privacy and security due to the exchange of patient health information among participants has increased. When asked if their organization experienced changes in the number of unauthorized disclosure of PHI, 41 percent say it is too early to tell. Twenty-three percent say they noticed an increase.

Confidence in the security of Health Information Exchanges (HIEs) remains low. An HIE is defined as the mobilization of healthcare information electronically across organizations within a region, community or hospital system. The percentage of organizations joining HIEs increased only slightly. This year, 32 percent say they are members and this is up slightly from 28 percent last year. One-third of organizations say they do not plan to become a member. The primary reason could be that 72 percent of respondents say they are only somewhat confident (32 percent) or not confident (40 percent) in the security and privacy of patient data share on HIEs.

Criminal attacks on healthcare organizations increase 100 percent since 2010. Insider negligence continues to be at the root of most data breaches reported in this study but a major challenge for healthcare organizations is addressing the criminal threat. These types of attacks on sensitive data have increased 100 percent since the study was conducted in 2010 from 20 percent of organizations reporting criminal attacks to 40 percent of organizations in this year's study.

Employee negligence is considered the biggest security risk. Seventy-five percent of organizations say employee negligence is their biggest worry followed by use of public cloud services (41 percent), mobile device insecurity (40 percent) and cyber attackers (39 percent).

BYOD usage continues to rise. Despite the concerns about employee negligence and the use of insecure mobile devices, 88 percent of organizations permit employees and medical staff to use their own mobile devices such as smart phones or tablets to connect to their organization's networks or enterprise systems such as email. Similar to last year, more than half of organizations are not confident that the personally-owned mobile devices or BYOD are secure.

Heavy use of cloud services increases. As discussed above, healthcare organizations view the use of public cloud services as a serious threat. In fact, only one-third are very confident or confident that information in a public cloud environment is secure. Despite the risk, 40 percent of organizations say they use the cloud heavily, an increase from 32 percent last year. The applications or services most used are backup and storage, file-sharing applications, business applications and document sharing and collaboration.

Half of healthcare organizations are compliant with the post-incident risk assessment requirement in the Final Rule. Fifty-one percent of respondents said they are in full compliance while 49 percent report they are not compliant or are only partially compliant. Thirty-nine percent say their incident assessment process is not effective and cite a lack of consistency and inability to scale their process as the primary reasons.

Healthcare organizations don't trust their third parties or business associates with sensitive patient information. Seventy-three percent of organizations are either somewhat confident (33 percent) or not confident (40 percent) that their business associates would be able to detect, perform an incident risk assessment and notify their organization in the event of a data breach incident as required under the business associate agreement. The business associates

they worry most about are IT service providers, claims processor and benefits management. Only 30 percent are very confident or confident that their business associates are appropriately safeguarding patient data as required under the Final Rule.

Organizations rely on policies and procedures to achieve compliance and secure sensitive information. Fifty-five percent of organizations agree they have the policies and procedures that effectively prevent or quickly detect unauthorized patient data access, loss or theft. Unfortunately, the budget, technologies and resources needed to safeguard patient information from a data breach are not as available. Further, less than half (46 percent) of organizations have personnel who are knowledgeable about HITECH and states' data breach notification laws.

Majority of organizations say the HIPAA Final Rule has either not affected patient data privacy and security programs or it's too early to tell. The HIPAA Final Omnibus Rule seeks to better protect patients by removing the harm threshold. Covered entities and their business associates must still conduct an incident risk assessment, for every data security incident that involves PHI. Rather than determine the risk of harm, the risk assessment determines the probability that PHI has been compromised. While 44 percent of organizations say it has affected their programs, 41 percent say it has not and 15 percent say it is too early to tell. The biggest change has been to require policies and procedures to be updated.

Most healthcare organizations are not in compliance with AOD requirements. Less than half of the organizations in this study report they are in full compliance (25 percent) or nearly in full compliance (23 percent) with the Accounting of Disclosures (AOD) requirement. These organizations say they achieve compliance mostly by an ad-hoc process (31 percent), a paper-based process or tool that was developed internally (27 percent), a software-based process or tool that was developed internally (27 percent) or a software-based process or tool that was developed by a third party (15 percent).

Part 2. Key findings

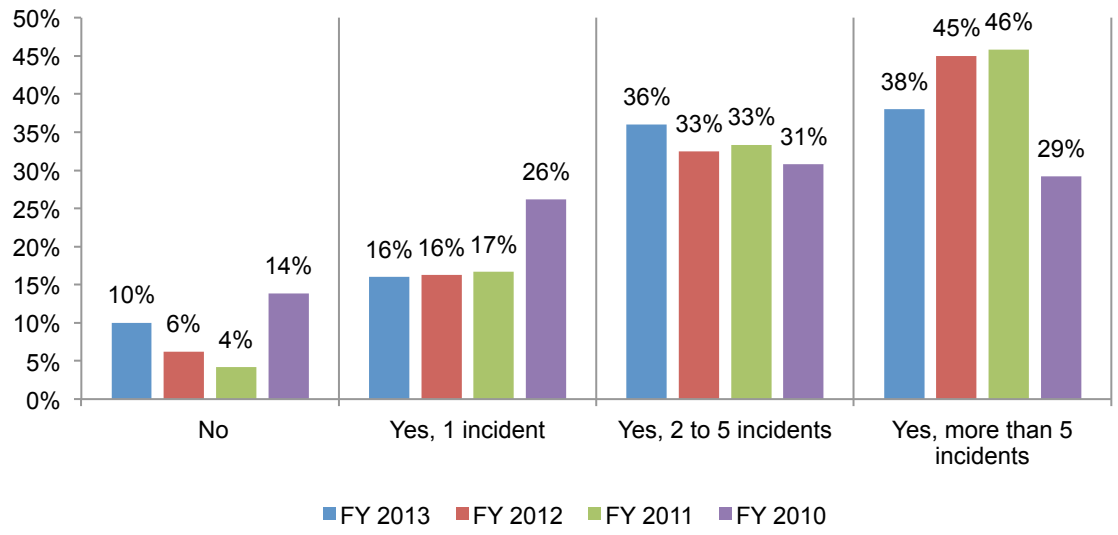
In this section, we provide a more detailed analysis of the research findings. Whenever possible, we show trends in the findings since the study was first conducted in 2010. The complete audited results are presented in the appendix of this report. The findings are organized according to the following issues:

- Data breaches decline but are still pervasive
- ACA puts patient data at risk
- Insider-outsider threats to sensitive data are on the rise
- Healthcare organizations struggle to comply with the HIPAA Final Rule

Data breaches decline but are still pervasive

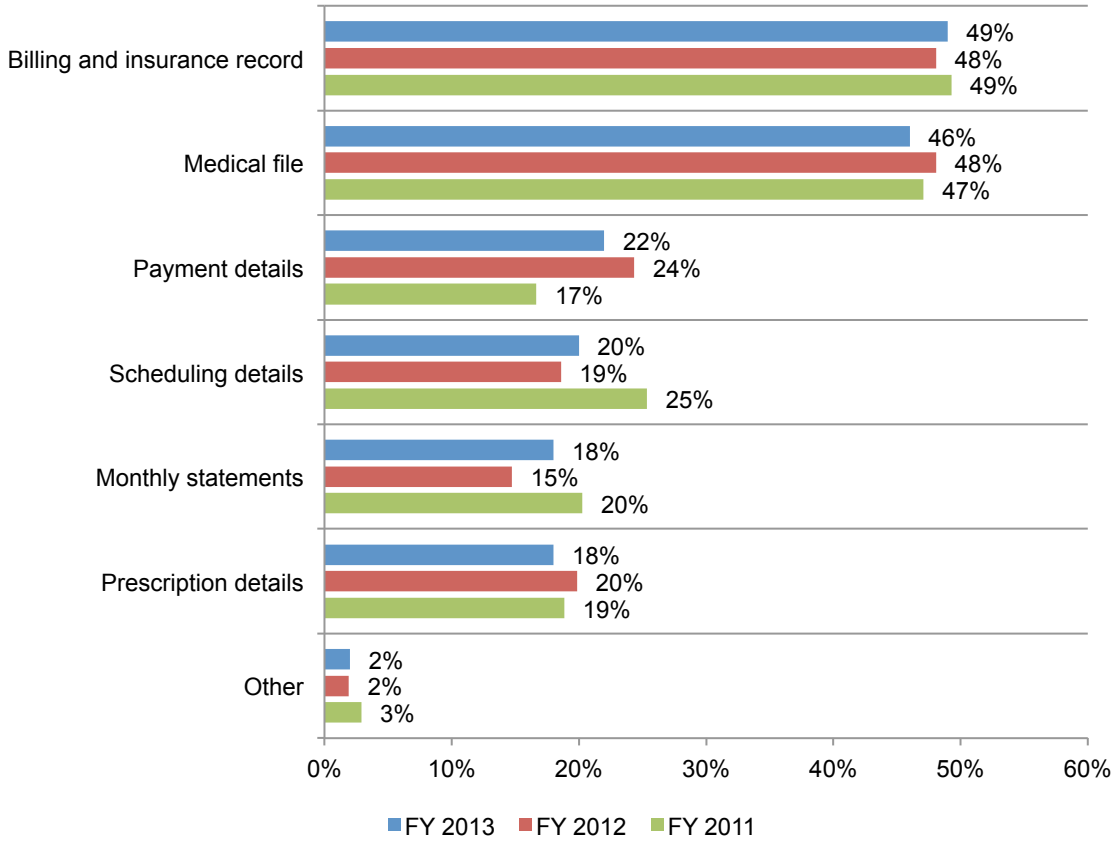
The number of data breaches decrease slightly. Ninety percent of healthcare organizations in this study have had at least one data breach in the past two years. As shown in Figure 1, 38 percent report they have had more than five incidents. This is a decline from last year's report when 45 percent of organizations had more than 5 but greater than what was first reported in 2010. This coupled with an increase in organizations' level of confidence in data breach detections suggests that modest improvements have been made in reducing threats to patient data.

