Second Annual Benchmark Study on Patient Privacy & Data Security

Sponsored by ID Experts

Independently conducted by Ponemon Institute LLC

Publication Date: December 2011

Second Annual Benchmark Study on Patient Privacy and Data Security

December 2011

Part 1. Introduction

Despite increased compliance with the HITECH Act and other federal regulations, healthcare data breaches are on the rise. Many hospitals and healthcare organizations in this study believe they have insufficient security and privacy budgets, and affected patients are not always receiving the privacy care they are promised. The growing use of unsecured mobile devices and the rising rate of employee mistakes compound the problem. This study was conducted to better understand healthcare providers' patient privacy practices and their experiences in dealing with the loss or theft of patient information, also called protected health information (PHI).

Our study found that the number of data breaches among healthcare organizations participating in the 2010 and 2011 studies is still growing—eroding patient privacy and contributing to medical identity theft. On average, it is estimated that data breaches cost benchmarked organizations $2,243,700. This represents an increase of $183,526 from the 2010 study despite healthcare organizations' increased compliance with federal regulations.

As the second annual study, the report examines the changes from 2010 to 2011 that may have occurred to healthcare organizations' privacy and data protection compliance activities, including policies, program management activities, enabling security technologies and security governance practices.[1] We also look at how well these organizations are able to comply with the notification requirements mandated by HITECH and HIPAA.

In some areas, healthcare organizations are making improvements in their efforts to stop data breaches. These include having more trained and knowledgeable staff and better policies and governance. Since last year's report, more respondents say that data breaches are being detected by employees or through audits and assessments. The percentage of respondents who say data breaches are discovered by patients has dropped from 41 percent to 35 percent. Healthcare organizations in this study also are relying less on an "ad hoc" process to prevent or detect data breach incidents and are relying more on policies, procedures and security technologies.

While those are positive trends, the study reveals respondents' concerns about the need to invest in enabling technologies, which may be a challenge because of budgetary constraints. To address the persistent problem of unintentional employee mistakes, healthcare organizations should focus on creating awareness among employees about the importance of safeguarding patient information. The following are the key research findings from this study.

Key Research Findings:

- **Data breaches in healthcare organizations are on the rise.** The frequency of data breaches among organizations in this study has increased 32 percent from the previous year. In fact, 96 percent of all healthcare providers say they have had at least one data breach in the last two years. Most of these were due to employee mistakes and sloppiness—49 percent of respondents in this study cite lost or stolen computing devices and 41 percent note unintentional employee action. Another disturbing cause is third-party error, including business associates, according to 46 percent of participants.

[1]The 2011 sample was matched to the 2010 sample based on organizational size, type of healthcare provider (entity) and regional location. We compare between-sample differences to infer possible trends over one year.

To reduce the risk of a data breach, healthcare personnel who handle sensitive and confidential patient information should be trained and aware of the policies and procedures governing the protection of this information. Billing records and medical files are considered by respondents to be the most frequently lost or stolen patient information. However, the perception is that not all personnel who are responsible for these documents understand the importance of protecting them. Sixty percent of respondents agree that medical billing personnel in their organizations do not understand the importance of patient data protection and 58 percent say IT personnel do not understand its importance. In contrast, 58 percent of respondents say administrative personnel do understand the importance of protecting patient data.

- **Widespread use of mobile devices is putting patient data at risk**. Eighty-one percent of healthcare organizations in this study report that they use mobile devices to collect, store, and/or transmit some form of PHI. However, 49 percent of participants admit their organizations do nothing to protect these devices.

- **Despite policies and federal mandates, prevention of unauthorized access to patient information is not a priority in many organizations in this study.** Forty-seven percent of respondents agree that their organization has sufficient policies that effectively prevent or quickly detect unauthorized patient data access, loss or theft. This is an increase from 41 percent of respondents last year. Concerns about the threat of upcoming HHS HIPAA audits and investigation has affected changes in patient data privacy and security programs, according to 55 percent of respondents.

  An area that needs to become more of a priority is privileged user and access governance. Only 29 percent of respondents agree that the prevention of unauthorized access to patient data and loss or theft of such data is a priority in their organizations.

- **Diminished productivity and financial consequences for healthcare organizations can be severe when a data breach incident occurs**. Respondents reported that the average economic impact of a data breach was $2.2 million, up 10 percent from last year. In addition, most respondents believe their organization has suffered from time and productivity loss (81 percent) followed by brand or reputation diminishment (78 percent) and loss of patient goodwill (75 percent). The potential result is patient churn; the average lifetime value of one lost patient (customer) is $113,400, an increase from $107,580 in last year's study.

- **Medical identity theft poses a greater risk to patients**. Employees are the group most likely to detect the data breach, according to 51 percent of participants. However, more than one-third (35 percent) of respondents say that data breaches were discovered by patient complaints. Once a breach is discovered, 83 percent of hospitals say that it takes in excess of one to two months to notify affected patients. Twenty-nine percent of respondents say their data breaches led to cases of identity theft, a 26 percent increase from last year.

  While 90 percent of healthcare organizations say that breaches cause harm to patients, the majority of them (65 percent) do not offer protection services for the affected patients. This may be due to the fact that 72 percent of respondents do not believe credit monitoring is effective and believe another solution for the prevention and detection of medical identity theft is needed.

Sponsored by ID Experts and conducted by Ponemon Institute, the study utilized in-depth, field-based research involving interviews with senior-level personnel at healthcare providers to collect information on the actual data loss and data theft experiences at their organizations. This benchmark research, in contrast to a traditional survey-based approach, enables researchers to collect both the qualitative and quantitative data necessary to understand the current status of patient privacy and data security in the healthcare organizations that participated in our study.

A total of 72 healthcare organizations participated in the study, an increase from last year's study when 65 healthcare organizations participated in this research. In both studies, the healthcare providers are integrated delivery systems—a network of healthcare organizations under a parent holding company (36 percent), part of a healthcare network (47 percent) and a standalone hospital or clinic (17 percent). Respondents interviewed work in all areas of the organization: security, administration, privacy, compliance, finance and clinical. On average we conducted 4 interviews in each organization. Last year we conducted 3.25 per organization.

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-six percent of organizations in our study have had at least one data breach in the past 24 months. On average organizations have had 4 data breach incidents during the past two years. Last year's report said the average was 3 per organization in the same timeframe.
- The average economic impact of a data breach over the past two years is approximately $2.2 million. This is an increase of approximately $200,000 in last year's study.
- The average number of lost or stolen records per breach was 2,575. This is an increase from an average of 1,769 reported in the previous year.
- The top three causes for a data breach are: lost or stolen computing devices, third-party snafu and unintentional employee action.
- Employees are most often the group to detect the data breach (51 percent) followed by 43 percent who say it was through audit/assessment and 35 percent say it was as a result of a patient complaint.
- More than half (55 percent) of respondents say they have little or no confidence that their organization has the ability to detect all privacy incidents and 57 percent say they have little or no confidence that their organization could detect all patient data loss or theft.
- The average time to notify data breach victims is approximately 7 weeks. Eighty-three percent of respondents believe it is critical to notify victims as soon as possible.
- The percentage of organizations fully implementing or in the process of implementing an electronic health records (EHR) system has increased from 56 percent last year to 66 percent in this year's study.
- Perceptions that EHR systems create more security decreased from 74 percent in last year's study to 67 percent of respondents this year. A higher percentage (19 percent vs. 12 percent) of respondents in this year's study say EHR has made no difference in the security of patient data.

Part 2. Key findings

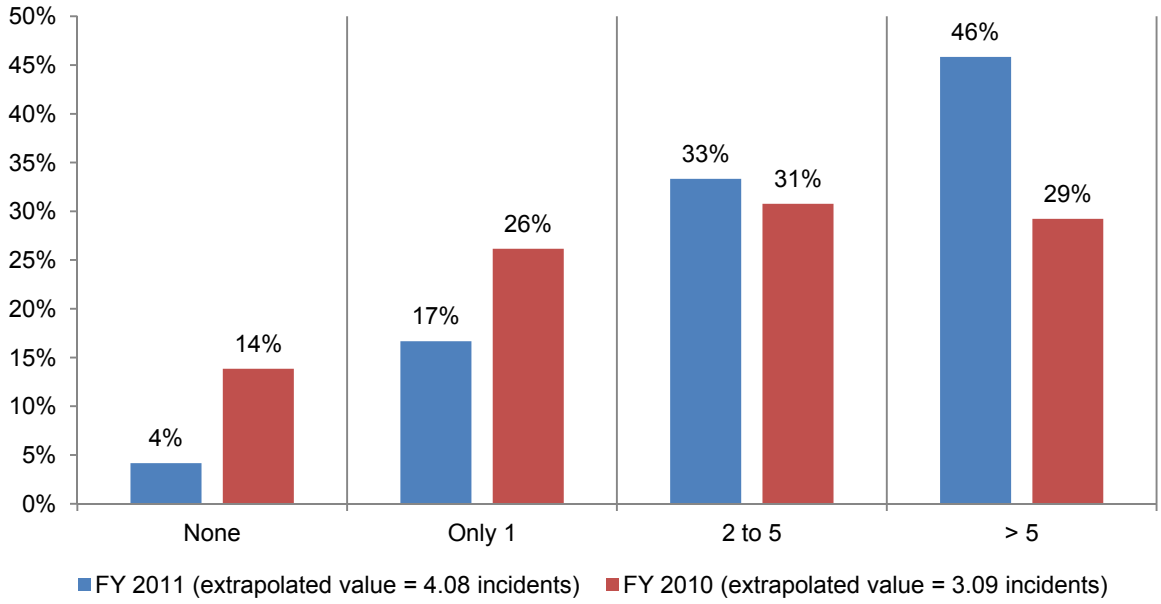
In this report, we have organized the most salient research results according to the following issues:

- The loss or theft of patient information experienced by healthcare providers in our study
- Barriers to detection and prevention of the loss or theft of patient information
- The impact of data breaches on providers and patients
- Providers' perceptions about their privacy and security environment

1. The loss or theft of patient information experienced by healthcare providers in our study

Data breaches in healthcare organizations are on the rise. In this year's study, 96 percent of respondents say their organizations have had at least one data breach, as shown in Bar Chart 1. Since last year's study, the average number of data breach incidents in organizations included in this study has increased from 3.09 to 4.08 incidents, respectively.

