



Benchmark Study on Patient Privacy and Data Security

Sponsored by ID Experts

Independently conducted by Ponemon Institute LLC

Publication Date: November 9, 2010

Benchmark Study on Patient Privacy and Data Security

Ponemon Institute, November 9, 2010

Part 1. Executive summary

The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 requires healthcare providers to provide stronger safeguards for patient data and to notify patients when their information has been breached. In light of these new regulations, this study was created to understand healthcare providers' patient privacy practices and their experience in dealing with the loss or theft of patient information.

The study also examines each healthcare organization's privacy and data protection compliance activities, including policies, program management activities, enabling security technologies and security governance practices in addition to their ability to comply with the notification requirements mandated by HITECH.

We utilized in-depth field-based research involving interviews with senior-level personnel at healthcare providers to collect data on the actual data loss and data theft experiences at their organizations. A traditional survey-based approach would not have been able to collect both the qualitative and quantitative data necessary to understand the current status of patient privacy in the healthcare organizations that participated in our study.

A total of 65 healthcare organizations participated in the study. The healthcare organizations participating in the study are integrated delivery systems -- a network of healthcare organizations under a parent holding company (35 percent), part of a healthcare network (46 percent) and standalone hospital or clinic (17 percent). Respondents interviewed work in all areas of the organization: security, administration, privacy, compliance, finance and clinical. On average the number of interviews conducted in each organization was 3.25.

Our study found that data breaches remain a frequent occurrence at healthcare organizations – threatening patient privacy and leaving healthcare organizations with a heavy financial burden.

Key takeaways from this report include:

- **Data breaches are costing the health care system billions.** According to respondents in our study, the economic impact of data breach incidents over a two-year period is approximately \$2 million per organization. These are dollars that could alternatively be used to keep healthcare costs down or improve quality of services as opposed to funding the direct costs and associated financial losses of remediating a data breach incident. Because our study primarily focuses on hospitals, we calculated the total economic burden created by data breaches on US hospitals as almost \$12 billion¹.
- **Most healthcare organizations experience undetected breaches of patient data due to lack of preparation and staffing.** Healthcare organizations in our study told us they have inadequate resources (71 percent), few (if any) appropriately trained personnel (52 percent) and insufficient policies and procedures in place (69 percent) to prevent and quickly detect patient data loss. These realities have left organizations with little or no confidence in their ability to appropriately secure patient records (58 percent).
- **Protecting patient data is not a priority.** Seventy percent of hospitals say that protecting patient data is not a top priority. The majority of responding organizations have less than two

¹Total number of all US registered hospitals is 5,815 from AHA Hospital Statistics, 2010 edition. 5,815 hospitals multiplied by \$2,060,174 (economic impact of data breach over 2 years as estimated by survey respondents) equals \$11,979,911,810.

staff dedicated to data protection management (67 percent). Most at risk is patient billing information and medical records, which is not being protected. In addition, patients are typically first to detect a significant number of breaches at healthcare organizations (41 percent). This finding suggests that patient data is being unknowingly exposed until the patients themselves detect the breach. Healthcare organizations' inability to prevent or detect patient data loss is putting patients at greater risk of medical identity theft, financial identity theft and having their personal health facts disclosed.

- **Federal regulations have not improved the safety of patient records.** The passage of the HITECH Act widened the scope of privacy and security protections under HIPAA to provide stronger safeguards for patient data. Despite the intent of these rules, the majority (71 percent) of respondents do not believe these new federal regulations have significantly changed the management practices of patient records.

Respondents in our study believe the move to electronic health records (EHR) may make patient records more secure. Eighty-nine percent of respondents say their organization has fully implemented, in process of implementation or will implement EHR in the near future. While the move to EHR may solve some of the security issues that healthcare organizations now face, it also creates new concerns for organizations to manage. This massive shift to digitized records makes patient data available to many more individuals within and outside the provider organization and leaves the data more vulnerable to the growing threat of cyber crime.

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.