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



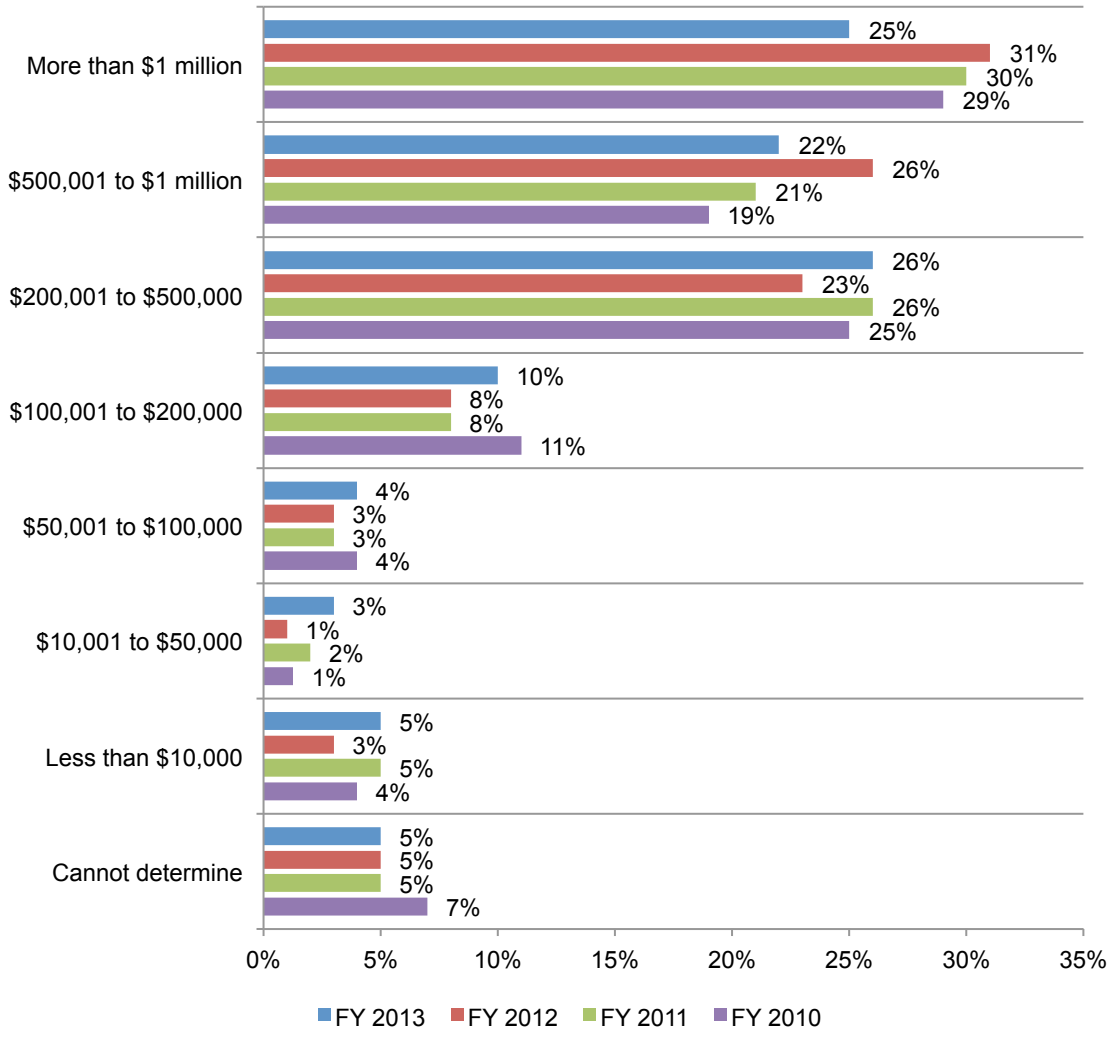
Consistent with the previous three annual studies, the data breaches are most likely to involve healthcare records with the most sensitive and valuable information for identity thieves. According to Figure 2, billing and insurance records and medical files are the most likely to be lost or stolen.

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



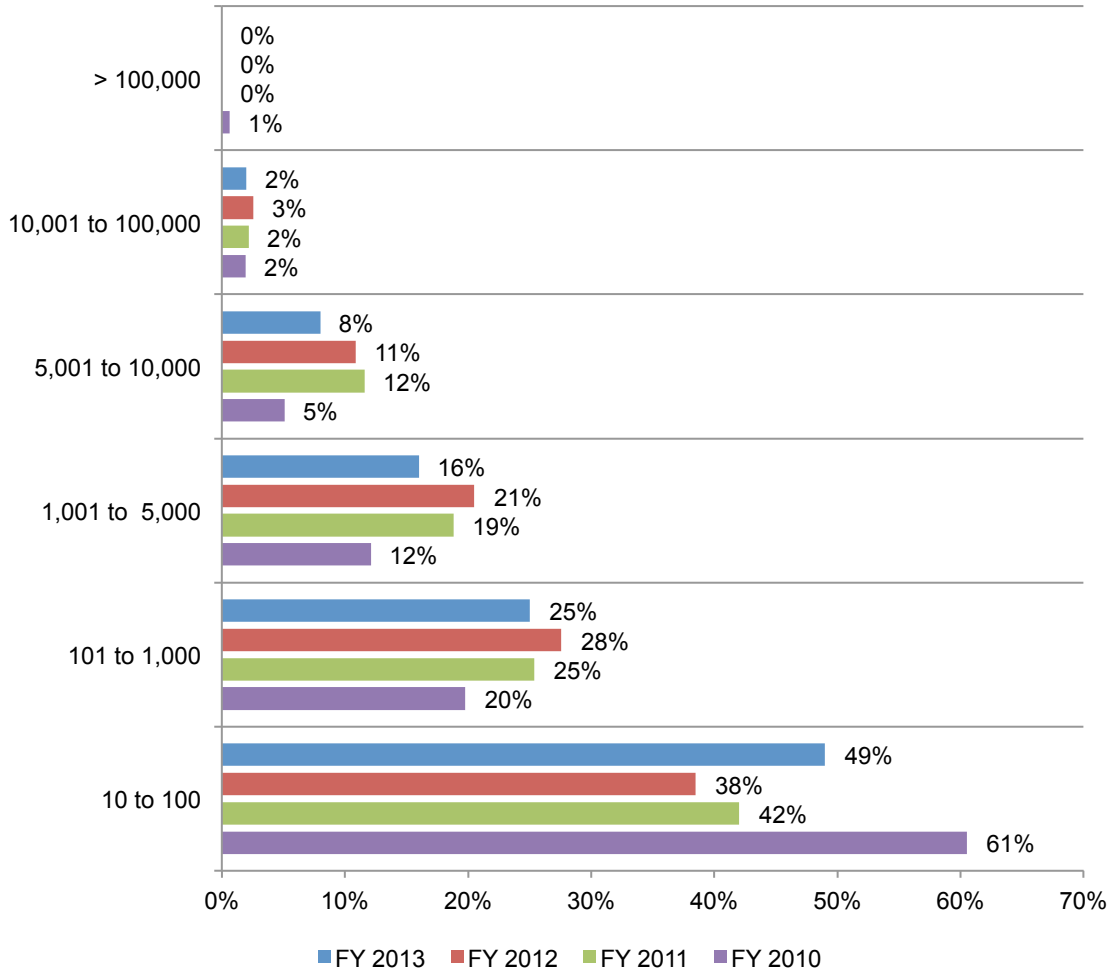
Healthcare organizations improve ability to control data breach costs. The economic impact of one or more data breaches for healthcare organizations in this study ranges from less than $10,000 to more than $1 million over a two-year period. Based on the ranges reported by respondents, we calculated that the average economic impact of data breaches over the past two years for the healthcare organizations represented in this study is $1,973,895, as shown in Figure 3. This is a decrease of 17 percent or almost $400,000 since last year.

Figure 3. Economic impact of data breach incidents experienced over the past two years
Average economic impact of data breach over the past two years is $1,973,895



Contributing to the cost reduction is the fact that the size of the breaches decreased. According to Figure 4, the average number of lost or stolen records per breach was 2,150. Last year the average number was almost 3,000 records. Based on other research conducted by Ponemon Institute, the average cost per one lost or stolen record is $188. This suggests that it could take only one data breach to have an economic impact of $404,200.[3]

Figure 4. Number of compromised records
Extrapolated average is 2,150

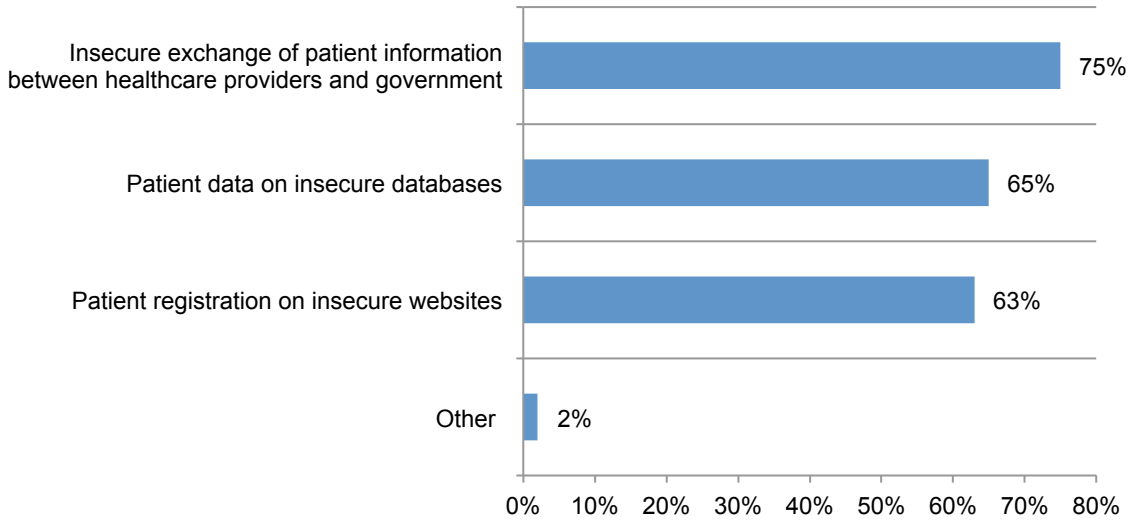


[3] See *2013 Cost of Data Breach*, conducted by Ponemon Institute, May 2013

ACA puts patient data at risk

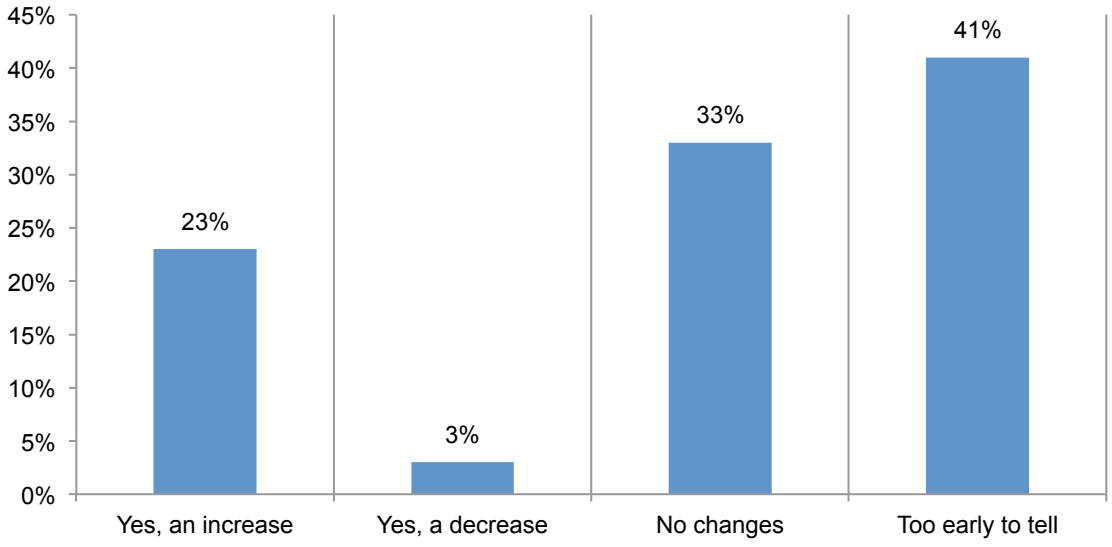
ACA increases risk to patient privacy and information security. Respondents in 69 percent of organizations represented believe the ACA significantly increases or increases the risk to patient privacy and security. As shown in Figure 5, the primary concerns are insecure exchange of patient information between healthcare providers and government (75 percent of organizations), patient data on insecure databases (65 percent) and patient registration on insecure websites (63 percent of organizations).

Figure 5. Primary concerns regarding the risks to patient information
More than one choice permitted



ACO participation increases data breach risks. Fifty-one percent of organizations say they are part of an Accountable Care Organization (ACO) and 66 percent say the risks to patient privacy and security due to the exchange of patient health information among participants has increased. According to Figure 6, when asked if their organization experienced changes in the number of unauthorized disclosure of PHI, 41 percent say it is too early to tell. Twenty-three percent say they noticed an increase as shown in Figure 6.