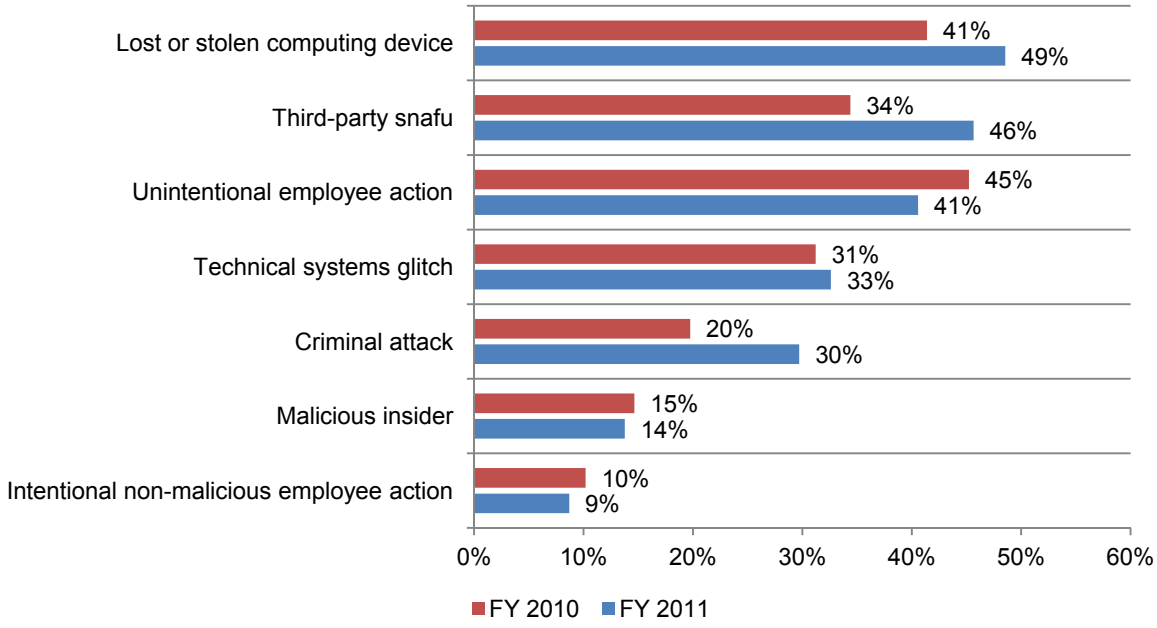
Bar Chart 1: Has your department suffered a data breach involving the loss or theft of patient data in the past two years as defined above?



The average number of lost or stolen records per breach was 2,575, an increase from 1,769 in the previous study. According to participants, it takes on average about 7 weeks to notify victims. Eighty-three percent of respondents believe it is critical to notify victims as soon as possible.

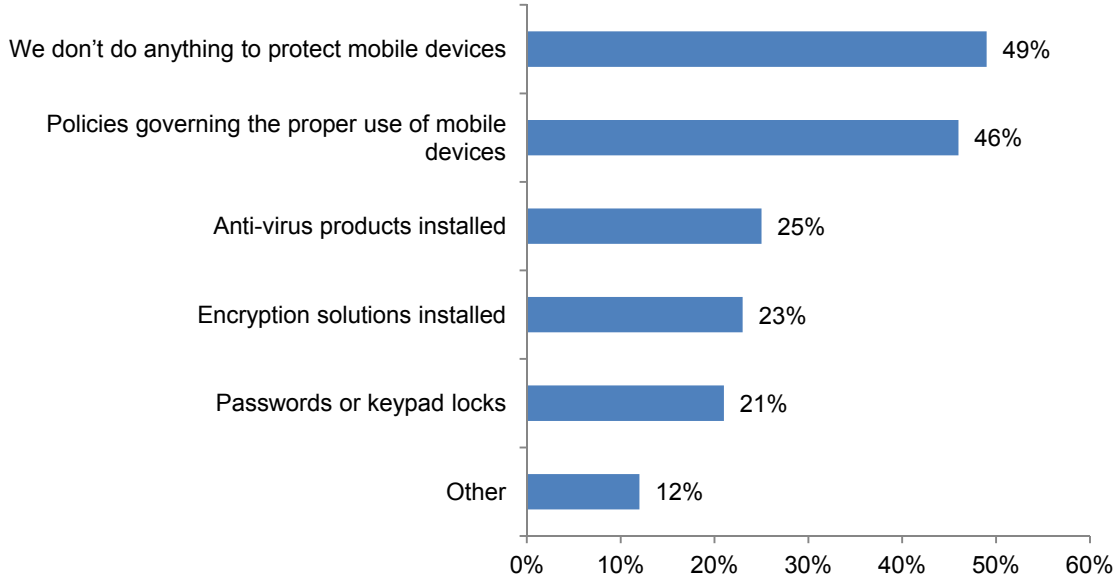
Bar Chart 2 reveals that the top three causes for data breaches remain unchanged from last year. The only exception is that lost or stolen computing devices have been cited by 49 percent of respondents (an increase from 41 percent last year). This is followed by third-party snafu (46 percent vs. 34 percent last year) and unintentional employee action (41 percent vs. 45 percent last year). According to Bar Chart 2, third party snafus as a root cause had the greatest increase. Criminal attacks followed with an increase from 20 percent to 30 percent of respondents reporting this as the root cause. Not shown in the chart is how breaches have been detected: through an employee (51 percent), an audit/assessment (43 percent) or as a result of a patient complaint (35 percent).

Bar Chart 2: Nature or root causes of the data breach incident
More than one choice permitted



Widespread use of mobile devices is putting patient data at risk. Given the concerns over the security of mobile devices and the finding that lost or stolen computing devices is often the number one cause of a data breach, we asked IT practitioners if their organizations use mobile devices that may collect, store and/or transmit PHI. According to Bar Chart 3, 81 percent say this is the case but almost half (49 percent) of respondents say their organizations don't do anything to protect these mobile devices and 46 percent depend upon policies and governance. Only 23 percent use encryption to safeguard patient data. As a result, only 15 percent are very confident and 23 percent are somewhat confident that patient data is protected from being accessed via mobile devices.

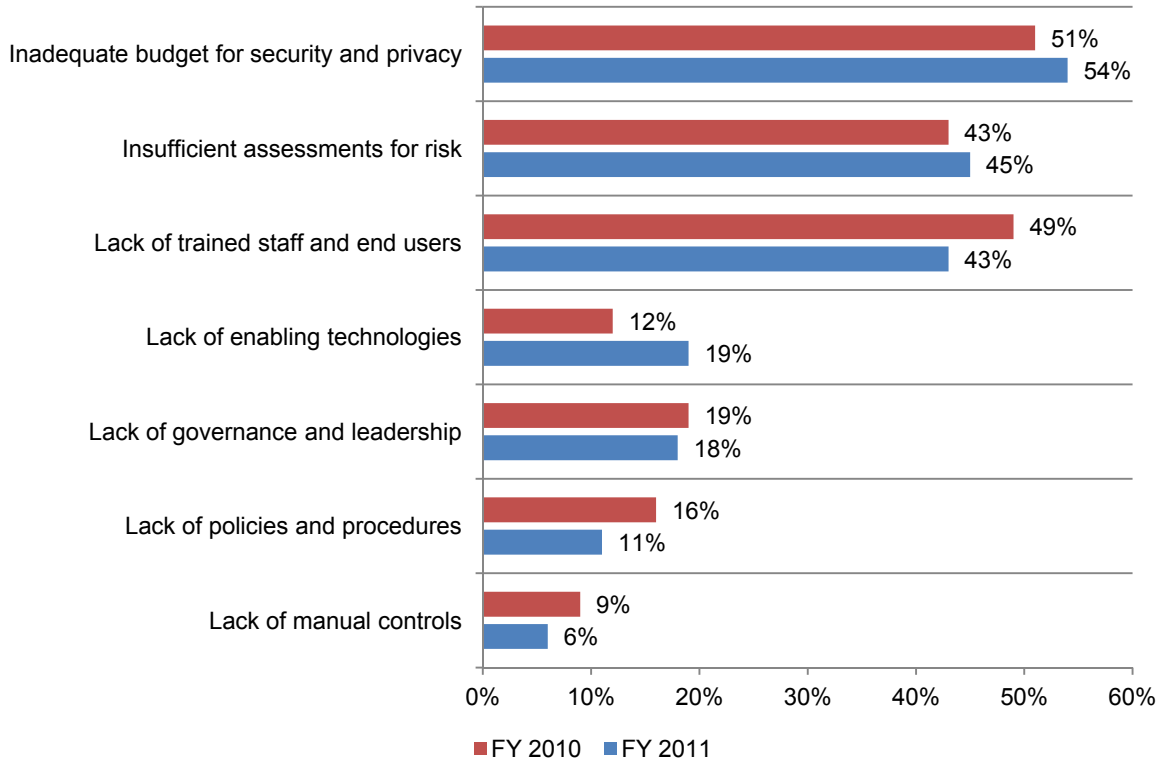
Bar Chart 3: Does your organization use any of the following security solutions or procedures to safeguard patient data contained on mobile devices?
More than one choice permitted