- Sixty percent of organizations in our study had more than two data breaches in the past two years. The average number for each participating organization was 2.4 data breach incidents.
- The economic impact of a data breach over the past two years is approximately \$2 million.
- The average number of lost or stolen records per breach was 1,769. A significant percentage of organizations either did not notify any patients (38 percent) or notified everyone (34 percent) that their information was lost or stolen.
- The top three causes of a data breach are: unintentional employee action, lost or stolen computing devices and third-party snafu.
- Forty-one percent discovered the data breach as a result of a patient complaint.
- More than half (58 percent) of organizations have little or no confidence that their organization has the ability to detect all patient data loss or theft.
- Sixty-three percent of organizations say it took them between one to six months to resolve the incident.
- Fifty-six percent of respondents have either fully implemented or are in the process of implementing an electronic health records (EHR) system. The majority (74 percent) of those who have an EHR system say it has made patient data more secure.
- Cross-tabulation analysis reveals healthcare organizations that have a strong security posture are less likely to experience a larger-sized data breach incident.

Part 2. Key findings

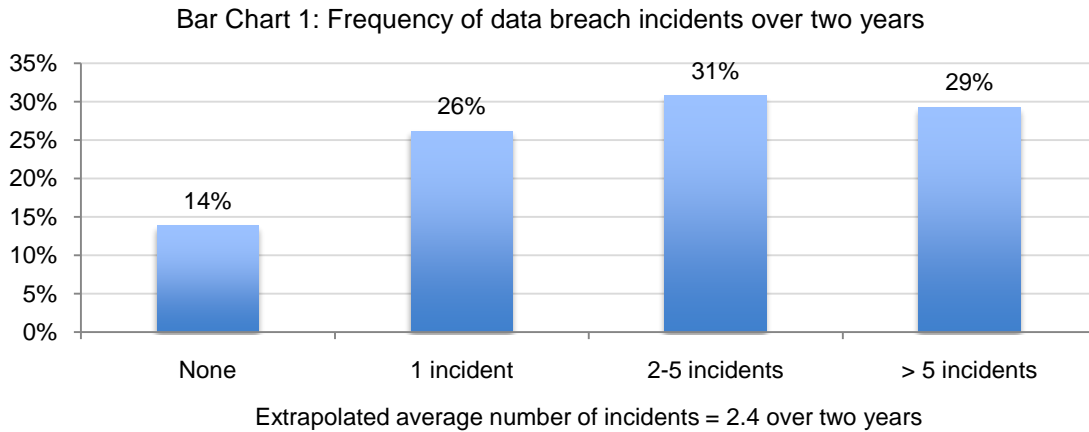
In this report, we have organized the most salient research results according to the following issues:

- The loss or theft of patient information experienced by healthcare providers in our study
- Healthcare organizations' ability to detect and prevent the loss or theft of patient information
- The impact of data breaches on providers and patients
- Providers' perceptions about their privacy and security environment

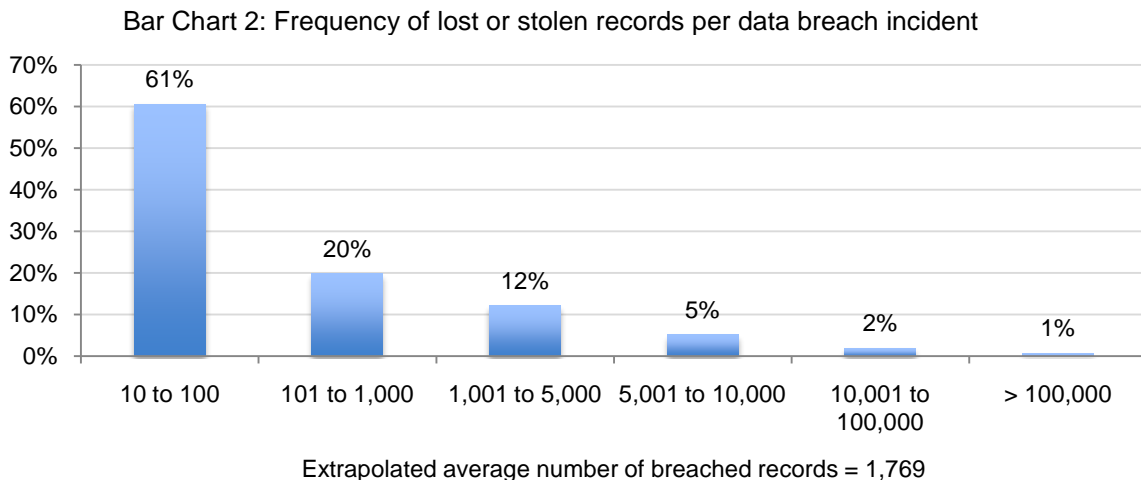
In this section, we provide the most important findings of our benchmark study. Graphs and tables are provided to illustrate the results. As shown above, we have organized the findings according to four major themes.