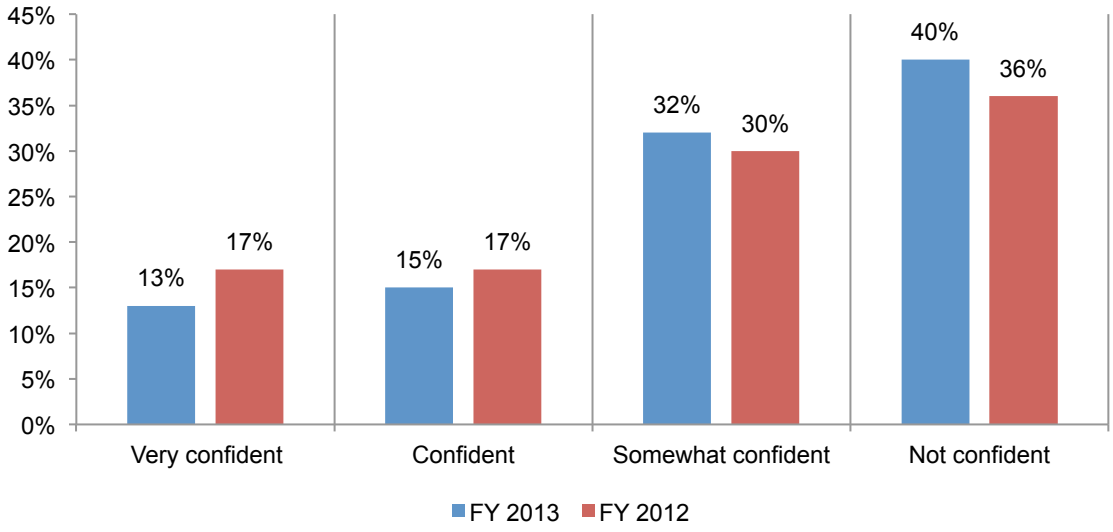
Figure 6. Changes in the number of unauthorized disclosures of PHI



Confidence in the security of Health Information Exchanges (HIEs) remains low. An HIE is defined as the mobilization of healthcare information electronically across organizations within a region, community or hospital system. The percentage of organizations joining HIEs increases only slightly. This year, 32 percent say they are members and this is up slightly from 28 percent last year. One-third of organizations say they do not plan to become a member.

Figure 7 shows that the primary reason could be that 72 percent of respondents say they are only somewhat confident (32 percent) or not confident (40 percent) in the security and privacy of patient data share on HIEs.

Figure 7. Confidence in the security and privacy of patient data shared on HIEs

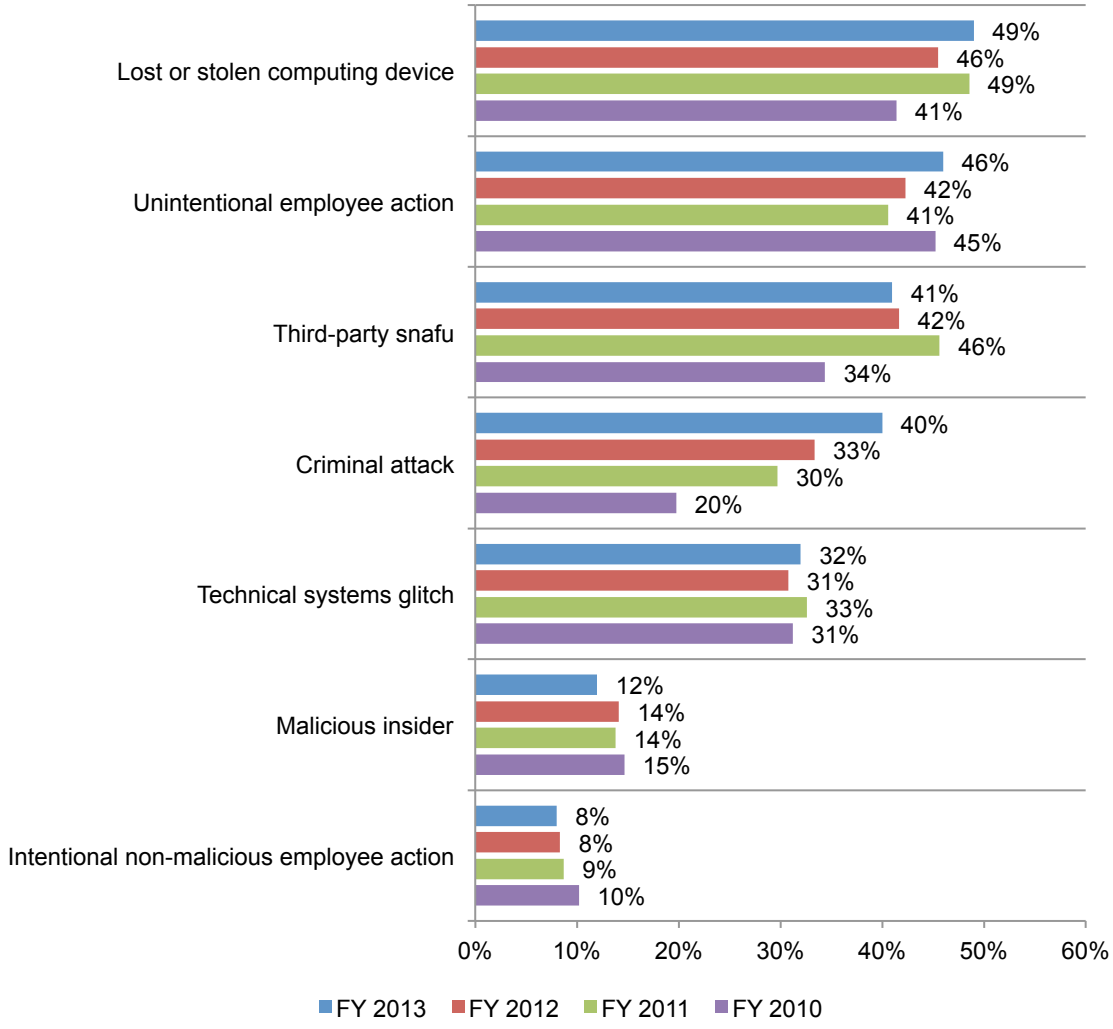


Insider-outsider threats to sensitive data are on the rise

Criminal attacks on healthcare organizations increase 100 percent since 2010. Insider negligence continues to be at the root of most data breaches reported in this study but a major challenge for healthcare organizations is addressing the criminal threat as shown in Figure 8. These types of attacks on sensitive data have increased 100 percent since the study was conducted in 2010 from 20 percent of organizations reporting criminal attacks to 40 percent of organizations in this year's study.

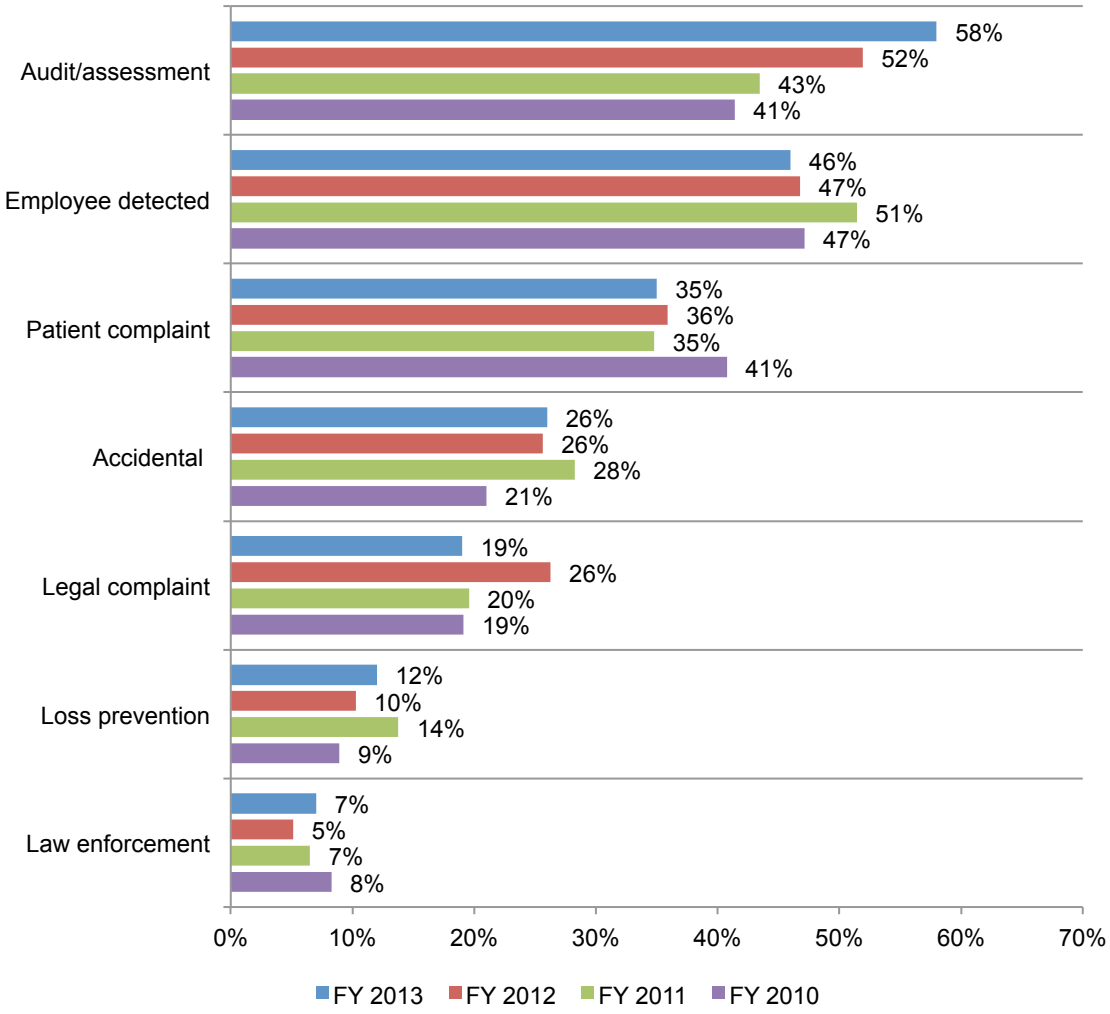
Consistent with previous studies, the primary cause of breaches is a lost or stolen computing device (49 percent), which can be attributed in many cases to employee carelessness. This is followed by employee mistakes or unintentional actions (46 percent), and third-party snafus (41 percent).