2. Barriers to the detection and prevention of the loss or theft of patient information

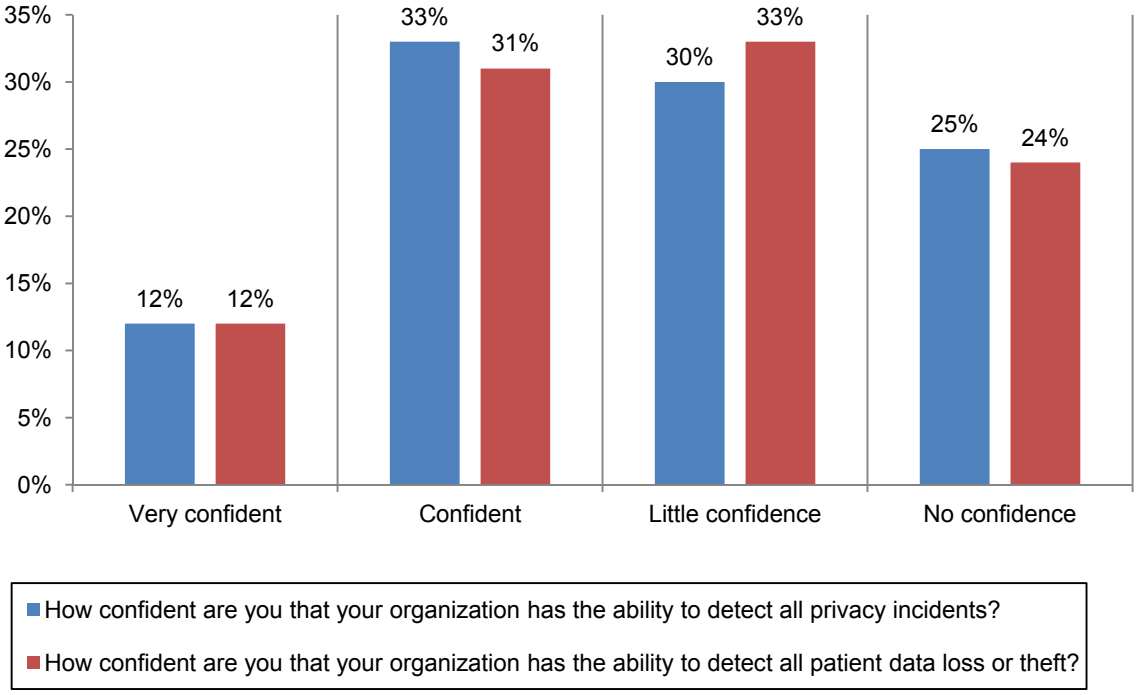
Insufficient budget and risk assessments are organizations' greatest weaknesses. Inadequate budget for security and privacy and insufficient assessments for risk have increased as weaknesses this year, as shown in Bar Chart 4. In addition, the lack of enabling technologies as a weakness increased from 12 percent to 19 percent. However, as a weakness the lack of trained staff and end users has declined from 49 percent to 43 percent of respondents. Also, respondents in this year's study are more positive about the availability of policies and procedures to address data breach risks.

Bar Chart 4: What do you believe are your two greatest weaknesses to preventing a data breach?
More than one choice permitted



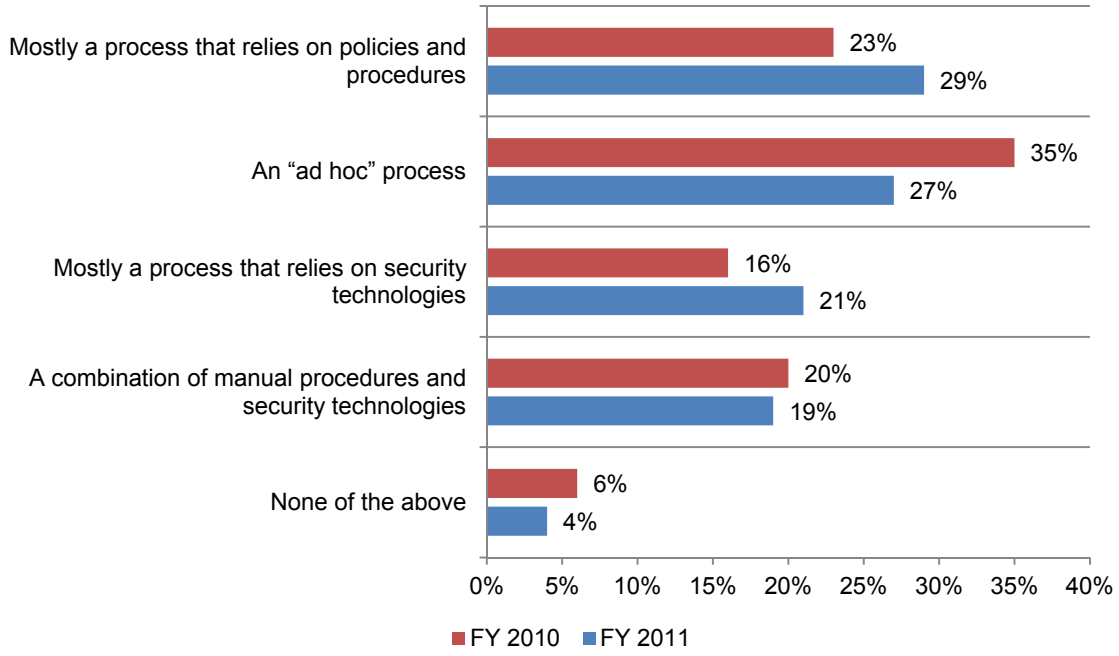
While organizations seem to be making progress in having sufficient technical expertise as well as trained staff and end users, the ability to detect all privacy incidents and all patient data loss or theft remains an elusive goal. Bar Chart 5 reveals that the majority of respondents have little (30 percent) or no confidence (25 percent) in their organizations' ability to detect all privacy incidents and an even higher percentage have little (33 percent) or no confidence (24 percent) in their organizations' ability to detect all patient data loss or theft. This level of confidence is understandable given the increase in the average number of data breaches occurring and the increase in the loss of patient records.

Bar Chart 5: How confident are you about your organization's ability to detect privacy incidents and the loss of patient data?



As shown in Bar Chart 6, comparison FY 2011 to FY 2010 results, fewer participants say their healthcare organizations are relying on an "ad hoc" process to prevent and detect data breach incidents. In contrast, more participants say their organizations are relying on policies, procedures and security technologies.

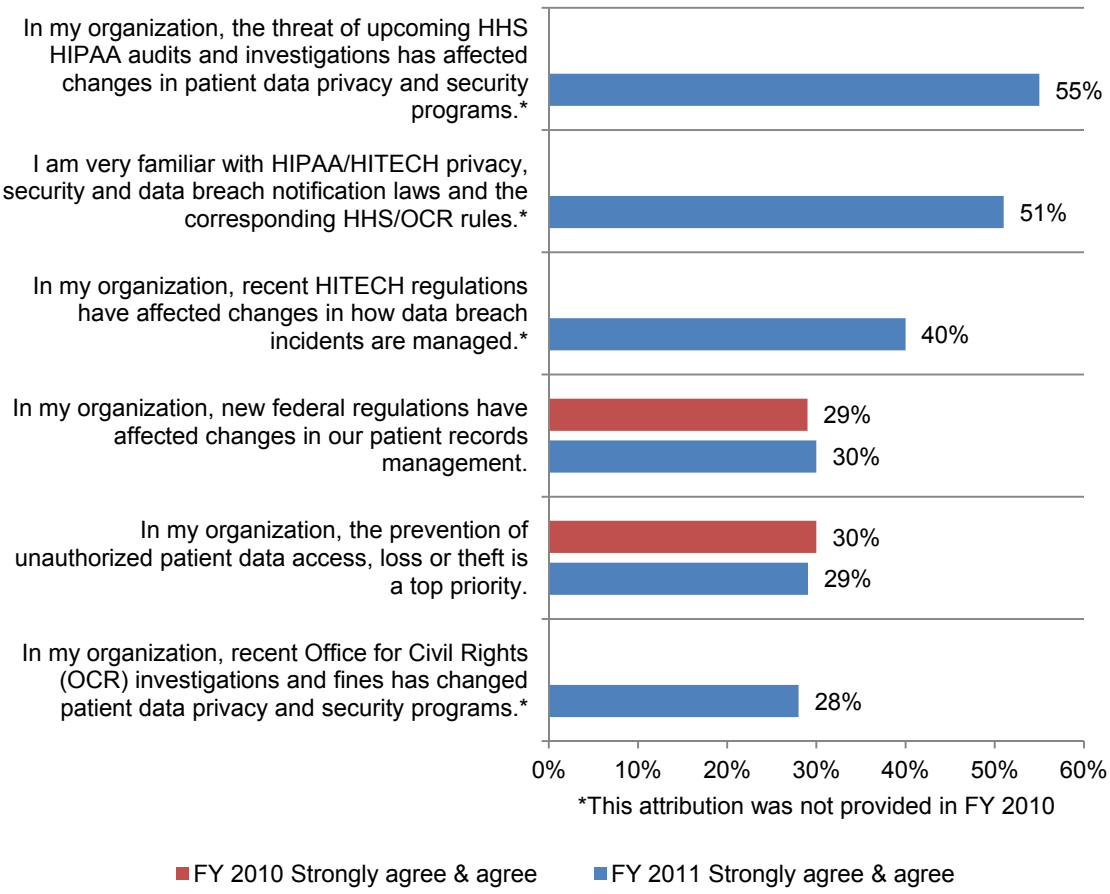
Bar Chart 6: What best describes the process for preventing and detecting data breach incidents in your organization today?



Despite policies and federal mandates, prevention of unauthorized access to patient information is not a priority in many organizations in this study. Forty-seven percent of respondents agree that their organization has sufficient policies that effectively prevent or quickly detect unauthorized patient data access, loss or theft. This is an increase from 41 percent of respondents last year.

As shown in Bar Chart 7, only 29 percent of respondents agree that the prevention of unauthorized access to patient data and loss or theft of such data is a priority.[2] Slightly more than half (55 percent) of respondents do agree that the threat of upcoming HHS HIPAA audits has affected changes in patient data privacy and security programs.

Bar Chart 7: Attributions about the impact of federal regulations
Five-point scale from strongly agree to strongly disagree



However, what is having a lesser impact on procedures are recent HITECH regulations on how data breach incidents are managed, on patient records management and how recent Office for Civil Rights (OCR) investigations and fines have changed patient data privacy and security programs.