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

Bar Chart 1 shows 29 percent of respondents say their organizations have had more than five data breaches in the past two years and the average number of data breach incidents for participants in this study was 2.4 over the past two years.

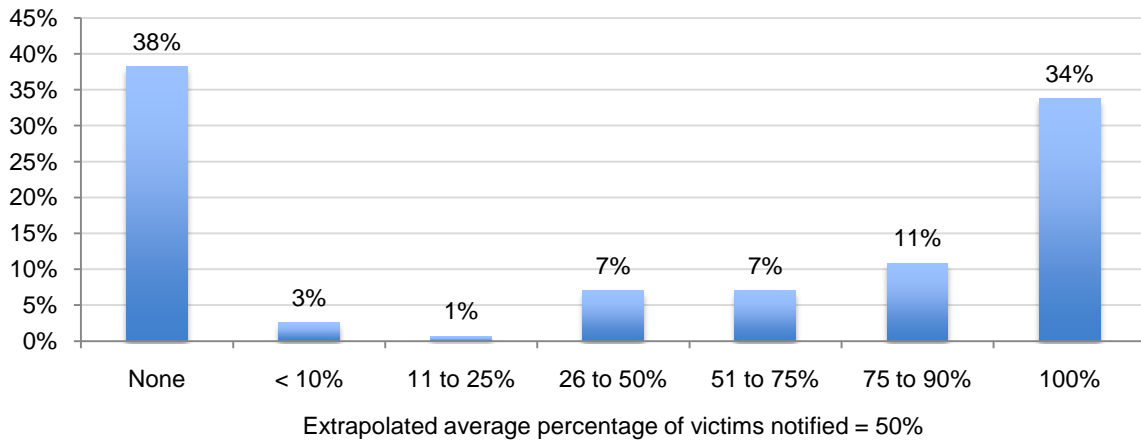


As can be seen in Bar Chart 2, the bulk of data breach incidents (61 percent) involve fewer than 100 records. The extrapolated average number of records for our benchmark sample is 1,769.



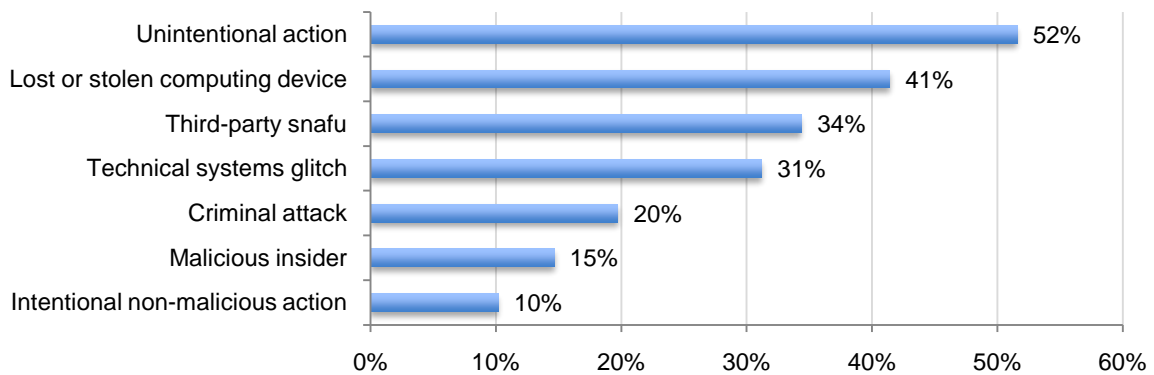
Notification procedures seem to be inconsistent among respondents' organizations. While 38 percent say no patients were notified of the breach, 34 percent say everyone was notified.

Bar Chart 3: Approximate percentage of patients notified about data loss or theft