Figure 8. Nature of the incident
More than one choice permitted



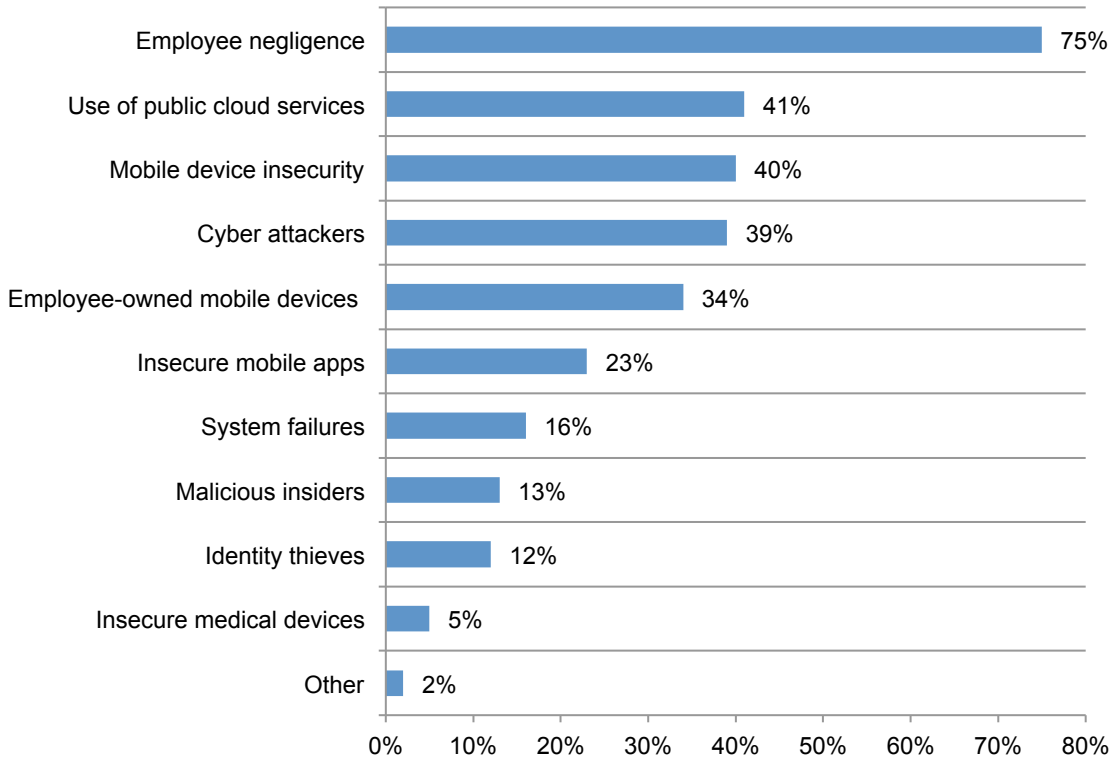
It is interesting that audit and assessment as the reason for discovering a data breach has increased significantly from 41 percent of respondents in 2010 to 58 percent of respondents this year while patient complaints declined since 2010. Finding out about the data breach from a legal complaint also declined, as shown in Figure 9.

Figure 9. How the data breach was discovered
More than one choice permitted



Employee negligence is considered the biggest security risk. Figure 10 reveals that 75 percent of organizations say employee negligence is their biggest worry followed by use of public cloud services (41 percent), mobile device insecurity (40 percent) and cyber attackers (39 percent).

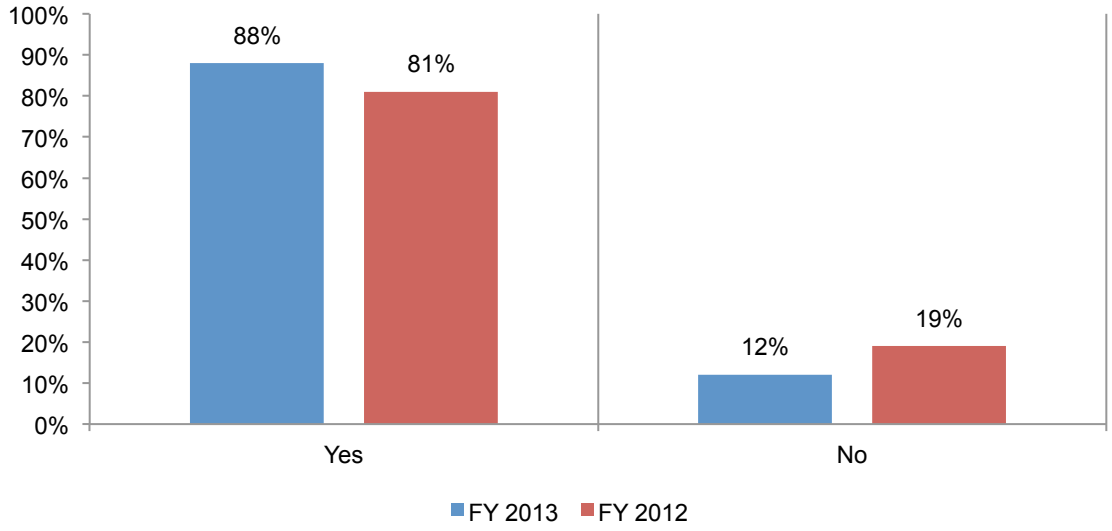
Figure 10. Security threats of most concern
Three choices permitted



BYOD usage continues to rise. As shown in Figure 11, despite the concerns about employee negligence and the use of insecure mobile device, 88 percent of organizations permit employees and medical staff to use their own mobile devices such as smart phones or tablets to connect to their organization's networks or enterprise systems such as email. More than half of organizations are not confident that the personally-owned mobile devices or BYOD are secure.

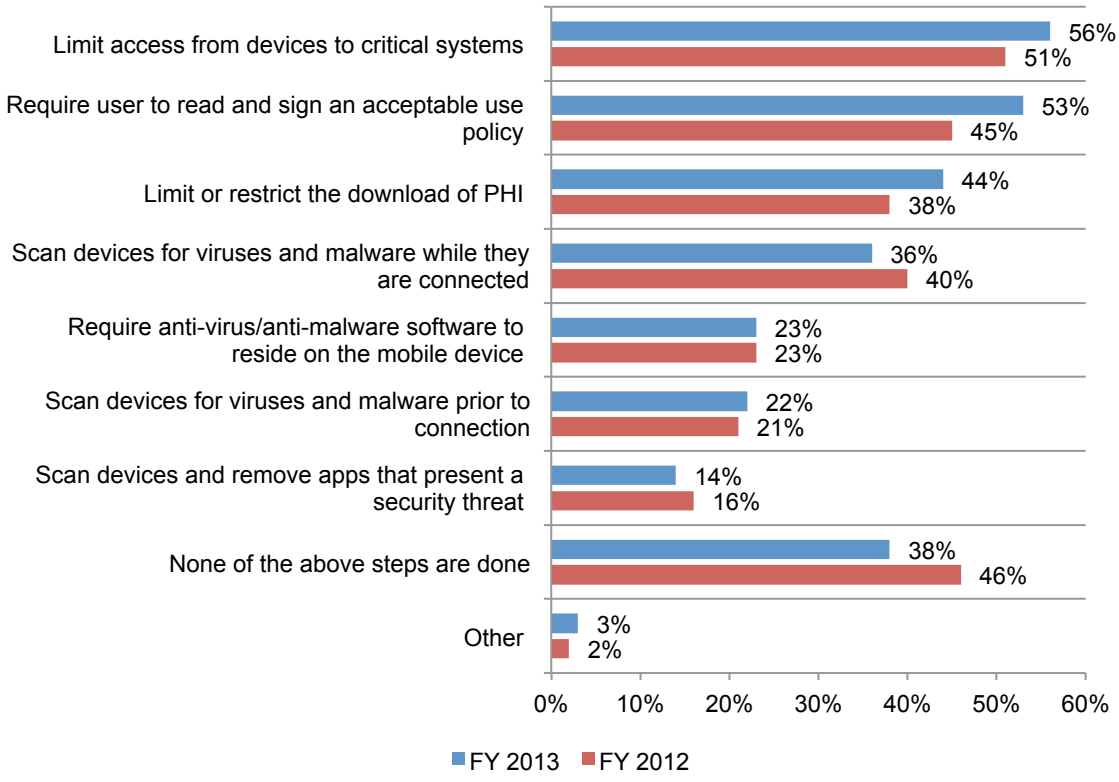
Very few organizations require their employees to take such security precautions as requiring anti-virus/anti-malware software to reside on the mobile device prior to connection (23 percent), scanning devices for viruses and malware prior to connection (22 percent) and scanning devices and removing all mobile apps that present a security threat prior to connection (14 percent).

Figure 11. Employees permitted to use personal mobile devices to connect to networks



Since last year, more organizations are taking steps to secure devices. These steps to protect their organization's network or enterprise systems from the insecurity of BYOD include 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 limiting or restricting the download of PHI onto these devices, according to Figure 12.

Figure 12. Measures to ensure devices are secure enough to connect to the network
More than one response permitted

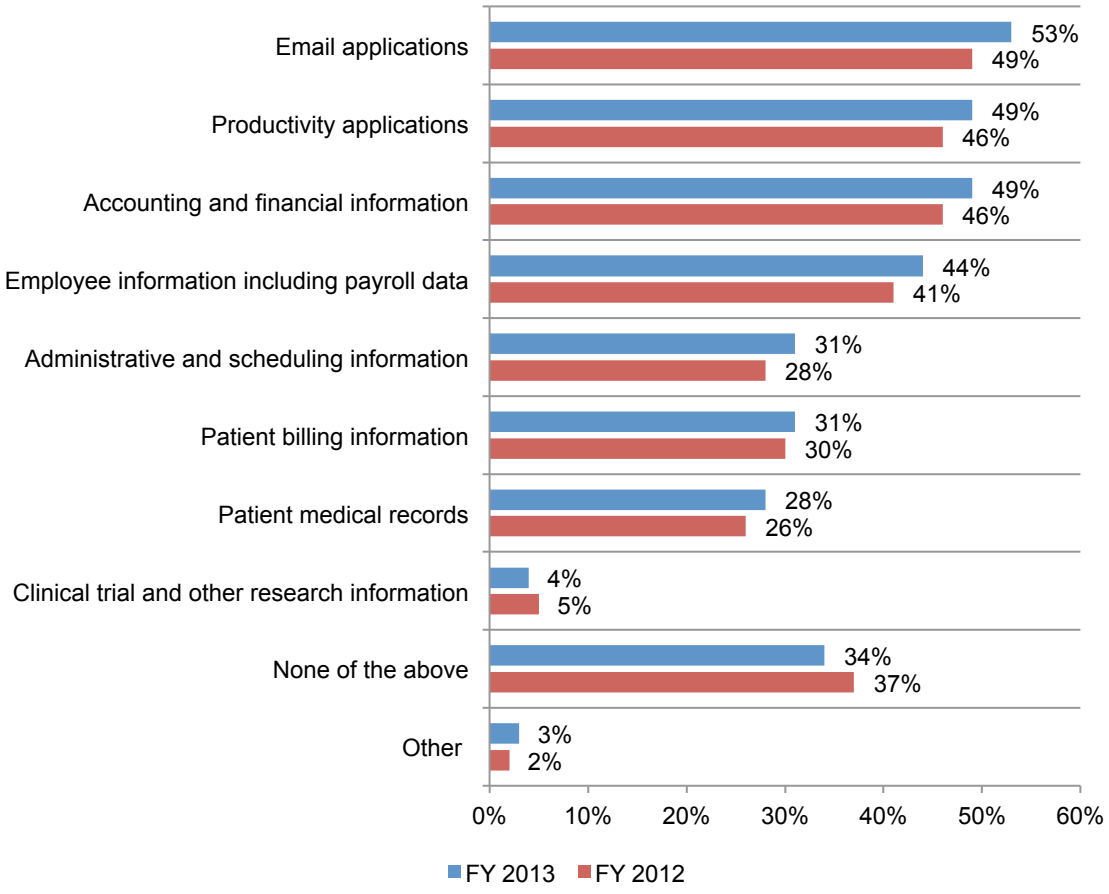


.

Heavy use of cloud services increases. As discussed above, healthcare organizations view the use of public cloud services as a serious threat. In fact, only one-third are very confident or confident that information in a public cloud environment is secure. Despite the risk, 40 percent of organizations say they use the cloud heavily, an increase from 32 percent last year. The applications or services most used are backup and storage, file-sharing applications, business applications and document sharing and collaboration.