More than half of respondents (51 percent), say they are very familiar with HIPAA/HITECH privacy, security and data breach notification laws and the corresponding HHS/OCR rules. However, 46 percent of respondents say others in their organization are knowledgeable about

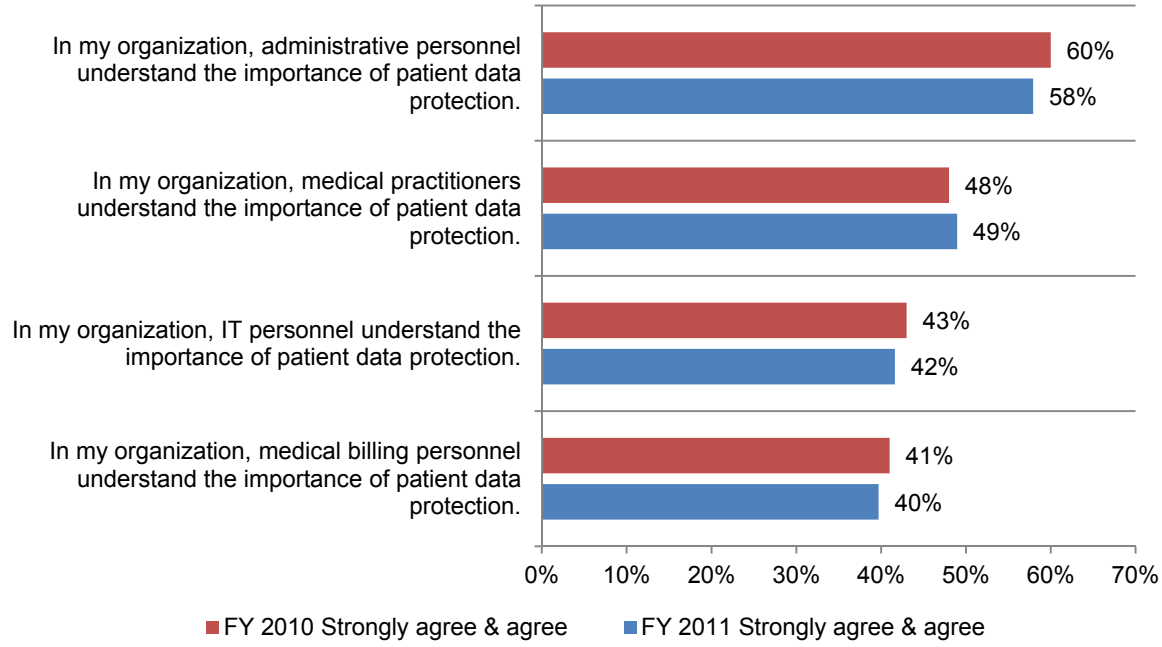
[2]Responses to attributions are rated from strongly agree to strongly disagree. A strongly agree and agree response combined that is equal to or exceeds 50 percent indicated a favorable response. A strongly disagree, disagree and unsure response that exceeds 50 percent indicates an unfavorable response.

compliance with healthcare regulations, including data breach notification and burden of proof and incident risk assessment requirements (not shown in the chart).

To reduce the risk of a data breach, healthcare personnel who handle sensitive and confidential patient information should be trained and aware of the policies and procedures governing the protection of this information. Billing records and medical files are considered by respondents to be the most frequently lost or stolen patient information.

Despite this reality, the perception is that not all personnel who are responsible for these documents understand the importance of protecting them. Only 40 percent of respondents agree that medical billing personnel in their organizations do understand the importance of patient data protection and 42 percent say IT personnel do not understand its importance. In contrast, 58 percent of respondents say administrative personnel understand the importance of protecting patient data.

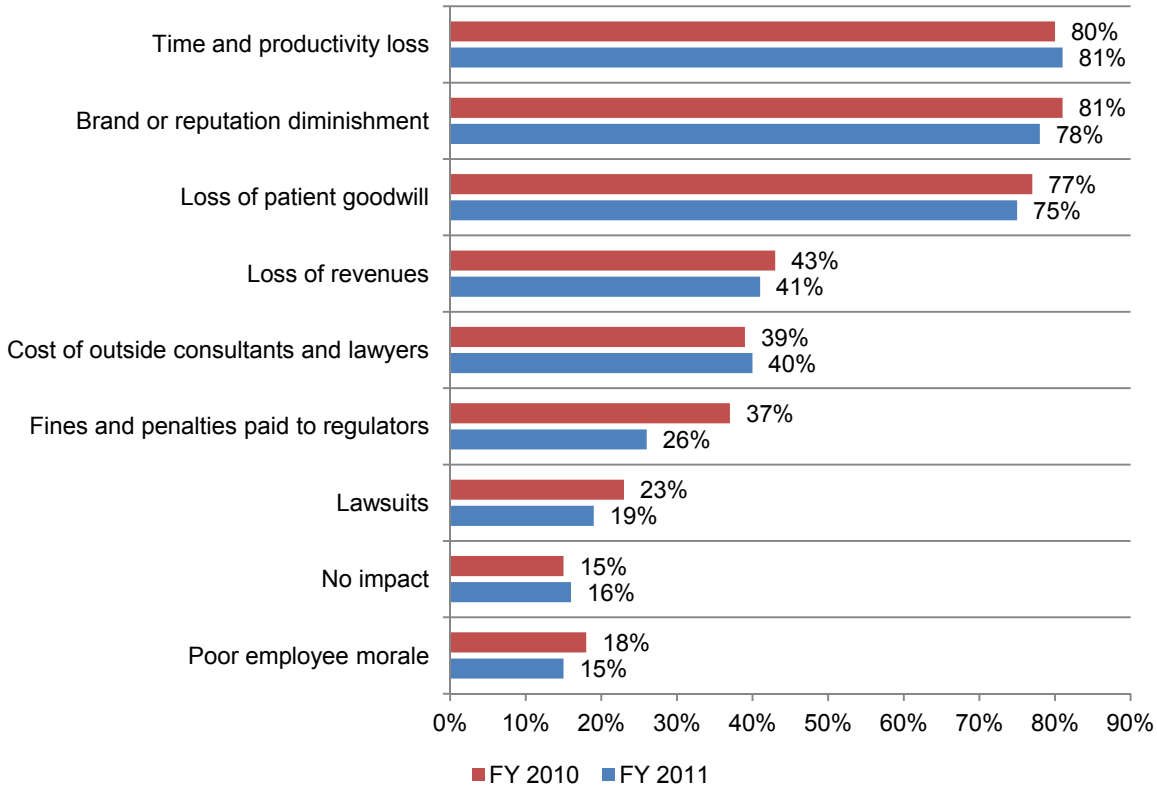
Bar Chart 8: Attributions about the impact of operational issues
Five-point scale from strongly agree to strongly disagree



3. The impact of data breaches on providers and patients

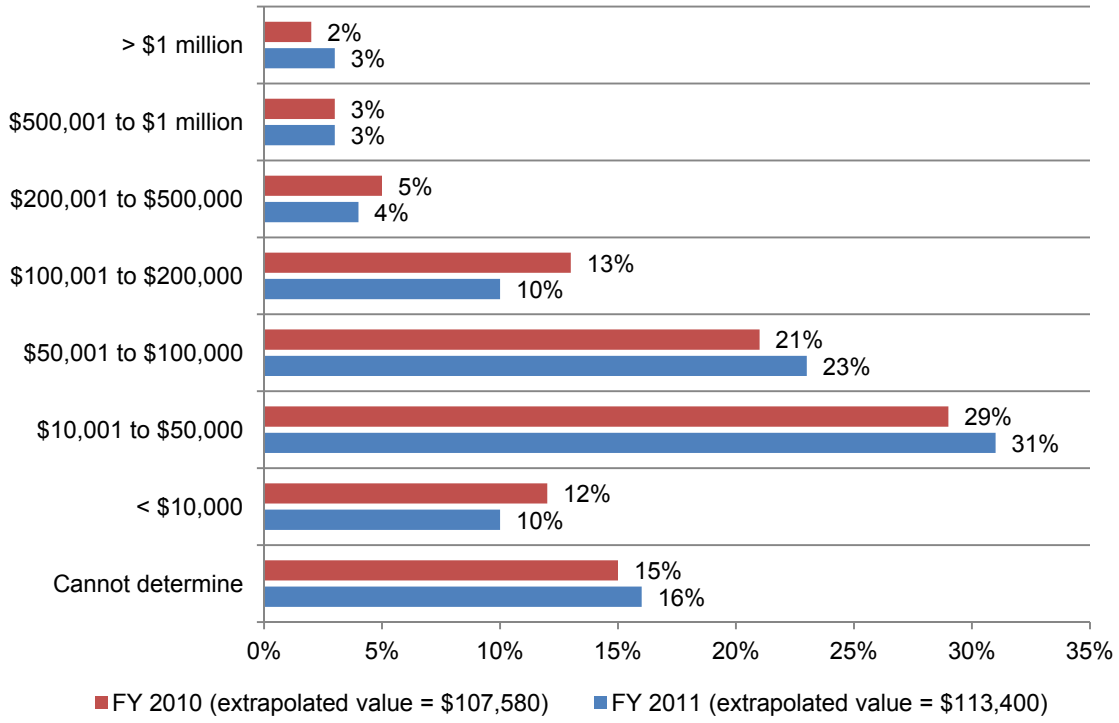
Diminished productivity and financial consequences for healthcare organizations can be severe when a data breach incident occurs. Very few (16 percent) say the breach had no negative impact on their organization. Bar Chart 9 reveals that most respondents believe they have suffered from time and productivity loss (81 percent) followed by brand or reputation diminishment (78 percent) and loss of patient goodwill (75 percent). The least negative affects were lawsuits (19 percent) and poor employee morale (15 percent).