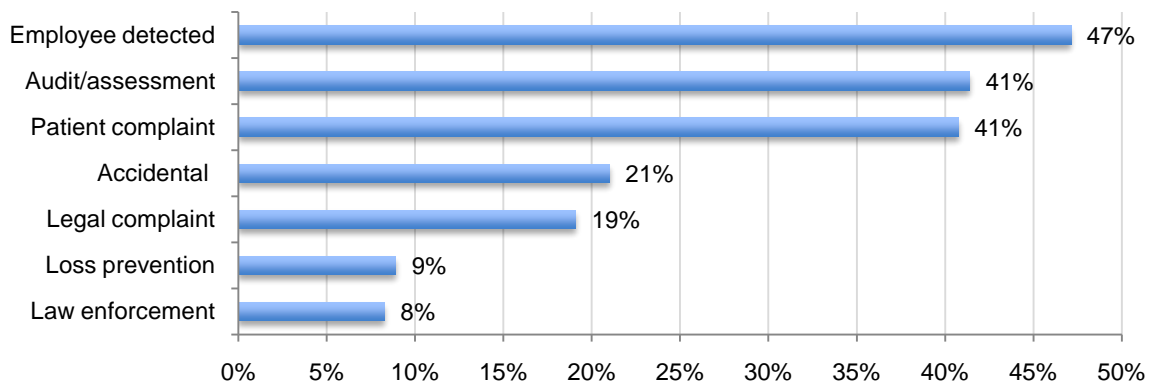
According to Bar Chart 4, the primary causes of data loss or theft were unintentional employee action (52 percent), lost or stolen computing device (41 percent) and third-party snafu (34 percent).

Bar Chart 4: The nature or root causes of patient data loss or theft



As shown in Bar Chart 5, employee (47 percent), audit/assessment (41 percent) or as a result of patient complaints (41 percent) were the primary ways the breach was discovered.

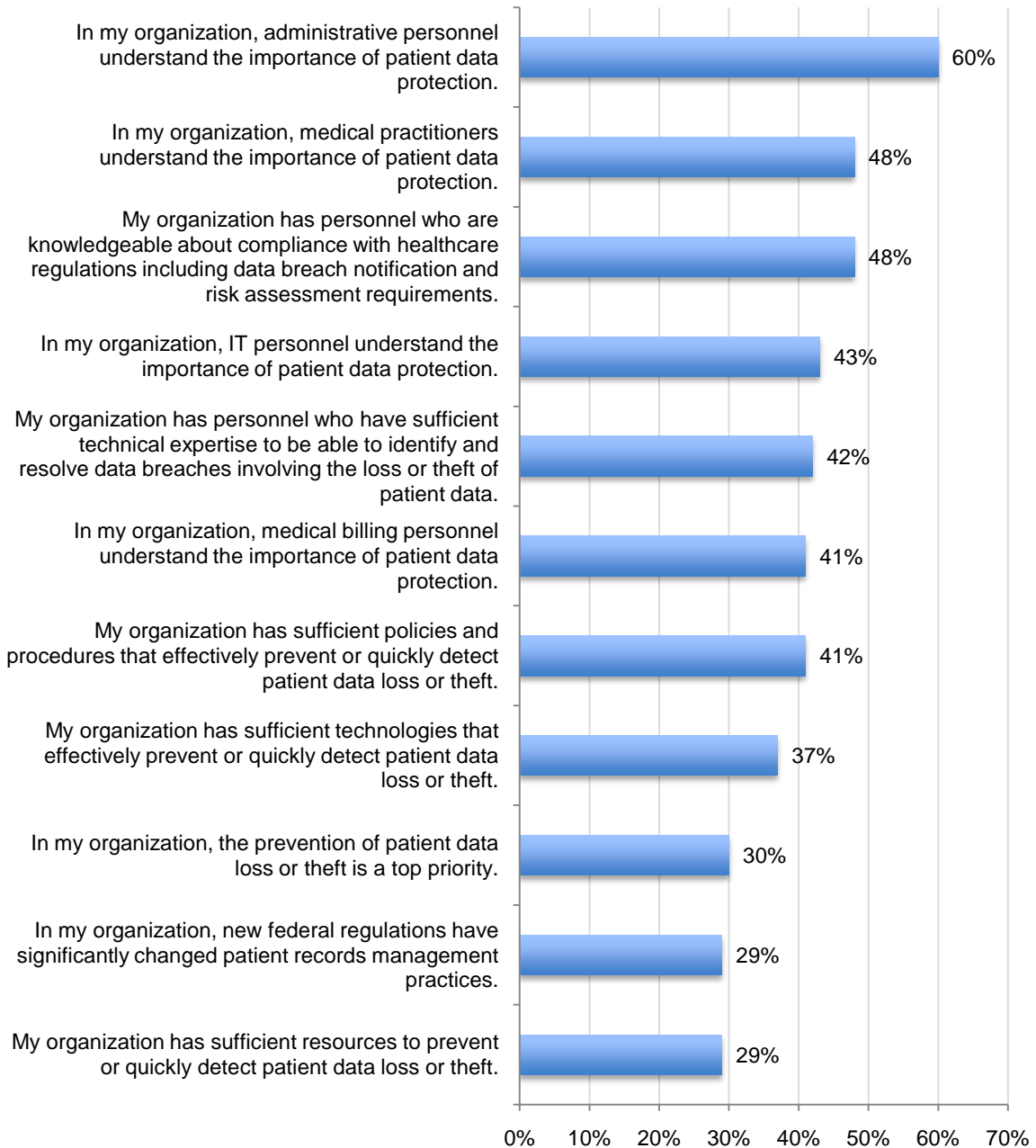
Bar Chart 5: How the data breach incident was discovered