According to Figure 13, 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. This is pretty much consistent with previous years. Also processed or stored in the cloud but not as often are patient medical records and billing information. The majority of organizations believe patient medical records and billing information is too sensitive to be processes and/or stored in a public cloud environment.

Figure 13. Types of information processed and/or stored in the cloud
More than one choice permitted

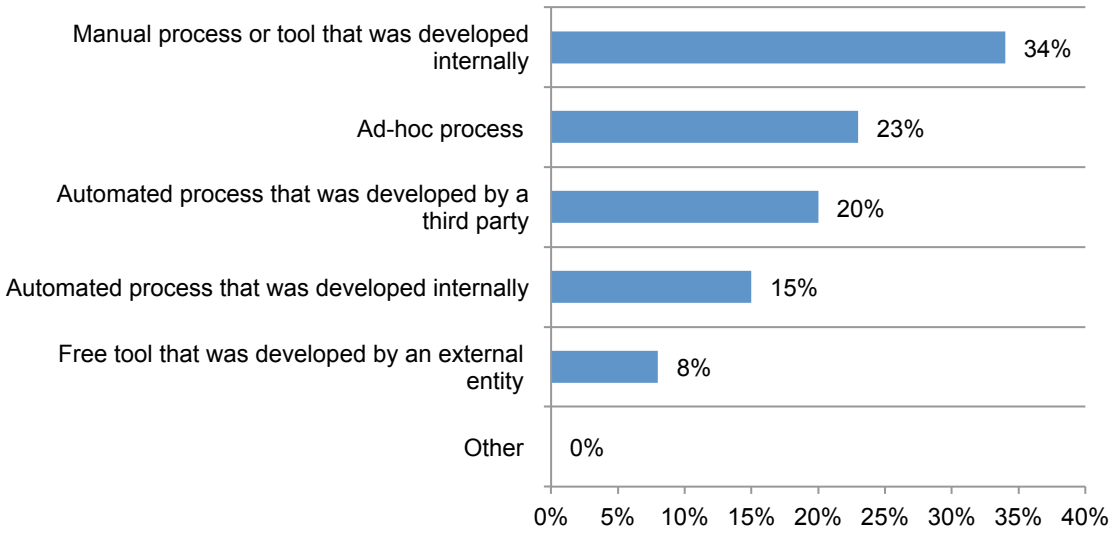


Healthcare organizations struggle to comply with the HIPAA Final Rule

Half of healthcare organizations are compliant with the post-incident risk assessment requirement in the Final Rule. Fifty-one percent of respondents said they are in full compliance while 49 percent report they are not compliant or are only partially compliant. Thirty-nine percent say their incident assessment process is not effective and cite a lack of consistency and inability to scale their process as the primary reasons.

As shown in Figure 14, the process most often used to conduct and document post incident risk assessment is a manual process that was developed internally (34 percent) followed by an ad-hoc process (23 percent). Only 15 percent use an automated tool or process developed internally or one that was developed by a third party (20 percent).

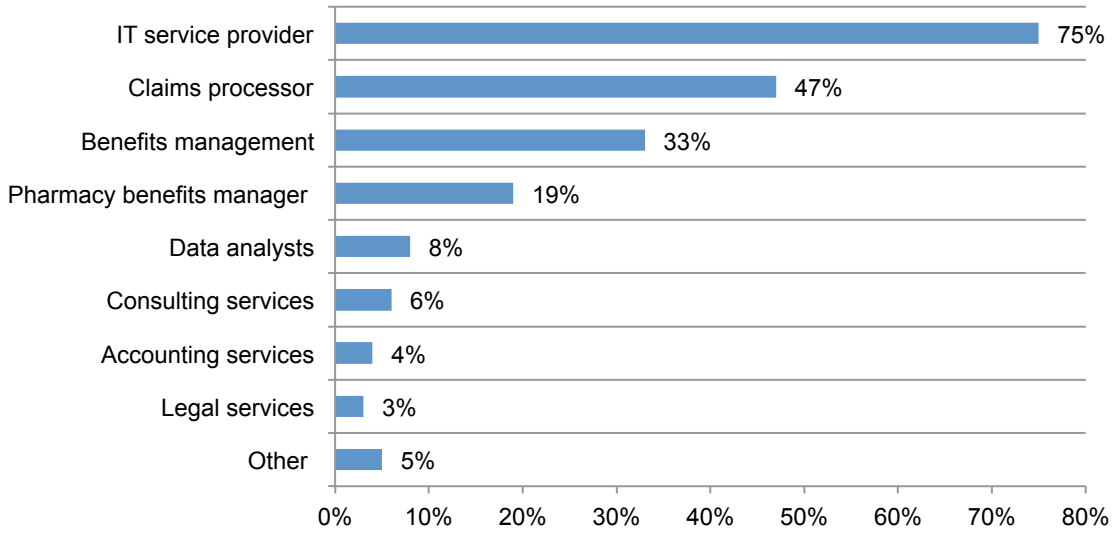
Figure 14. Post incident risk assessment process



Healthcare organizations don't trust their third parties or business associates[4] with sensitive patient information. Seventy-three percent of organizations are either somewhat confident (33 percent) or not confident (40 percent) that their business associates would be able to detect, perform an incident risk assessment and notify your organization in the event of a data breach incident as required under the business associate agreement.

The business associates they worry most about are IT service providers, claims processors and benefits management, as shown in Figure 15. Only 30 percent are very confident or confident that their business associates are appropriately safeguarding patient data as required under the Final Rule.

Figure 15. Business associates that present the greatest risk to privacy and security
Two choices permitted

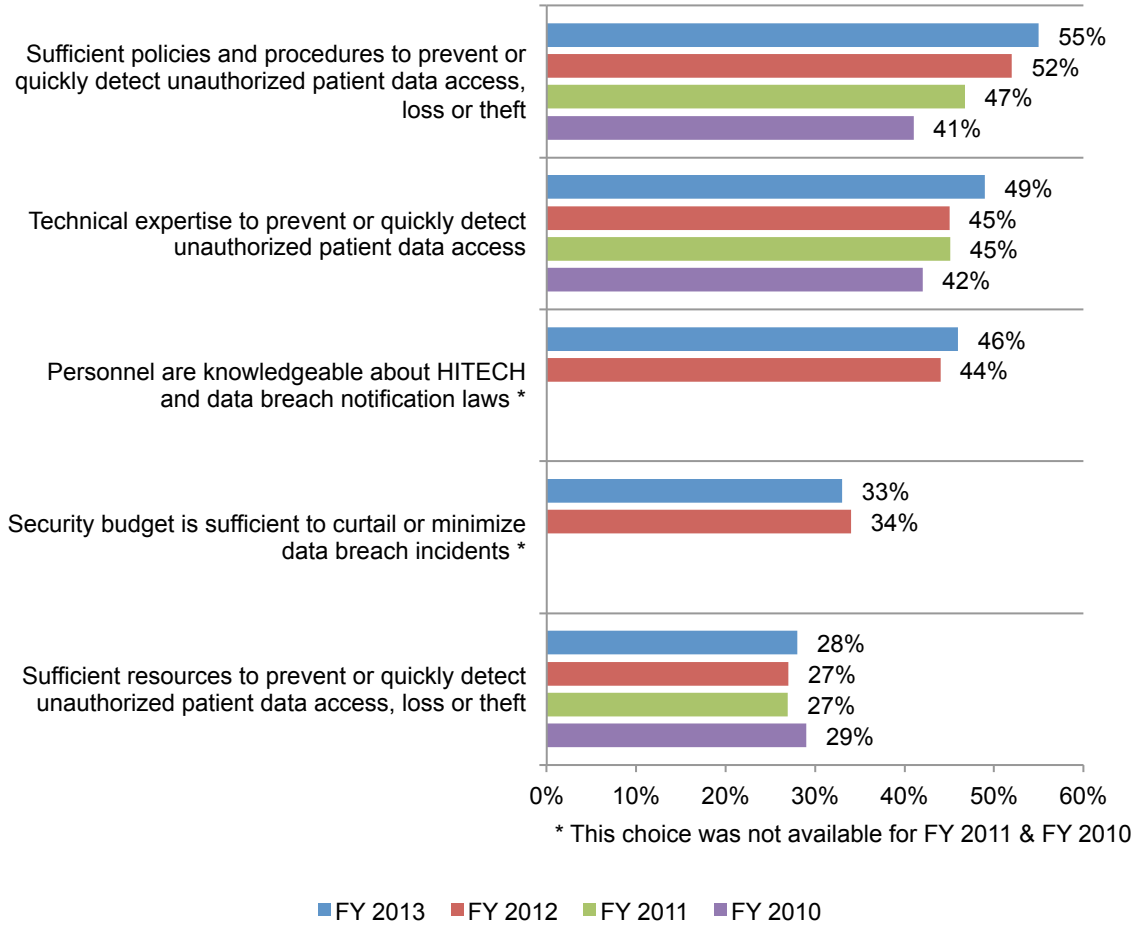


[4] A business associate conducts activities on behalf of healthcare organizations that involve the use or disclosure of individually identifiable health information. Such activities can include claims processing or administration, data analysis, billing and other services. According to the HIPAA Final Omnibus Rule, new rules expand the obligations of physicians and other healthcare providers to protect patients' protected health information (PHI), extend these obligations to other individuals and companies who, as business associates, have access to PHI, and increase the penalties for violations of any of these obligations.

Organizations rely on policies and procedures to achieve compliance and secure sensitive information. According to Figure 16, fifty-five percent of organizations agree they have the policies and procedures that effectively prevent or quickly detect unauthorized patient data access, loss or theft. This has increased significantly since 2010 when 41 percent said this was the case. Technical expertise has increased as well since 2010 (from 42 percent of respondents to 49 percent).

Unfortunately, the budget, technologies and resources needed to safeguard patient information from a data breach are not as available. Further, less than half (46 percent) of organizations have personnel who are knowledgeable about HITECH and states' data breach notification laws.

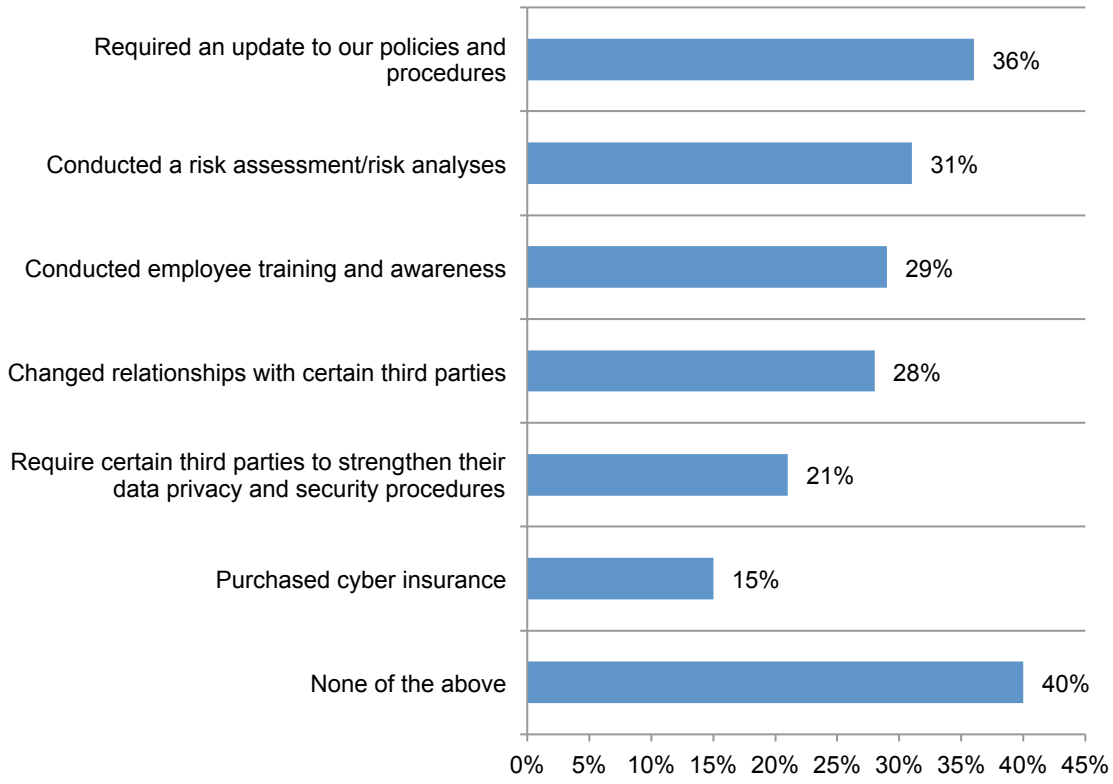
Figure 16. Attributions about patient data security
Strongly agree and agree response combined



Majority of organizations say the HIPAA Final Rule has either not affected patient data privacy and security programs or it's too early to tell. The HIPAA Final Omnibus Rule seeks to better protect patients by removing the harm threshold. Covered entities and their business associates must still conduct an incident risk assessment, for every data security incident that involves PHI. Rather than determine the risk of harm, the risk assessment determines the probability that PHI has been compromised. While 44 percent of organizations say it has affected their programs, 41 percent say it has not and 15 percent say it is too early to tell.