Bar Chart 9: What best describes the negative impact of data breach incidents experienced by your organization over the past two years?
More than one choice permitted



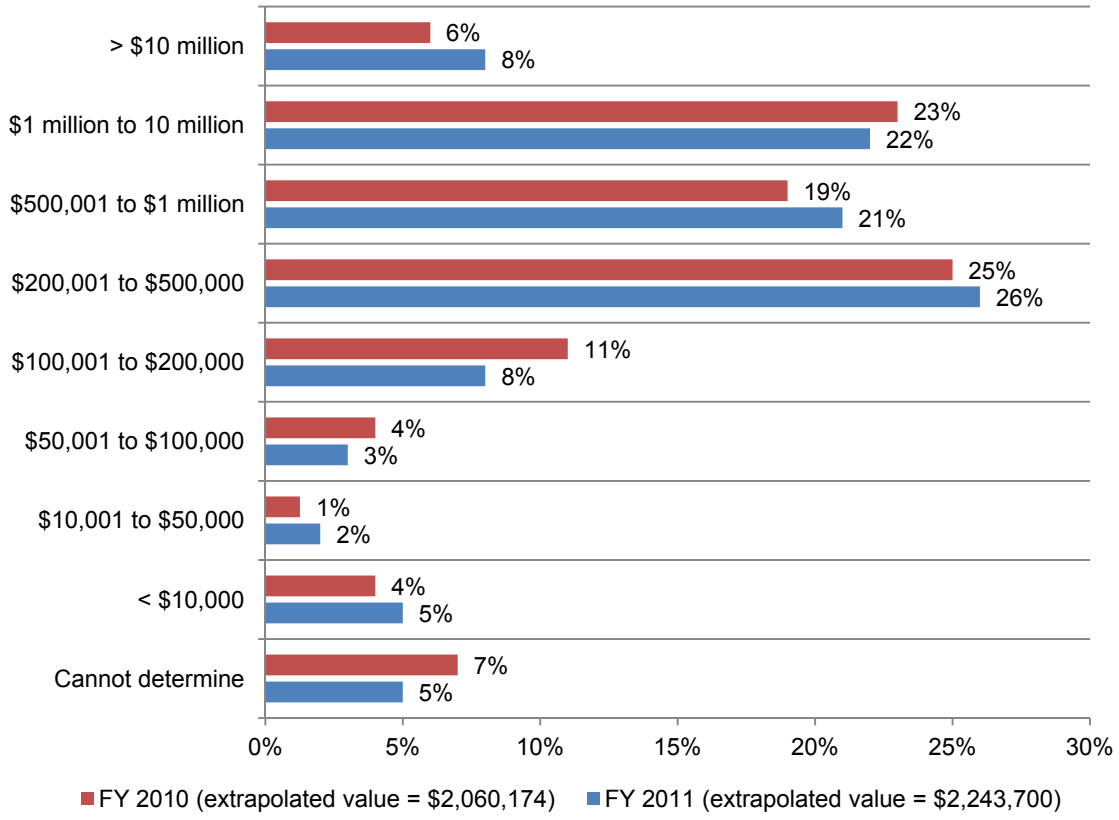
As mentioned above, one of the most negative consequences of a data breach is brand or reputation diminishment related to this is the loss of patient goodwill. The potential result is patient churn. According to respondents (using an extrapolation method), the average lifetime value of one lost patient (customer) is $113,400, an increase from $107,580 in last year's study. The distribution used for this extrapolation is reported in Bar Chart 10.

Bar Chart 10: What best describes the lifetime economic value, on average, of one patient or customer to your organization?



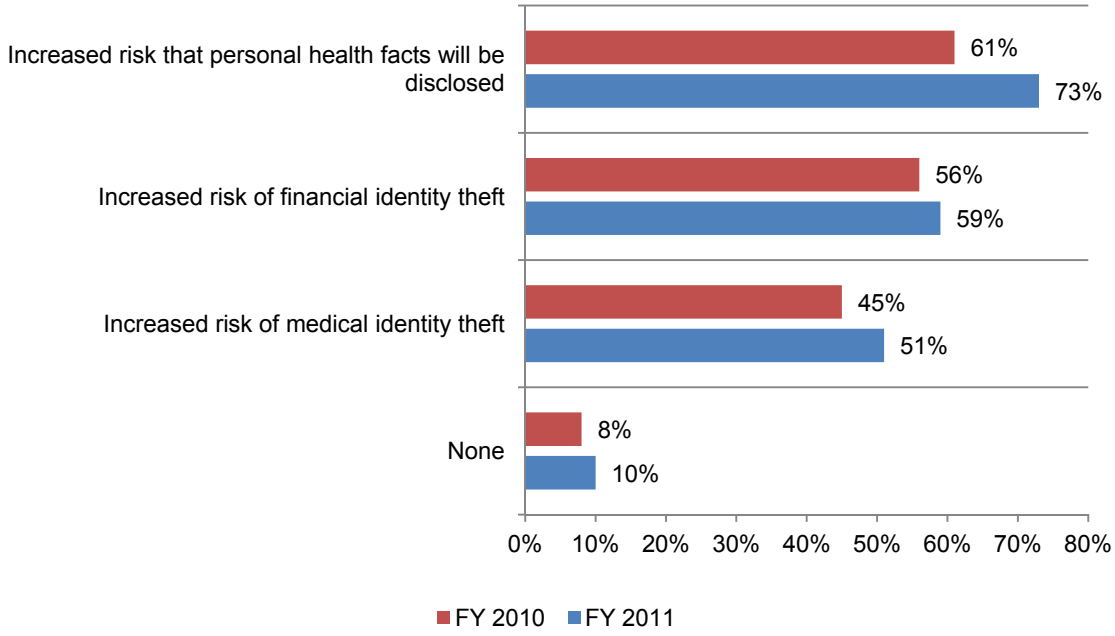
Again using an extrapolation method, the average economic impact of a data breach as determined by respondents has also increased from $2,060,174 to $2,247,700. Bar Chart 11 shows the distribution used in this extrapolation. While not shown in a chart, we also determined healthcare organizations spent, on average, $249,290 on legal fees during the past year to resolve data breaches and other privacy violations.

Bar Chart 11: What best describes the economic impact of data breach incidents experience by your organization over the past two years?



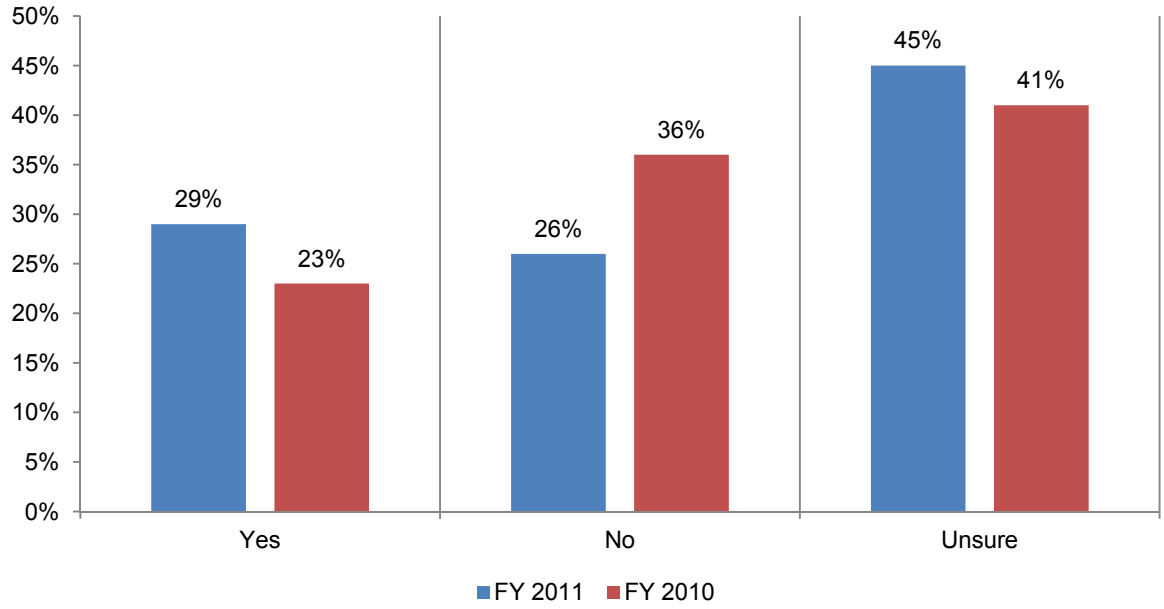
Medical identity theft poses a risk to patient data. Bar Chart 12 reveals that 73 percent of respondents' say the harm patients suffer as a result of a data breach is the increased risk that personal health facts will be disclosed followed by an increased risk of financial identity theft (59 percent) and increased risk of medical identity theft (51 percent). Only 10 percent say patients suffer no harms. These percentages all represent an increase from last year's study.

Bar Chart 12: What harms do patients actually suffer if their records are lost or stolen?
More than one choice permitted



Because so many organizations have difficulty in detecting a data breach and confirming the cause, a significant number of respondents (45 percent) are unsure whether or not the breach led to any cases of identity theft (financial or medical), according to Bar Chart 13.

Bar Chart 13: If you organization has experienced a data breach, has the breach led to any cases of identity theft (financial or medical) among the affected population?

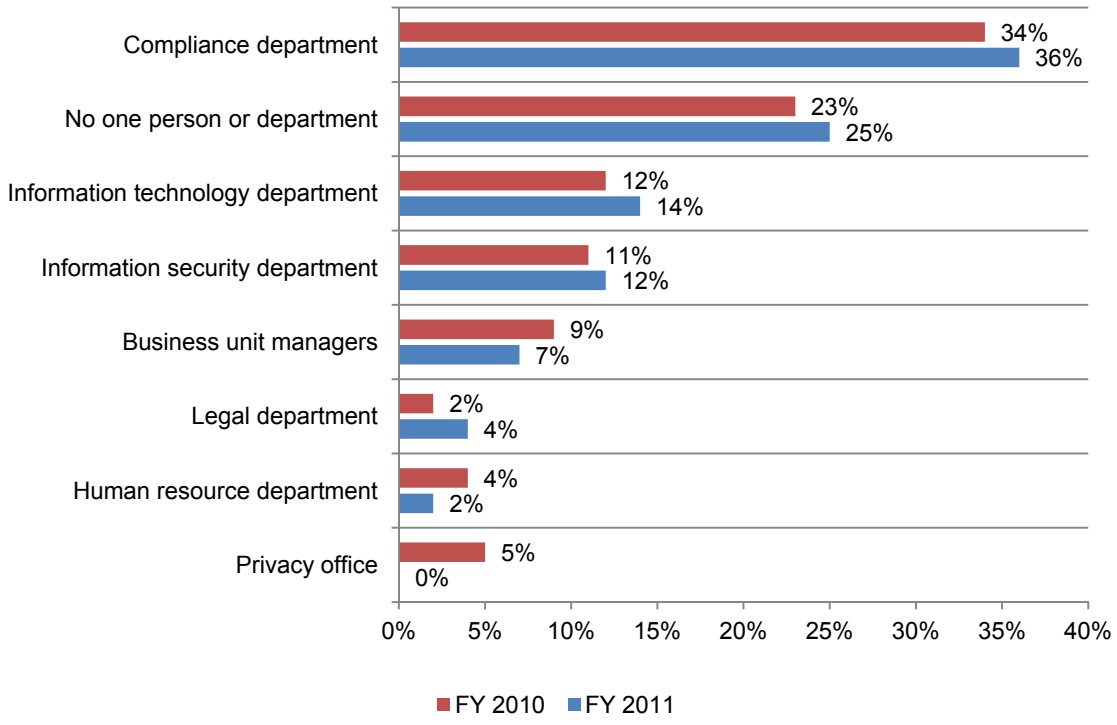


Further, the majority of organizations (65 percent) do not offer victims protection services. Seventy-two percent say that credit monitoring is not effective and 74 percent of those respondents believe there should be another solution for the prevention and detection of medical identity theft.