Participating healthcare organization’s ability to detect and prevent the loss or theft of patient information

Bar Chart 6 summarizes how respondents view 11 key attributions about privacy and data protection practices within their healthcare organizations. As shown below, many respondents believe administrative personnel understand the importance of patient data protection better than medical practitioners. Sixty percent strongly agree and agree that administrative personnel in their organizations understand the importance of patient data protection versus less than half (48 percent) of medical practitioners.

Bar Chart 6: Respondents’ response to attributions about privacy and data protection
Strongly agree and agree response combined

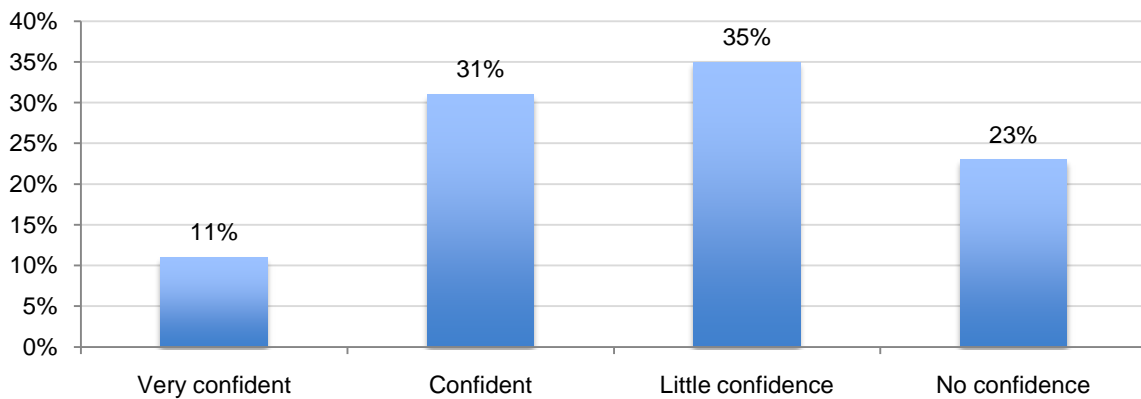


Less than half (48 percent) strongly agree or agree that they have personnel who are knowledgeable about compliance with healthcare regulations, including data breach notification and risk assessment requirements, as shown in Bar Chart 6. Seventy-one percent do not believe new federal regulations have significantly changed patient records management practices.

Further, the majority of organizations in the study do not believe they have sufficient policies and procedures in place to effectively prevent or quickly detect patient data loss or theft (69 percent). Seventy-one percent do not believe they have sufficient resources to prevent or quickly detect patient data loss or theft.

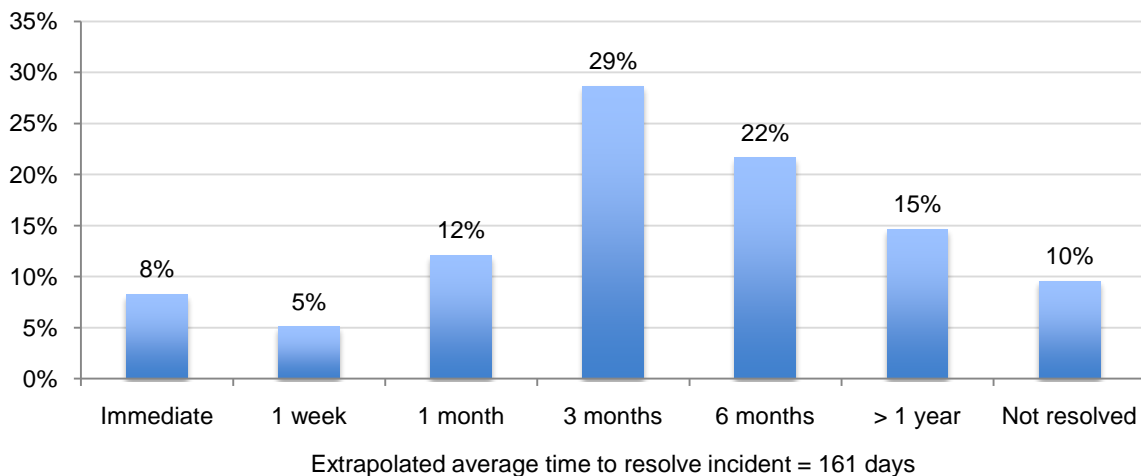
As noted in Bar Chart 7, many respondents say they have little (35 percent) or no (23 percent) confidence that their organization has the ability to detect all patient data loss or theft. Only 11 percent say they are very confident.