According to Figure 17, the biggest change has been to require policies and procedures to be updated followed by conducted a risk assessment or analyses.

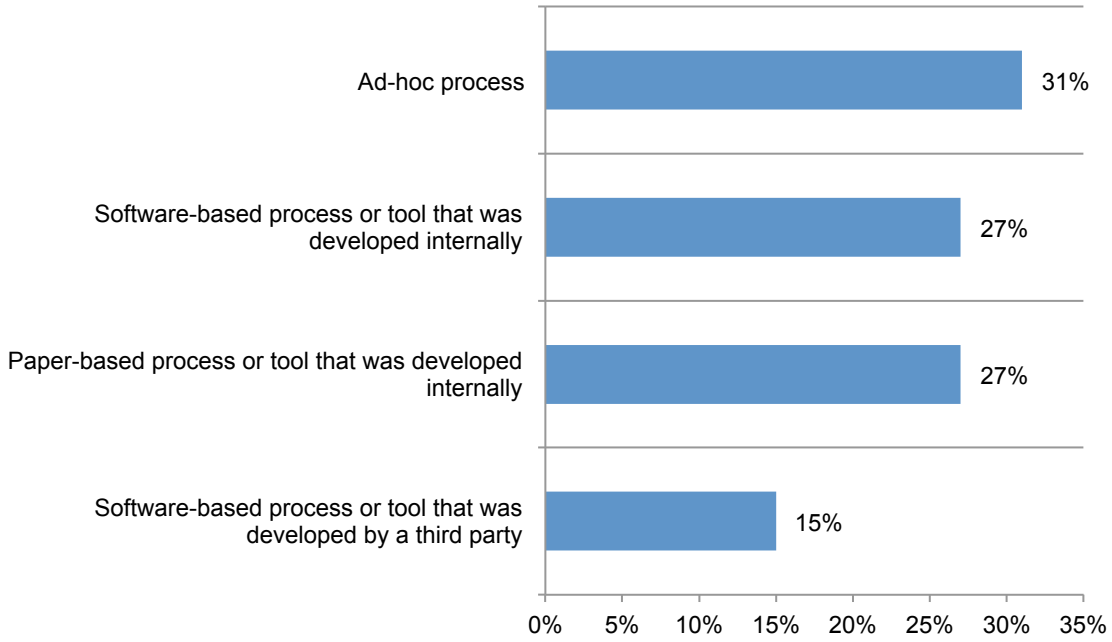
Figure 17. How the Final Rule changed patient data privacy and security programs
More than one choice permitted



Most healthcare organizations are not in compliance with AOD requirements. Less than half of the organizations in this study report they are in full compliance (25 percent) or nearly in full compliance (23 percent) with the Accounting of Disclosures (AOD) requirement.

Figure 18 reveals that these organizations say they achieve compliance mostly by an ad-hoc process (31 percent), a paper-based process or tool that was developed internally (27 percent), a software-based process or tool that was developed internally (27 percent) or a software-based process or tool that was developed by a third party (15 percent).

Figure 18. How is compliance with the Accounting of Disclosures achieved?



Part 3. Conclusion

The more things change the more they stay the same. Four years of conducting this research reveals that healthcare organizations continue to have data breaches due to the human factor. These include employees' carelessness with their computing devices and other unintended but negligent acts that put patient data in jeopardy. For the first time, we asked what is the greatest risk to the security and privacy of patient information. The vast majority (75 percent) of organizations say it is employee negligence.

A major change in the delivery of healthcare services is also having an impact on the risks to patient information. The ACA has healthcare organizations worried about insecure websites, databases and health information exchanges that are highly vulnerable to insider and outsider threats.

Healthcare security professionals need to address both internal and external threats. The research reveals that many organizations are relying on policies and procedures to achieve compliance and secure sensitive information. In addition to policies, organizations should be focused on technologies that secure mobile devices and protect sensitive data that is stored in the cloud. Training and awareness programs should be conducted at every level of the organization to reduce the negligent employee risk. Finally, the growth in criminal attacks against healthcare organizations calls for assessments of areas vulnerable to attack and investment in technologies that protect organizations from malicious outsiders. Implementing these measures is a huge challenge but critical to the future of the industry.

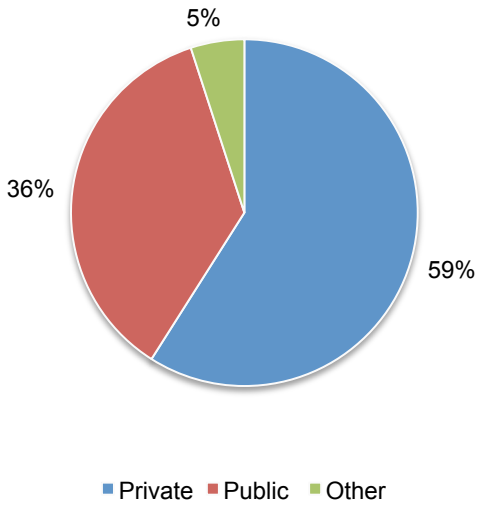
Part 4. Benchmark Methods

Table 1 summarizes the responses completed over a three-month period concluding in January 2014. A total of 505 health care organizations were selected for participation and contacted by the researcher. One hundred and eleven organizations agreed to complete the benchmark survey; however, 93 completed the benchmark instrument. Two benchmarked organizations were deemed incomplete and, hence, removed from the sample. A final sample of 91 organizations was used in our analysis, which is a net increase of 11 organizations from our 2012 study.

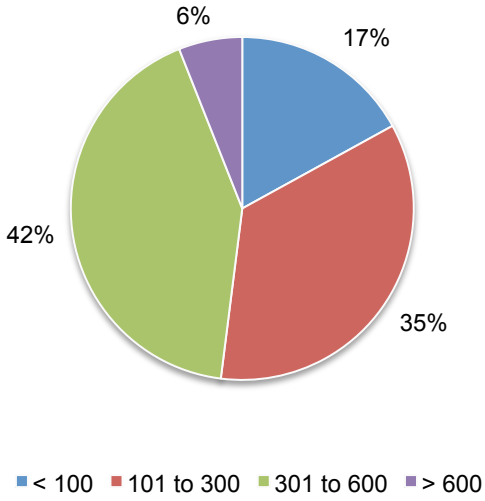
Table 1. Benchmark sampling response	FY 2013	FY 2012	FY 2011	FY 2010
Total healthcare organizations contacts made	505	499	511	457
Total healthcare organizations recruited	111	92	98	99
Total healthcare organizations participating	93	81	75	67
Total healthcare organizations providing incomplete responses	2	1	3	2
Final benchmark sample	91	80	72	65

Pie Chart 1 reports the type of healthcare providers that participated in this research, with 59 percent representing private organizations. Pie Chart 2 shows the size of organizations with respect to the number of patient beds. Forty-two percent of participating healthcare providers have a 301 to 600-bed capacity, while 35 percent have 101 to 300 beds.

Pie Chart 1. Type of health care provider

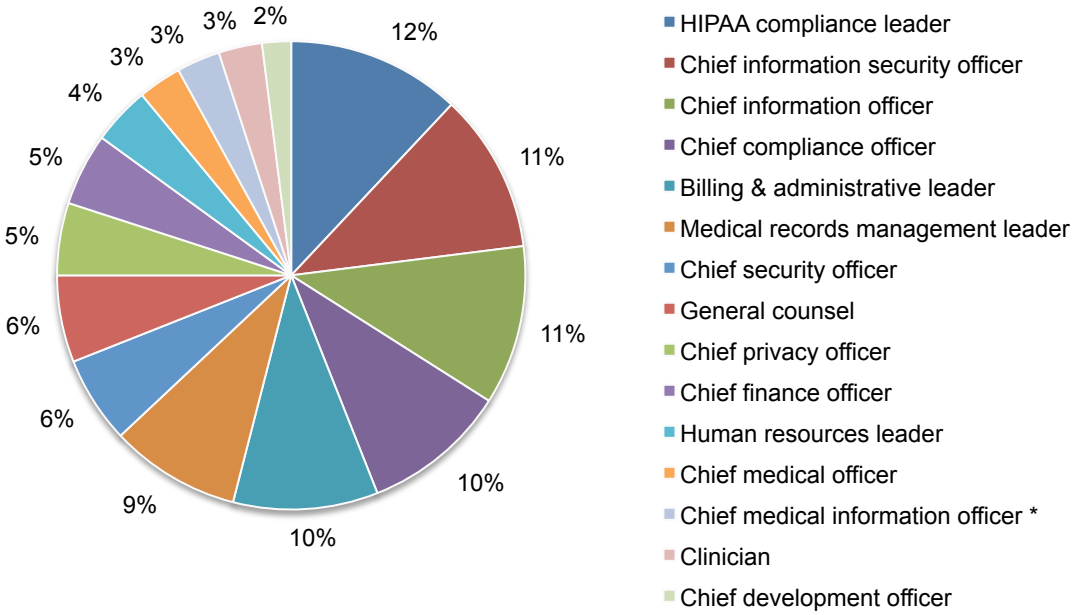


Pie Chart 2. The number of patient beds (size)



According to Pie Chart 3, the primary roles of respondents or their supervisors interviewed in this study are HIPAA compliance leader (12%), chief information security officer (11 percent), chief information officer (11 percent), chief compliance officer (10 percent) and billing & administrative leader (10 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 5. Limitations

The presented findings are based on self-reported benchmark survey returns. Usable returns from 91 organizations – or about 18 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 2013 results to benchmark studies completed in 2012, 2011 and 2010. While these four 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 91 participating companies. All field research was completed over a three-month period concluding in January 2014

Benchmark sampling response	FY 2013	FY 2012	FY 2011	FY 2010
Total healthcare organizations contacts made	505	499	511	457
Total healthcare organizations recruited	111	92	98	99
Total healthcare organizations participating	93	81	75	67
Total healthcare organizations providing incomplete responses	2	1	3	2
Final benchmark sample	91	80	72	65