4. Providers' perceptions about their organizations' privacy and security environment

Security technologies are considered essential or very important to defending their organizations' patient data, according to 72 percent of respondents. However, as shown in Bar Chart 14, the function considered by respondents to be most responsible for preventing and detecting data breach incidents is the compliance department (36 percent) followed by no one person or department (25 percent). The IT and IT security functions are at a lowly 14 percent and 12 percent, respectively. This is virtually unchanged from last year.

Bar Chart 14: Who is most responsible for preventing and detecting data breach incidents in your organization?



As shown in Table 1, IT respondents in this year's study are more confident in their ability to identify major data breaches involving patient information (44 percent vs. 32 percent) and determining the root causes of major data breaches involving patient information (43 percent vs. 30 percent). However, only 29 percent are very confident or confident that they can prevent or curtail major data breaches involving patient information. Last year 31 percent had this level of confidence. This decline could be attributed to the increase in data breaches experienced by healthcare organizations.

Attributes that describe information security environment for healthcare organizations. These are rated based on the respondents' level of confidence that their organization presently accomplishes the stated attribute.	Very confident and confident response combined*	
Table 1: Information security environment	FY 2011	FY 2010
Comply with all applicable privacy laws and statutes	87%	85%
Training and awareness program for all system users	73%	71%
Ensure minimal downtime or disruptions to systems resulting from security problems	66%	65%
Enforce policies, including the termination of employees who pose insider threats	64%	72%
Perform timely updates for all major security patches	57%	53%
Have agreements with business associates that define data protection requirements	56%	66%
Conform with leading self-regulatory requirements such as ISO, NIST and others	54%	61%
Prevent or curtail viruses and malware infections	53%	56%
Attract and retain high quality IT security personnel	51%	55%
Secure patient data in motion	50%	47%
Security program administration is consistently managed	50%	52%
Secure patient data at rest	47%	42%
Identify major data breaches involving patient information	44%	32%
Determine the root causes of major data breaches involving patient information	43%	30%
Secure endpoints to the network	43%	51%
Identify system end-users before granting access rights to patient information	42%	45%
Protect patient information used by outsourcers including cloud computing vendors	40%	10%
Know where patient information is physically located	39%	47%
Control all live data used in systems development activities	38%	39%
Prevent or curtail cyber attacks	37%	39%
Conduct independent audits of the system	36%	45%
Prevent or curtail cyber attacks that attempt to acquire patient information	33%	37%
Protect patient information used by business associates	31%	29%
Prevent or curtail major data breaches involving patient information	29%	31%
Limit physical access to data storage devices containing patient information	22%	23%
Demonstrate the economic value or other tangible benefits of the security program	16%	17%
Average	46%	46%

*Four-point scale from very confident to not confident

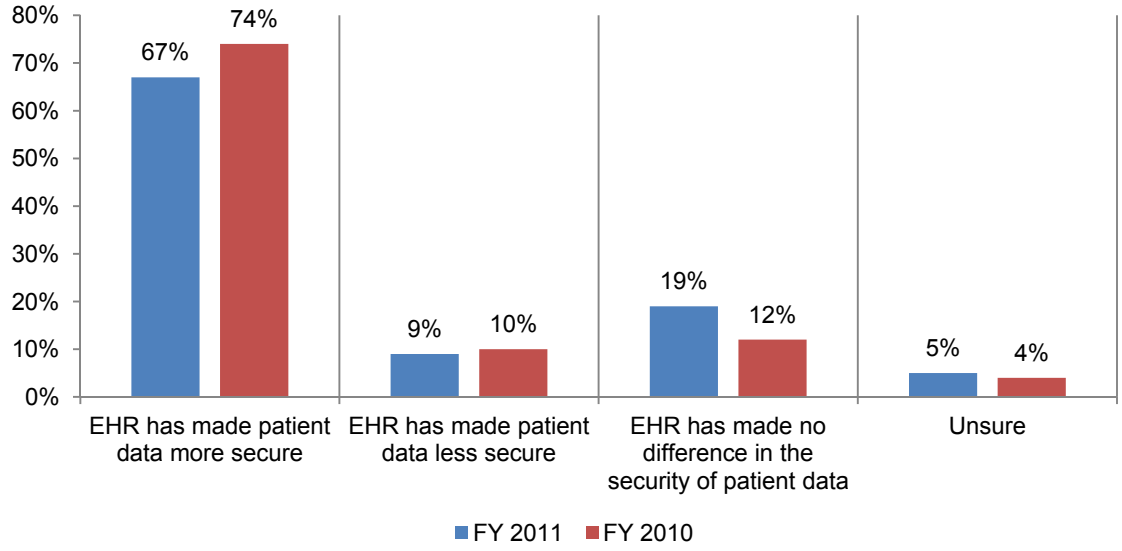
In general, respondents appear to be most confident about their organization's ability to comply with legal requirements and policies including privacy laws and statutes followed by training and awareness programs for all system users and the ability to ensure minimal downtime or disruption to systems resulting from security problems. They are also confident that their organization can

enforce corporate policies, including the termination of employees or contractors who pose a serious insider threat and have standard agreements with business associates that clearly explain the requirements for data protection.

In contrast, respondents are not very confident in limiting physical access to data storage devices containing patient information and demonstrating the economic value or other tangible benefits of the company's security program.

The percentage of organizations fully implementing or in the process of implementing an electronic health records (EHR) system has increased from 56 percent last year to 66 percent in this year's study. As reported in Bar Chart 15, the percentage of respondents who believe EHR has made patient data more secure has declined from 74 percent to 67 percent. A higher percentage (19 percent vs. 12 percent) of respondents in this year's study say EHR has made no difference in the security of patient data.

Bar Chart 15: If your organization has implemented an EHR system, what impact do you think it has had on privacy and security of patient data?



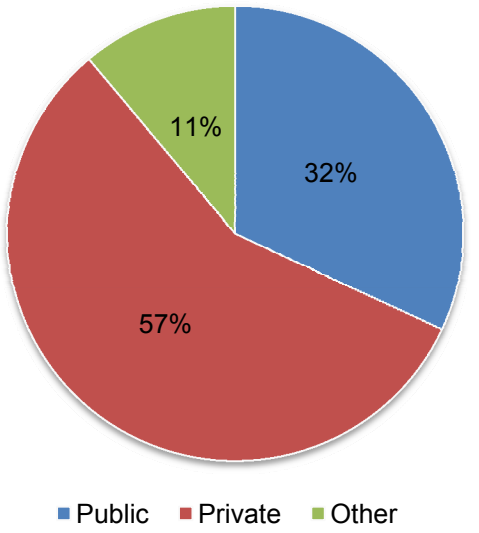
Part 3. Benchmark Methods

Table 2 summarizes the response completed over a three-month period concluding in November 2011. A total of 511 health care organizations were selected for participation and contacted by the researcher. Ninety-nine organizations agreed to complete the benchmark survey; however, 75 completed the benchmark instrument. Three benchmarked organizations were deemed incomplete and, hence, removed from the sample. A final sample of 72 organizations was used in our analysis, which is a net increase of seven organizations from our 2010 study.

Table 2: Benchmark sampling response	Freq	Pct%
Total healthcare organizations contacts made	511	100%
Total healthcare organizations recruited	98	19%
Total healthcare organizations participating	75	15%
Incomplete responses	3	1%
Final benchmark sample	72	14%

Pie Chart 1 reports the type of healthcare providers that participated in this research, with 57 percent represented private organizations. Pie Chart 2 shows the size of organizations with respect to the number of patient beds. Forty-one 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)

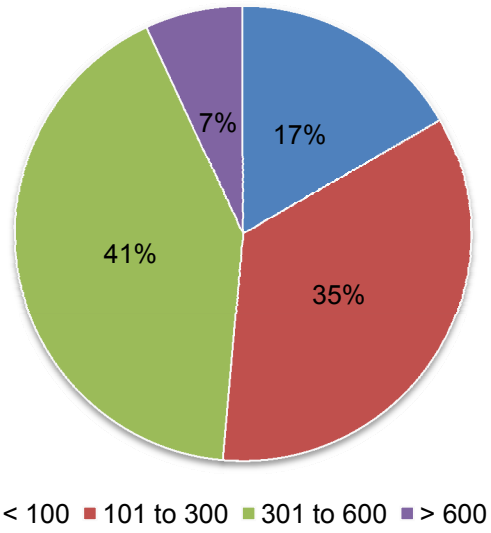


Table 3 provides a detailed breakdown of our final sample by US region. It shows the Northeast and mid-Atlantic regions as having the highest frequency of responding organizations.

Table 3: U.S. regional location	Freq	Pct%
Northeast	16	22%
Mid-Atlantic	15	21%
Midwest	11	15%
Southeast	9	13%
Southwest	9	13%
Pacific-West	12	17%
Total	72	100%

Table 4 reports the department locations of individuals who responded to benchmark questions. As can been, compliance and IT are the most frequently cited functional areas. In total, 300 individuals from 72 organizations completed the diagnostic interview with the researcher (for an average of 4.17 per participating healthcare entity). Last year's study involved 211 individuals from 65 organizations completing the diagnostic interviews.