Bar Chart 7: Level of confidence in the organization's ability to detect all patient data loss or theft



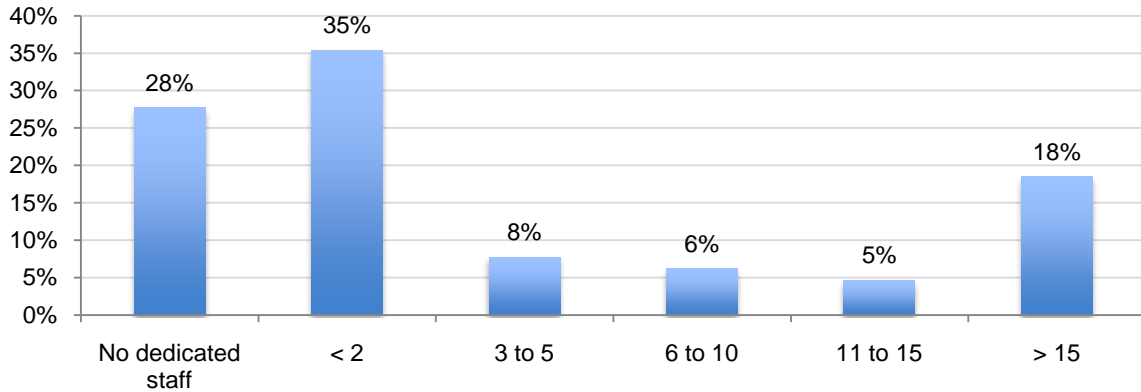
Bar Chart 8 shows that only 13 percent (8 + 5 percent) of respondents say their ability to resolve the data breach incident was immediate or within one week. In contrast, 37 percent (22 + 15 percent) respondents say it took them six months or longer to resolve the incident.

Bar Chart 8: Approximate length of time to resolve data breach incidents



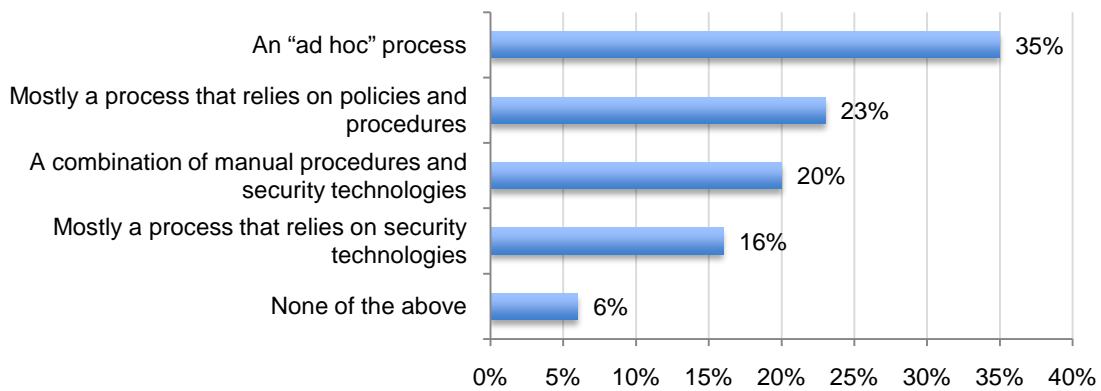
Bar Chart 9 shows 28 percent of respondents say they have no staff dedicated to manage data protection activities. Thirty-five percent say they have less than two dedicated staff members.