Screening Question				
S1. Is your organization a healthcare provider subject to HIPAA as a coverend entity	FY 2013	FY 2012	FY 2011	FY 2010
Yes	91			
No	0			

Part 1: Organizational characteristics				
Q1a. What best describes your organization:	FY 2013	FY 2012	FY 2011	FY 2010
Public healthcare provider	36%	35%	32%	35%
Private healthcare provider	59%	58%	57%	54%
Other	5%	8%	11%	11%
Total	100%	100%	100%	100%

Q1b. How many patient beds (capacity) does your organization have?	FY 2013	FY 2012	FY 2011	FY 2010
Less than 100	17%	16%	17%	18%
101 to 300	35%	36%	35%	32%
301 to 600	42%	40%	42%	45%
More than 600	6%	8%	7%	5%
Total	100%	100%	100%	100%

Q1c. What best describes your organization's operating structure?	FY 2013	FY 2012	FY 2011	FY 2010
Integrated Delivery System	34%	36%	36%	35%
Hospital or clinic that is part of a healthcare network	49%	46%	47%	46%
Standalone hospital	13%	14%	17%	17%
Standalone Clinic	4%	4%		
Other	0%	0%	0%	2%
Total	100%	100%	100%	100%

Q1d. Please indicate the region of the United States where you are located.	FY 2013	FY 2012	FY 2011	FY 2010
Northeast	20%	21%	22%	23%
Mid-Atlantic	20%	20%	21%	20%
Midwest	15%	16%	15%	15%
Southeast	12%	11%	13%	12%
Southwest	14%	13%	13%	14%
Pacific-West	19%	19%	17%	15%
Total	100%	100%	100%	100%

Q1e. What best describes your role or the role of your supervisor?	FY 2013	FY 2012	FY 2011	FY 2010
Chief security officer	6%	5%	5%	7%
Chief information security officer	11%	9%	10%	9%
Chief information officer	11%	12%	11%	6%
Chief privacy officer	5%	5%	6%	4%
Chief compliance officer	10%	11%	11%	11%
Chief medical officer	3%	2%	3%	1%
Chief clinical officer	0%	1%	1%	0%
Chief risk officer (2012)	0%	2%		
Chief medical information officer (2012)	3%	2%		
Chief finance officer	5%	4%	4%	6%
Chief development officer	2%	1%	2%	2%
General counsel	6%	6%	5%	6%
HIPAA compliance leader	12%	11%	11%	12%
Clinician	3%	4%	3%	1%
Billing & administrative leader	10%	10%	12%	15%
Medical records management leader	9%	8%	11%	13%
Human resources leader	4%	5%	5%	5%
Other	0%	2%	1%	1%
Total	100%	100%	100%	100%
Total number of individual interviews	388	324	300	211
Average number of interviews per HC organization	4.26	4.05	4.17	3.25

Q1f. What best describes your department or function?	FY 2013	FY 2012	FY 2011	FY 2010
Compliance	100%	94%	100%	91%
Privacy	42%	34%	39%	48%
Information technology (IT)	81%	79%	76%	45%
Legal	23%	21%	21%	20%
Finance	19%	16%	15%	20%
Marketing	4%	6%	8%	6%
Medical informatics	26%	24%	24%	17%
Medical staff	21%	19%	18%	15%
Patient services	52%	48%	47%	38%
Records management	20%	23%	14%	9%
Risk management	9%	6%	15%	9%
Development (foundation)	4%	6%	11%	8%
Planning	6%	10%	4%	6%
Human resources	13%	14%	19%	20%
Other	6%	6%	4%	0%
Total	426%	405%	417%	352%

			Strongly agree and Agree response combined	
Part 2. Attributions. Please rate your opinion about the statements contained in Q2 to Q7 using the scale provided below each item.	FY 2013	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.	55%	52%	47%	41%
Q3. My organization has sufficient technologies that effectively prevent or quickly detect unauthorized patient data access, loss or theft.	44%	40%	38%	37%
Q4. My organization has sufficient resources to prevent or quickly detect unauthorized patient data access, loss or theft.	28%	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.	49%	45%	45%	42%
Q6. Our organization's security budget is sufficient to curtail or minimize data breach incidents.	33%	34%		
Q7. My organization has personnel who are knowledgeable about HITECH and states' data breach notification laws.	46%	44%		

Part 3: Data Breach				
Q8. Has your department suffered a data breach involving the loss or theft of patient data in the past two years as defined above?	2013 Pct%	2012 Pct%	2011 Pct%	2010 Pct%
No	10%	6%	4%	14%
Yes, 1 incident	16%	16%	17%	26%
Yes, 2 to 5 incidents	36%	33%	33%	31%
Yes, more than 5 incidents	38%	45%	46%	29%
Total	100%	100%	100%	100%
Extrapolated average number of data breaches for the sample	3.70	4.00	4.08	3.09
Extrapolated total number of data breaches for the sample	337	320	294	201

Q9. How confident are you that your organization has the ability to detect all patient data loss or theft?	2013 Pct%	2012 Pct%	2011 Pct%	2010 Pct%
Very confident	15%	13%	12%	11%
Confident	38%	33%	31%	31%
Little confidence	29%	31%	33%	35%
No confidence	18%	23%	24%	23%
Total	100%	100%	100%	100%

Q10. Two separate data breach incidents over the past two years.	FY 2013	FY 2012	FY 2011	FY 2010
Number of incidents reported	337	320	294	201
Number of observed incidents used in the analysis of Q10	169	156	138	157

Q10a. Approximate number of compromised records	FY 2013	FY 2012	FY 2011	FY 2010
< 10	0%			
10 to 100	49%	38%	42%	61%
101 to 1,000	25%	28%	25%	20%
1,001 to 5,000	16%	21%	19%	12%
5,001 to 10,000	8%	11%	12%	5%
10,001 to 100,000	2%	3%	2%	2%
> 100,000	0%	0%	0%	1%
Total	100%	100%	100%	100%
Extroplated average number of lost or stolen records over two years	2,150	2,769	2,575	1,769

Q10b. Nature of the incident	FY 2013	FY 2012	FY 2011	FY 2010
Unintentional employee action	46%	42%	41%	45%
Intentional non-malicious employee action	8%	8%	9%	10%
Technical systems glitch	32%	31%	33%	31%
Criminal attack	40%	33%	30%	20%
Malicious insider	12%	14%	14%	15%
Third-party snafu	41%	42%	46%	34%
Lost or stolen computing device	49%	46%	49%	41%
Total	228%	216%	220%	197%
*More than one selection is permitted				

Q10c. Type of device compromised or stolen	FY 2013	FY 2012	FY 2011	FY 2010
Desktop or laptop	30%	38%	43%	
Smartphone	28%	24%	21%	
Tablet	27%	18%	7%	
Notebook	1%	2%	4%	
Server	3%	5%	7%	
USB drive	11%	13%	16%	
Total	100%	100%	100%	

Q10d. Type of patient data lost or stolen	FY 2013	FY 2012	FY 2011	FY 2010
Medical file	46%	48%	47%	
Billing and insurance record	49%	48%	49%	
Scheduling details	20%	19%	25%	
Prescription details	18%	20%	19%	
Payment details	22%	24%	17%	
Monthly statements	18%	15%	20%	
Other	2%	2%	3%	
Total	175%	176%	180%	
*More than one selection is permitted				

Q10e. How the data breach was discovered	FY 2013	FY 2012	FY 2011	FY 2010
Accidental	26%	26%	28%	21%
Loss prevention	12%	10%	14%	9%
Patient complaint	35%	36%	35%	41%
Law enforcement	7%	5%	7%	8%
Legal complaint	19%	26%	20%	19%
Employee detected	46%	47%	51%	47%
Audit/assessment	58%	52%	43%	41%
Total	203%	202%	198%	187%
*More than one selection is permitted				

Q10f. Offer of protection services	FY 2013	FY 2012	FY 2011	FY 2010
None offered	70%	65%	65%	
Credit monitoring	20%	22%	19%	
Other identity monitoring	6%	4%	6%	
Insurance	0%	1%	1%	
Identity restoration	4%	7%	9%	
Financial incentives (i.e., gift cards)	0%			
Other	0%	0%	0%	
Total	100%	100%	100%	
*More than one selection is permitted				

Q11. What best describes the process for preventing and detecting data breach incidents in your organization today? Please select only one.	FY 2013	FY 2012	FY 2011	FY 2010
An "ad hoc" process	19%	23%	27%	35%
Mostly a process that relies on policies and procedures	29%	28%	29%	23%
Mostly a process that relies on security technologies	20%	20%	21%	16%
A combination of manual proceduress and security technologies	29%	24%	19%	20%
None of the above	3%	5%	4%	6%
Total	100%	100%	100%	100%

Q12. How confident are you that your organization has the abiility to prevent or quickly detect patient data loss or theft?	FY 2013	FY 2012*	FY 2011*	FY 2010*
Very confident	13%	13%	12%	11%
Confident	32%	33%	31%	31%
Somewhat confident	34%	31%	33%	35%
Not confident	21%	23%	24%	23%
Total	100%	100%	100%	100%
*Question was worded differently in prior studies				

Q13. In your opinion (best guess), what best describes the lifetime economic value, on average, of one patient or customer to your organization?	FY 2013	FY 2012	FY 2011	FY 2010
Less than $10,000	11%	9%	10%	12%
$10,001 to $50,000	35%	32%	31%	29%
$50,001 to $100,000	21%	24%	23%	21%
$100,001 to $200,000	11%	12%	10%	13%
$200,001 to $500,000	6%	7%	4%	5%
$500,001 to $1 million	2%	3%	3%	3%
More than $1 million	2%	2%	3%	2%
Cannot determine	12%	11%	16%	15%
Total	100%	100%	100%	100%
Average lifetime value of one lost patient (customer)	$97,990	$111,810	$113,400	$107,580

Q14. 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 2013	FY 2012	FY 2011	FY 2010
Less than $10,000	5%	3%	5%	4%
$10,001 to $50,000	3%	1%	2%	1%
$50,001 to $100,000	4%	3%	3%	4%
$100,001 to $200,000	10%	8%	8%	11%
$200,001 to $500,000	26%	23%	26%	25%
$500,001 to $1 million	22%	26%	21%	19%
More than $1 million	25%	31%	30%	29%
Cannot determine	5%	5%	5%	7%
Total	100%	100%	100%	100%
Average economic impact of data breach over the past two years	$1,973,895	$2,390,270	$2,243,700	$2,060,174

Q15. In your opinion, what harms do patients actually suffer if their records are lost or stolen?	FY 2013	FY 2012	FY 2011	FY 2010
Increase risk of financial identity theft	60%	61%	59%	56%
Increase risk of medical identity theft	55%	59%	51%	45%
Increased risk that personal health facts will be disclosed	72%	70%	73%	61%
None	8%	9%	10%	8%
Total	195%	199%	193%	170%

Q16a. Does your organization consult with third parties to determine if a data exposure incident requires notification under applicable federal and state regulations?	FY 2013	FY 2012	FY 2011	FY 2010
Yes, we consult with outside legal counsel	53%			
Yes, we consult with our cyber insurance carrier	12%			
Yes, we consult with auditors	15%			
Yes, we consult with privacy & data protection experts	13%			
No we determine this through ourselves (internally)	36%			
Total	129%			

Q16b. If yes, how have these third parties changed the frequency of your organization's data breach notifications?	FY 2013	FY 2012	FY 2011	FY 2010
We now report more breaches	17%			
We now report fewer breaches	12%			
We report about the same number of breaches	71%			
Total	100%			