Table 4. Department locations participating on organizations	Freq	Pct%
Chief security officer	16	5%
Chief information security officer	29	10%
Chief information officer	32	11%
Chief privacy officer	18	6%
Chief compliance officer	33	11%
Chief medical officer	9	3%
Chief clinical officer	2	1%
Chief finance officer	11	4%
Chief development officer	5	2%
General counsel	15	5%
HIPAA compliance leader	33	11%
Billing & administrative leader	36	12%
Medical records management leader	33	11%
Human resources leader	14	5%
Clinician	10	3%
Other	4	1%
Total	300	100%
Average number of interviews per HC organization	4.17	

Part 4. Limitations

The presented findings are based on self-reported benchmark survey returns.[3] Usable returns from 72 organizations – or about 14 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 decided to omit 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 2011 results to a benchmark study completed one year earlier. While these two samples were approximately matched based on organizational size, type and regional location, we can only infer trends from between-sample differences.

[3] The survey was developed with the assistance and input of ID Experts. The final survey was reviewed before launch by Fellows of Ponemon Institute, members of the RIM Council and other learned experts.

Part 5. Conclusion

We believe this second annual study continues to help healthcare organizations concerned about their privacy and data security practices to better understand their risks and areas of vulnerability. As is shown in this study, healthcare providers are at risk of non-compliance with regulations based on their practices. They also risk severe economic consequences based on the data breach experience of organizations in this study.

In some areas, healthcare organizations are making improvements. These include having more trained and knowledgeable employees who are better at detecting and reporting a data breach. Areas that are in need of improvement include the availability of enabling technologies. We believe this information can help organizations benchmark their own practices to understand how best to allocate their resources to strengthen their security and privacy safeguards.

Appendix: Detailed Results

The following tables provide the frequency and percentage frequency of all benchmark survey questions completed by 72 participating companies. All field research was completed over a three-month period concluding in November 2011.

Benchmark sampling response	Freq	Pct%
Total healthcare organizations contacts made	511	100%
Total healthcare organizations recruited	98	19%
Total healthcare organizations participating	75	15%
Incomplete responses	3	1%
Final benchmark sample	72	14%

Part 1: Organizational characteristics		
Q1a. What best describes your organization:	Freq	Pct%
Public	23	32%
Private	41	57%
Other	8	11%
Total	72	100%

Q1b. How many patient beds (capacity) does your organization have?	Freq	Pct%
< 100	12	17%
101 to 300	25	35%
301 to 600	30	42%
> 600	5	7%
Total	72	100%

Q1c. What best describes your organization's operating structure?	Freq	Pct%
Integrated Delivery System	26	36%
Hospital or clinic that is part of a healthcare network	34	47%
Standalone hospital	12	17%
Other	0	0%
Total	72	100%

Q1d. Please indicate the region of the United States where you are located.	Freq	Pct%
Northeast	16	22%
Mid-Atlantic	15	21%
Midwest	11	15%
Southeast	9	13%
Southwest	9	13%
Pacific-West	12	17%
Total	72	100%

Q1e. What best describes your role or the role of your supervisor?	Freq	Pct%
Chief security officer	16	5%
Chief information security officer	29	10%
Chief information officer	32	11%
Chief privacy officer	18	6%
Chief compliance officer	33	11%
Chief medical officer	9	3%
Chief clinical officer	2	1%
Chief finance officer	11	4%
Chief development officer	5	2%
General counsel	15	5%
HIPAA compliance leader	33	11%

Billing & administrative leader	36	12%
Medical records management leader	33	11%
Human resources leader	14	5%
Clinician	10	3%
Other	4	1%
Total	300	100%
Average number of interviews per HC organization	4.17	

Q1f. What best describes your department?	Freq	Pct%
Compliance	72	100%
Privacy	28	39%
Information technology (IT)	55	76%
Legal	15	21%
Finance	11	15%
Marketing	6	8%
Medical informatics	17	24%
Medical staff	13	18%
Patient services	34	47%
Records management	10	14%
Risk management	11	15%
Development – foundation	8	11%
Planning	3	4%
Human resources	14	19%
Other	3	4%
Total	300	417%
Average number of interviews per HC organization	4.17	

	Five-point scale	
Part 2. Attributions. Please rate your opinion about the statements contained next to each statement using the scale provided.	Strongly agree	Agree
Q2. My organization has sufficient policies and procedures that effectively prevent or quickly detect unauthorized patient data access, loss or theft.	21%	26%
Q3. My organization has sufficient technologies that effectively prevent or quickly detect unauthorized patient data access, loss or theft.	16%	22%
Q4. My organization has sufficient resources to prevent or quickly detect unauthorized patient data access, loss or theft.	9%	18%
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.	17%	28%
Q6. My organization has personnel who are knowledgeable about compliance with healthcare regulations including data breach notification and burden of proof and incident risk assessment requirements.	20%	26%
Q7. In my organization, medical practitioners understand the importance of patient data protection.	27%	22%
Q8. In my organization, administrative personnel understand the importance of patient data protection.	30%	28%
Q9. In my organization, medical billing personnel understand the importance of patient data protection.	19%	21%
Q10. In my organization, IT personnel understand the importance of patient data protection.	19%	23%
Q11. In my organization, the prevention of [unauthorized patient data access/patient data], loss or theft is a top priority.	12%	17%
Q12. In my organization, [recent HITECH regulations/new federal regulations] have affected changes in our patient records management.	14%	16%

Q13. In my organization, recent HITECH regulations have affected changes in how data breach incidents are managed.	19%	21%
Q14. I am very familiar with HIPAA/HITECH privacy, security and data breach notification laws and the corresponding HHS/OCR rules.	25%	26%
Q15. In my organization, recent Office for Civil Rights (OCR) investigations and fines has changed patient data privacy and security programs.	15%	13%
Q16. In my organization, the threat of upcoming HHS HIPAA audits and investigations has affected changes in patient data privacy and security programs.	25%	30%

Part 3: Privacy Incidents & Data Breach		
Q17. How many privacy incidents that were not classified as a data breach has your organization experienced in the past year?	Freq	Pct%
None	3	4%
Less than 5	5	7%
Between 6 and 10	14	19%
Between 11 and 20	17	24%
Between 21 and 30	26	36%
Between 31 and 50	4	6%
More than 50	3	4%
Total	72	100%
Extrapolated average number of privacy incidents not classified as a data breach for the benchmark sample	18.8	
Extrapolated total number of privacy incidents not classified as a data breach for the benchmark sample	1,350	

Q18. How confident are you that your organization has the ability to detect all privacy incidents?	Pct%
Very confident	12%
Confident	33%
Little confidence	30%
No confidence	25%
Total	100%

Q19. Has your department suffered a data breach involving the loss or theft of patient data in the past two years as defined above?	Freq	Pct%
No	3	4%
Yes, 1 incident	12	17%
Yes, 2 to 5 incidents	24	33%
Yes, more than 5 incidents	33	46%
Total	72	100%
Extrapolated average number of data breaches for the benchmark sample	4.08	
Extrapolated total number of data breaches for the benchmark sample	294	

Q20. How confident are you that your organization has the ability to detect all patient data loss or theft?	Pct%
Very confident	12%
Confident	31%
Little confidence	33%
No confidence	24%
Total	100%

Q21. Two separate data breach incidents over the past two years.	Freq
Number of incidents reported	294
Number of incidents included in the analysis for Q21	138

21a. Approximate number of compromised records	Freq	Pct%
10 – 100	58	42%
101 - 1,000	35	25%
1,000 - 5,000	26	19%
5,001 - 10,000	16	12%
10,001 – 100,000	3	2%
Over 100,000	0	0%
Total	138	100%
Extrapolated average number of lost or stolen records per breach	2,575	

Q21b. Time it took to notify	Freq	Pct%
< 1 week	3	2%
1 to 2 weeks	6	4%
2 to 4 weeks	15	11%
1 to 2 months	84	61%
> 2 months	30	22%
Total	138	100%
Extrapolated average time to notify data breach victims (weeks)	6.9	

21c. Nature of the incident	Freq*	Pct%
Unintentional employee action	56	41%
Lost or stolen computing device	67	49%
Third-party snafu	63	46%
Technical systems glitch	45	33%
Criminal attack	41	30%
Malicious insider	19	14%
Intentional non-malicious employee action	12	9%
Total	303	220%
*More than one selection is permitted		

21d. Type of device lost or stolen	Freq	Pct%
A data-bearing device was not lost or stolen	71	
Desktop or laptop	29	43%
Smartphone	14	21%
Tablet	5	7%
Netbook	3	4%
Server	5	7%
USB drive	11	16%
Total	67	100%

21e. Type of patient data lost or stolen	Freq	Pct%
Medical file	65	47%
Billing and insurance record	68	49%
Scheduling details	35	25%
Prescription details	26	19%
Payment details	23	17%
Monthly statements	28	20%
Other	4	3%
Total	249	180%
*More than one selection is permitted		

21f. How the data breach was discovered	Freq*	Pct%
Employee detected	71	51%
Audit/assessment	60	43%
Patient complaint	48	35%
Accidental	39	28%
Legal complaint	27	20%
Loss prevention	19	14%
Law enforcement	9	7%
Total	273	198%
*More than one selection is permitted		

21g. Offer of protection services	Freq	Pct%
None offered	90	65%
Credit monitoring	26	19%
Other identity monitoring	8	6%
Insurance	2	1%
Identity restoration	12	9%
Other	0	0%
Total	138	100%
*More than one selection is permitted		

Q22. In your opinion, what best describes the negative impact of data breach incidents experienced by your organization over the past two years? Please check all that apply.	Pct%
Brand or reputation diminishment	78%
Time and productivity loss	81%
Loss of patient goodwill	75%
Loss of revenues	41%
Cost of outside consultants and lawyers	40%
Fines and penalties paid to regulators	26%
Lawsuits	19%
Poor employee morale	15%
No impact	16%
Other (please describe)	3%
Total	394%

Q23a. Based on your past data breach experience, do you believe it is important to notify individuals affected by the breach as soon as possible?	Pct%
Yes	83%
No	17%
Total	100%

Q23b. If yes, why do you believe it is important to notify quickly. Please select the top two reasons.	Pct%
To maintain patient loyalty and satisfaction	56%
To avoid regulatory fines and penalties	38%
To avoid class action lawsuits	8%
To avoid negative media publicly and news reports	23%
To avoid pressure from internal stakeholders and board of directors	18%
To maintain reputation	55%
Other	198%