Bar Chart 9: Level of dedicated staffing to manage data protection efforts



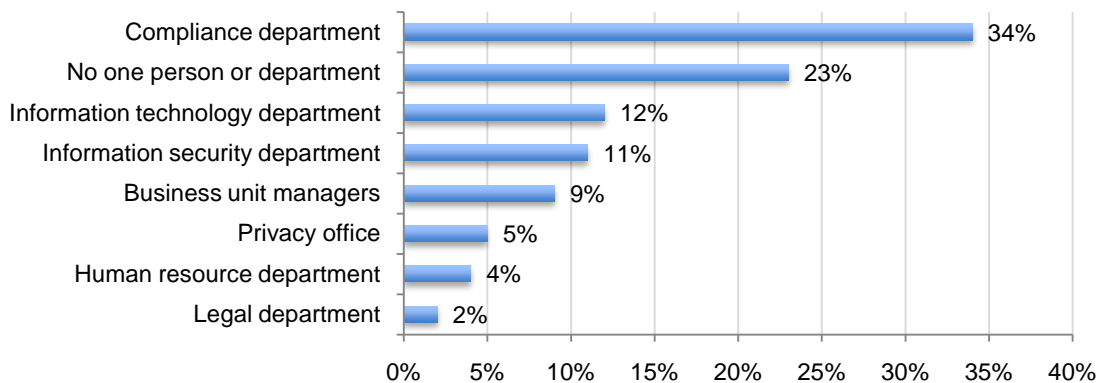
Bar Chart 10 reports that the process for preventing and detecting data breach incidents is “ad hoc,” according to 35 percent of respondents. Only 16 percent say it is a process that relies on security technologies and 23 percent say it relies on policies and procedures.

Bar Chart 10: What best describes the process for preventing and detecting data breach?



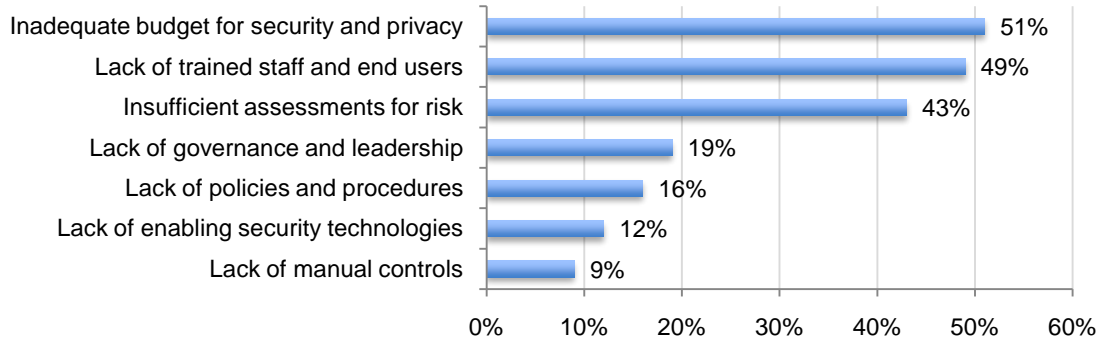
There is no clear responsibility for the prevention and detection of data breach incidents in their organization. While 34 percent say it is compliance, only 12 percent say it is IT and 11 percent say it is IT security. Twenty-three percent say it is no one person or department.

Bar Chart 11: Who is most responsible for preventing and detecting data breach incidents



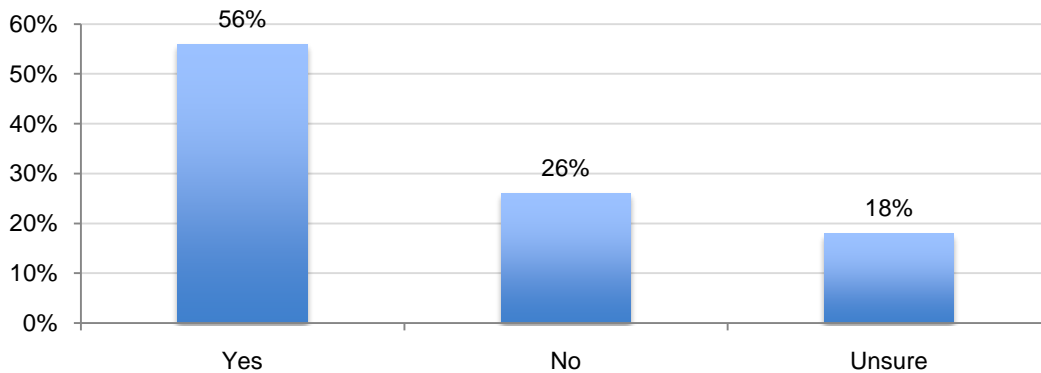
As noted in Bar Chart 12, more than half (51 percent) say it is an inadequate budget for security and privacy followed by lack of trained staff and end users (49 percent) as the biggest areas of vulnerability for a data breach to occur.