Q17. Does your organization perform the following activities (Please check all that apply)?	FY 2013	FY 2012	FY 2011	FY 2010
Annual or periodic privacy risk assessments	18%	16%		
Annual or periodic security risk assessments	51%	48%		
Incident response plan development and or test	31%	26%		
Updated policies and procedures in response to regulatory changes	46%	47%		
Annual or periodic HIPAA privacy and security awareness training of all staff	63%	56%		
Vetting and monitoring of third parties, including business associates	55%	49%		
Updating of agreements with business associates	53%	48%		
Total	317%	290%		

Q18. Is your EHR system in compliance with the HHS mandated requirements to protect patient privacy?	FY 2013	FY 2012	FY 2011	FY 2010
Yes, fully	28%	22%		
Partially	33%	29%		
No	14%	19%		
We don't use EHRs	25%	30%		
Total	100%	100%		

Q19. Is your organization a member of a Health Information Exchange (HIE)?	FY 2013	FY 2012	FY 2011	FY 2010
Yes	32%	28%		
We will become a member	20%	17%		
We are considering membership	15%	20%		
No, we do not plan to become a member of HIE	33%	35%		
Total	100%	100%		

Q20. What is your level of confidence as to the security and privacy of patient data shared on Health Information Exchanges?	FY 2013	FY 2012	FY 2011	FY 2010
Very confident	13%	17%		
Confident	15%	17%		
Somewhat confident	32%	30%		
Not confident	40%	36%		
Total	100%	100%		

Q21a. Has the HIPAA Final Omnibus Rule affected your organization's patient data privacy and security programs?	FY 2013	FY 2012	FY 2011	FY 2010
Yes	44%			
No	41%			
Too early to tell	15%			
Total	100%			

Q21b. If yes, how has the Final Rule changed your organization's patient data privacy and security programs? Please select all that apply.	FY 2013	FY 2012	FY 2011	FY 2010
Required an update to our policies and procedures	36%			
Require certain third parties to strengthen their data privacy and security procedures	21%			
Changed relationships with certain third parties	28%			
Conducted employee training and awareness	29%			
Conducted a risk assessment/risk analyses	31%			
Purchased cyber insurance	15%			
None of the above	40%			
Total	200%			

Q22. How confident are you that your organization's business associates are appropriately safeguarding patient data as required under the Final Rule?	FY 2013	FY 2012	FY 2011	FY 2010
Very confident	13%			
Confident	17%			
Somewhat confident	31%			
Not confident	39%			
Total	100%			

Q23. How confident are you that your organization's business associates would be able to detect, perform an incident risk assessment and notify your organization in the event of a data breach incident as required under your business associate agreement?	FY 2013	FY 2012	FY 2011	FY 2010
Very confident	11%			
Confident	16%			
Somewhat confident	33%			
Not confident	40%			
Total	100%			

Q24. In your opinion, which of the following business associates present the greatest risk to the privacy and security of patient data. Please select the top two?	FY 2013	FY 2012	FY 2011	FY 2010
IT service provider	75%			
Claims processor	47%			
Data analysts	8%			
Accounting services	4%			
Legal services	3%			
Consulting services	6%			
Benefits management	33%			
Pharmacy benefits manager (PBM)	19%			
Other (please specify)	5%			
Total	200%			

Q25a. Does your organization conduct and document post incident risk assessments as required in the Final Rule?	FY 2013	FY 2012	FY 2011	FY 2010
Yes, full compliance	51%			
Yes, partial compliance (in-process)	33%			
No	16%			
Total	100%			

Q25b. If yes, which one of the following choices best describes your process?	FY 2013	FY 2012	FY 2011	FY 2010
An ad-hoc process	23%			
A manual process or tool that was developed internally	34%			
An automated process or software tool that was developed internally	15%			
An automated process or software tool that was developed by a third party	20%			
A free tool that was developed by an external entity or association	8%			
Other (please specify)	0%			
Total	100%			

Q26a. How effective is your organization's incident risk assessment process?	FY 2013	FY 2012	FY 2011	FY 2010
Very effective	21%			
Effective	40%			
Not effective	39%			
Total	100%			

Q26b. If you selected not effective, what are your primary concerns? Please select all that apply.	FY 2013	FY 2012	FY 2011	FY 2010
Lack of consistency in the outcomes of the incident risk assessment process	79%			
Difficulty in using applications and tools	23%			
Lack of scalability of the process	48%			
Other (please specify)	6%			
Total	156%			

Q27a. How does the Affordable Care Act affect the privacy and security of patient information?	FY 2013	FY 2012	FY 2011	FY 2010
Significantly increases risk	36%			
Increases risk	33%			
No impact on risk	13%			
Decreases risk	6%			
Significantly decreases risk	7%			
Cannot determine	5%			
Total	100%			

Q27b. If you believe the risk to patient information increases, what are your primary concerns? Please select all that apply.	FY 2013	FY 2012	FY 2011	FY 2010
Patient registration on insecure websites	63%			
Patient data on insecure databases	65%			
Insecure exchange of patient information between healthcare providers and government	75%			
Other (please specify)	2%			
Total	205%			

Q28a. Is your organization part of an Accountable Care Organization (ACO)?	FY 2013	FY 2012	FY 2011	FY 2010
Yes	51%			
No	49%			
Total	100%			

Q28b. If yes, are you finding increased patient privacy and security risks with the exchange of patient health information among participants?	FY 2013	FY 2012	FY 2011	FY 2010
Yes	66%			
No	34%			
Total	100%			

Q28c. If yes, has your organization experienced changes in the number of unauthorized disclosures of PHI?	FY 2013	FY 2012	FY 2011	FY 2010
Yes, we noticed an increase	23%			
Yes, we noticed a decrease	3%			
No, we have not noticed any changes	33%			
Too early to tell	41%			
Total	100%			

Q29a. What best describes your organization's state of compliance with the Accounting of Disclosures requirement? Please select only one.	FY 2013	FY 2012	FY 2011	FY 2010
We are in full compliance	25%			
We are nearly in full compliance	23%			
We are not near full compliance	38%			
We are not taking steps to be in compliance	7%			
Unsure	7%			
Total	100%			

Q29b. If your organization is in full or near full compliance with the Accounting of Disclosures requirement, how is this achieved? Please select only one.	FY 2013	FY 2012	FY 2011	FY 2010
An ad-hoc process	31%			
A paper-based process or tool that was developed internally	27%			
A software-based process or tool that was developed internally	27%			
A software-based process or tool that was developed by a third party	15%			
Total	100%			

Q30a. Does your organization permit employees and medical staff to use their own mobile devices such as smart phones or tablets to connect to your organization's networks or enterprise systems (such as email)?	FY 2013	FY 2012	FY 2011	FY 2010
Yes	88%	81%		
No	12%	19%		
Total	100%	100%		

Q30b. If yes, approximately what percentage of your organization's employees (including part-time and contract employees) use their personally owned mobile device such as a smartphone or tablet?	FY 2013	FY 2012	FY 2011	FY 2010
Less than 10%	5%	5%		
10 to 25%	9%	11%		
26 to 50%	26%	35%		
51 to 75%	30%	21%		
More than 75%	30%	28%		
Total	100%	100%		
Extrapolated percentage use rate	57%	53%		

Q30c. 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 2013	FY 2012	FY 2011	FY 2010
Scan devices for viruses and malware prior to connection	22%	21%		
Scan devices and remove all mobile apps that present a security threat prior to connection	14%	16%		
Scan devices for viruses and malware while they are connected	36%	40%		
Require anti-virus/anti-malware software to reside on the mobile device prior to connection	23%	23%		
Require user to read and sign an acceptable use policy prior to connection	53%	45%		
Limit access from devices to critical systems including those that connect to PHI	56%	51%		
Limit or restrict the download of PHI onto these devices	44%	38%		
None of the above steps are done	38%	46%		
Other (please specify)	3%	2%		
Total	289%	282%		

Q30d. If yes, how confident are you that the personally-owned mobile devices used in your organization are secure?	FY 2013	FY 2012	FY 2011	FY 2010
Very confident	9%	9%		
Confident	17%	16%		
Somewhat confident	23%	21%		
Not confident	51%	54%		
Total	100%	100%		

Q31. 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 2013	FY 2012	FY 2011	FY 2010
Yes	30%	31%		
No	70%	69%		
Total	100%	100%		

Q32. What best describes your organization's use of cloud services?	FY 2013	FY 2012	FY 2011	FY 2010
No use of cloud services (skip to Q37)	8%	9%		
Light use of cloud services	23%	29%		
Moderate use of cloud services	29%	30%		
Heavy use of cloud services	40%	32%		
Total	100%	100%		

Q33. What cloud applications or services does your organization presently use? Please select all that apply.	FY 2013	FY 2012	FY 2011	FY 2010
Peer-to-peer communications (such as Skype)	39%	35%		
Social media applications (such as Facebook, LinkedIn, Twitter, etc.)	25%	26%		
Business applications (such as SalesForce.com, webmail, HR, etc.)	43%	39%		
Document sharing and collaboration (such as Dropbox, etc.)	42%	35%		
Infrastructure applications (online backup, security, archiving, etc.)	33%	33%		
Services such as identity management, payments, search and others	29%	28%		
Solution stacks such as Java, PHP, Python, ColdFusion and others	18%	19%		
Backup & storage	45%	41%		
Other (please specify)	3%	2%		
Total	277%	258%		

Q34. What types of information does your organization process and/or store in a public cloud environment? Please select all that apply.	FY 2013	FY 2012	FY 2011	FY 2010
Patient medical records	28%	26%		
Patient billing information	31%	30%		
Clinical trial and other research information	4%	5%		
Employee information including payroll data	44%	41%		
Administrative and scheduling information	31%	28%		
Accounting and financial information	49%	46%		
Email applications	53%	49%		
Productivity applications	49%	46%		
None of the above	34%	37%		
Other (please specify)	3%	2%		
Total	326%	310%		

Q35. What types of information does your organization consider **too sensitive** to be processed and/or stored in a public cloud environment? Please select all that apply.	FY 2013	FY 2012	FY 2011	FY 2010
Patient medical records	52%	56%		
Patient billing information	50%	51%		
Clinical trial and other research information	44%	37%		
Employee information including payroll data	31%	34%		
Administrative and scheduling information	25%	29%		
Accounting and financial information	32%	33%		
Email applications	12%	15%		
Productivity applications	13%	18%		
None of the above	34%	35%		
Other (please specify)	2%	2%		
Total	295%	310%		

Q36. How confident are you that information in a public cloud environment is secure?	FY 2013	FY 2012	FY 2011	FY 2010
Very confident	12%	11%		
Confident	21%	19%		
Somewhat confident	21%	23%		
Not confident	46%	47%		
Total	100%	100%		

Q37. What best describes your organization's privacy and security functions. Please select only one.	FY 2013	FY 2012	FY 2011	FY 2010
Privacy and security functions are completely separate	30%			
Privacy and security functions overlap in some places (hybrid)	51%			
Privacy and security functions are combined	19%			
Total	100%			

Q38. What security threats is your organization most concerned about? Select the top three.	FY 2013	FY 2012	FY 2011	FY 2010
Employee-owned mobile devices or BYOD	34%			
Mobile device insecurity	40%			
Use of public cloud services	41%			
Insecure medical devices	5%			
Employee negligence	75%			
Malicious insiders	13%			
Cyber attackers	39%			
Identity thieves	12%			
Insecure mobile apps (eHealth)	23%			
System failures	16%			
Other (please specify)	2%			
Total	300%			

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.