Q24. In the event of a future breach, what actions would you take to minimize the negative impact? Please check all that apply.	Pct%
Notify breach victims more quickly	34%
Offer identity monitoring services (credit monitoring)	35%
Hire a service provider specializing in managing and resolving data breach incidents	41%
Hire a media or public relations firm	19%
Have more internal resources available	50%
Have a larger budget available	46%
Total	225%

Q25. In your opinion (best guess), what best describes the lifetime economic value, on average, of one patient or customer to your organization?	Pct%
Less than $10,000	10%
$10,001 to $50,000	31%
$50,001 to $100,000	23%
$100,001 to $200,000	10%
$200,001 to $500,000	4%
$500,001 to $1 million	3%
More than $1 million	3%
Cannot determine	16%
Total	100%
Average lifetime value of one lost patient (customer)	$113,400

Q26. In your opinion (best guess), what best describes the economic impact of data breach incidents experience by your organization over the past two years?	Pct%
Less than $10,000	5%
$10,001 to $50,000	2%
$50,001 to $100,000	3%
$100,001 to $200,000	8%
$200,001 to $500,000	26%
$500,001 to $1 million	21%
$1 million to 10 million	22%
More than $10 million	8%
Cannot determine	5%
Total	100%
Average economic impact of data breach over the past two years	$2,243,700

Q27. In your opinion (best guess), how much has your organization spent on legal fees to resolve data breaches over the past year?	Pct%
Less than $10,000	6%
$10,001 to $50,000	10%
$50,001 to $100,000	15%
$100,001 to $200,000	18%
$200,001 to $500,000	23%
$500,001 to $1 million	13%
More than $1 million	3%
Cannot determine	12%
Total	100%
Average legal fees spent to resolve data breaches over the past year	$249,290

	Five-point scale	
Q28. Please rate each statement about your organization's budget using the scale provided to the right of each attribute.	Strongly agree	Agree
My organization's security budget is sufficient to accomplish its mission and objectives.	13%	20%
My organization's security budget is sufficient to ensure our IT systems are not attacked or disrupted by attackers.	8%	19%
My organization's security budget is sufficient to achieve compliance with HIPAA and other regulatory requirements.	21%	32%
My organization's security budget ensures expenditures are made efficiently (i.e., costs are not squandered).	22%	26%
My organization's security budget is sufficient to curtail or minimize data breach incidents.	8%	14%
My organization's security budget is sufficient to ensure policies are strictly enforced throughout the enterprise.	14%	22%
Average	14%	22%

Q29a. Has your organization implemented an electronic health records (EHR) system?	Pct%
Yes, fully implemented	30%
Yes, implementation is in process	36%
No, but we have plans to implement in the near future	22%
No, and we do not have plans to implement at this time	12%
Total	100%

Q29b, If your organization has implemented an EHR system, what impact do you think it has had on privacy and security of patient data?	Pct%
EHR has made patient data more secure	67%
EHR has made patient data less secure	9%
EHR has made no difference in the security of patient data	19%
Unsure	5%
Total	100%

Q30a. Does your organization use mobile devices that may collect, store and/or transmit PHI?	Pct%
Yes	81%
No	19%
Total	100%

Q30b. If yes, does your organization use any of the following security solutions or procedures to safeguard patient data? Please check all that apply.	Pct%
Encryption solutions installed	23%
Passwords or keypad locks	21%
Anti-virus products installed	25%
Policies governing the proper use of mobile devices that collect, store and/or transmit PHI	46%
Other	12%
We don't do anything to protect these mobile devices	49%
Total	176%

Q30c. If yes, what is your level of confidence as to the security of patient data that may be accessed via mobile devices?	Pct%
Very confident	15%
Somewhat confident	23%
Somewhat concerned	26%
Very concerned	36%
Total	100%

Q31a. Do employees in your organization use social media from their desktop, laptop or other devices?	Pct%
Yes	63%
No	30%
Unsure	7%
Total	100%

Q31b. If yes, does your organization have a policy for employees about the appropriate use of social media?	Pct%
Yes	38%
No	45%
We are writing a policy about the use of social media in the workplace	12%
Unsure	5%
Total	100%

Part 4: Security Environment	Four-point scale	
Q32. The following table lists attributes that describes information security environment for most healthcare organizations. Please assess the effectiveness of your company's security and data protection efforts using the scale provided to the right of each attribute. The scale requires you to rate each item based on your level of confidence that your organization presently accomplishes the stated attribute.	Very confident	Confident
Identify major data breaches involving patient information	21%	23%
Determine the root causes of major data breaches involving patient information	20%	23%
Know where patient information is physically located	14%	25%
Secure patient data at rest	18%	29%
Secure patient data in motion	16%	34%
Secure endpoints to the network	15%	28%
Identify system end-users before granting access rights to patient information	15%	27%
Protect patient information used by outsourcers including cloud computing vendors	15%	25%
Protect patient information used by business associates	11%	20%
Have standard agreements with business associates that clearly explain the requirements for data protection	31%	25%
Prevent or curtail major data breaches involving patient information	13%	16%
Prevent or curtail cyber attacks that attempt to acquire patient information	15%	18%
Limit physical access to data storage devices containing patient information	11%	11%
Demonstrate the economic value or other tangible benefits of the company's security program	5%	11%
Ensure minimal downtime or disruptions to systems resulting from security problems	36%	30%
Comply with legal requirements and policies including privacy laws and statutes (i.e., HIPAA)	33%	54%

Conform with leading self-regulatory requirements such as ISO, NIST and others	20%	34%
Prevent or curtail viruses and malware infections	15%	38%
Perform timely updates for all major security patches	15%	42%
Control all live data used in systems development activities	19%	19%
Enforce corporate policies, including the termination of employees or contractors who pose a serious insider threat	29%	35%
Attract and retain high quality IT security personnel	21%	30%
Training and awareness program for all system users	38%	35%
Conduct independent audits of the system	16%	20%
Security program administration is consistently managed	24%	26%
Prevent or curtail cyber attacks	15%	22%
Average	19%	27%

	Five-point scale	
Q33. How important are security technologies for your organization's ability to defend itself against patient data loss or theft. Essential and very important.	Essential	Very important
Rating	38%	34%

Part 5. Data Protection & GRC Practices	
Q34. What best describes the process for preventing and detecting data breach incidents in your organization today? Please select one best choice.	Pct%
An "ad hoc" process	27%
Mostly a process that relies on policies and procedures	29%
Mostly a process that relies on security technologies	21%
A combination of manual procedures and security technologies	19%
None of the above	4%
Total	100%

Q35. Who is most responsible for preventing and detecting data breach incidents in your organization?	Pct%
Information technology department	14%
Information security department	12%
Compliance department	36%
Privacy office	0%
Legal department	4%
Business unit managers	7%
Human resource department	2%
No one person or department	25%
Other	0%
Total	100%

Q36a. Do you have a clear written policy for employees to notify the appropriate authority if they suspect a data breach has occurred?	Pct%
Yes	83%
No	17%
Total	100%

Q36b. If yes, do you think this policy is effective in curtailing or detecting most data breaches?	Pct%
Yes	43%
No	57%
Total	100%

	FY 2011	
Q37. How confident are you that your organization has the ability to prevent or quickly detect patient data loss or theft in your organization? Very confident and confident.	Very confident	Confident
Rating	18%	16%

Q38a. Does your organization conduct and document post data breach incident risk assessments as mandated by the HITECH Act?	Pct%
Yes	61%
No	21%
Unsure	18%
Total	100%

Q38b. If yes, which one of the following choices best describes your process?	Pct%
An ad-hoc process	33%
A paper-based process or tool that was developed internally	31%
A software-based process or tool that was developed internally	15%
A software-based process or tool that was developed by a third party	21%
Total	100%

Q39. Do you believe HHS-mandated incident risk assessments can be objectively conducted by covered entities in determining the risk of harm to individuals affected by data breaches and for determining whether to notify?	Pct%
Yes	63%
No	37%
Total	100%

Q40. What do you believe are your two most effective measures in preventing a data breach incident within your organization?	Pct%
Training and awareness programs	45%
Enabling security technologies	60%
Policies and procedures	8%
Governance and leadership	21%
Manual controls	15%
Risk assessments	46%
Independent audits	3%
Other	0%
Total	198%

Q41. What do you believe are your two greatest weaknesses to preventing a data breach?	Pct%
Lack of trained staff and end users	43%
Inadequate budget for security and privacy	54%
Lack of enabling technologies	19%
Lack of manual controls	6%
Lack of governance and leadership	18%
Insufficient assessments for risk	45%
Lack of policies and procedures	11%
Other	0%
Total	196%

Q42. In your opinion, what harms do patients actually suffer if their records are lost or stolen?	Pct%
Increased risk of financial identity theft	59%
Increased risk of medical identity theft	51%
Increased risk that personal health facts will be disclosed	73%
None	10%
Total	193%

Q43. If you organization has experienced a data breach, has the breach led to any cases of identity theft (financial or medical) among the affected population?	Pct%
Yes	29%
No	26%
Unsure	45%
Total	100%

Q44. What type of data is most susceptible to data loss or theft within your department?	Pct%
Billing information	39%
Medical records	25%
Clinical trial data	0%
Employee records	9%
Non-patient related confidential information	24%
Other	3%
Total	100%

Q45a. Do you believe credit monitoring is effective in preventing or detecting medical identity theft?	Pct%
Yes, credit monitoring is very effective	5%
Yes, credit monitoring is effective	8%
Yes, credit monitoring is somewhat effective	15%
No, credit monitoring is not effective	72%
Unsure	100%

Q45b. 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?	Pct%
Yes	74%
No	11%
Unsure	15%
Total	100%

Q46. Please review the following list of 7 GRC activities that may be performed in your organization today. First, indicate whether the stated activity is presently performed. Then use the following three-point scale to rate each technology in terms of its impact on data breach prevention. 1 = significant impact, 2 = moderate impact, 3 = little or no impact.	Pct% activity is deployed	Points assigned
Incident response plans	79%	1.22
Training of patient or customer data handlers	73%	1.54
Annual (periodic) risk assessments	56%	1.66
Training of end users	67%	2.00
Vetting & monitoring of third parties including business associates	50%	2.23
Certification of security staff	62%	2.45
Business continuity plans	81%	2.56

Please contact research@ponemon.org or call us at 800.877.3118 if you have any questions.

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.