Bar Chart 12: Most likely reasons for data breach
 Respondents select their top two reasons



Bar Chart 13 shows 56 percent say they need help to assess their risks and procedures to make sure they are compliant. Only 26 percent say they do not need help and 18 percent are unsure.

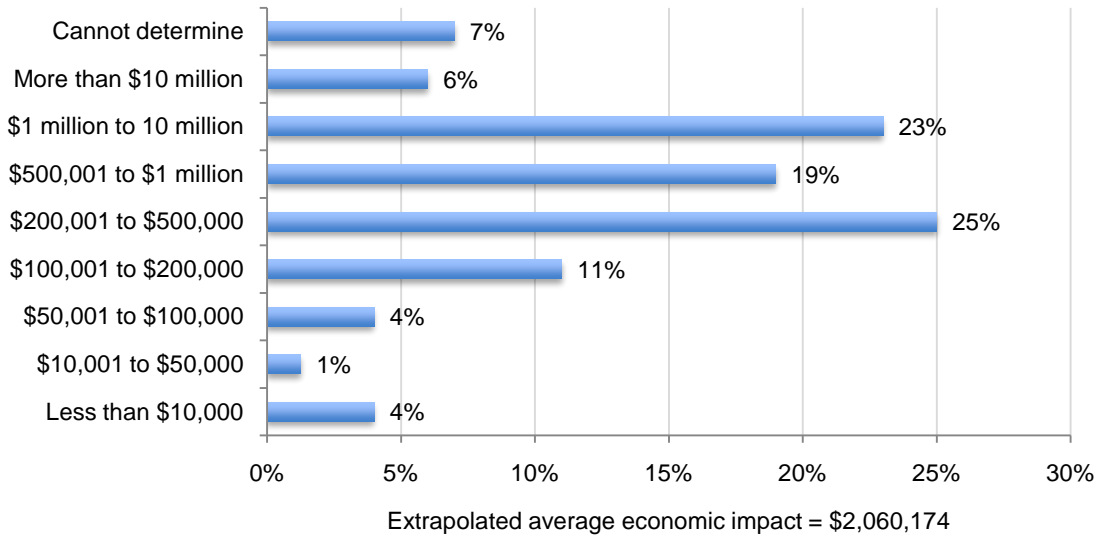
Bar Chart 13: Do you need help to make sure that you are in compliance?



The impact of data breaches on providers and patients

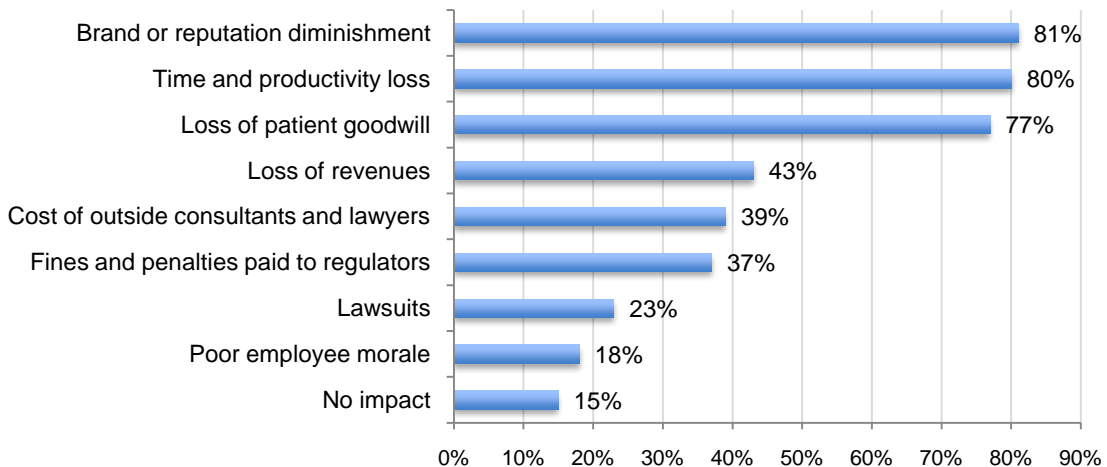
Bar Chart 14 reports the estimated cost or total economic impact of data breach over the past two years for benchmarked companies. As shown, 23 percent of respondents say it cost their healthcare organization between \$1 and \$10 million. The extrapolated average economic impact is over \$2 million.

Bar Chart 14: The estimated economic impact of data breach incidents over the past two years



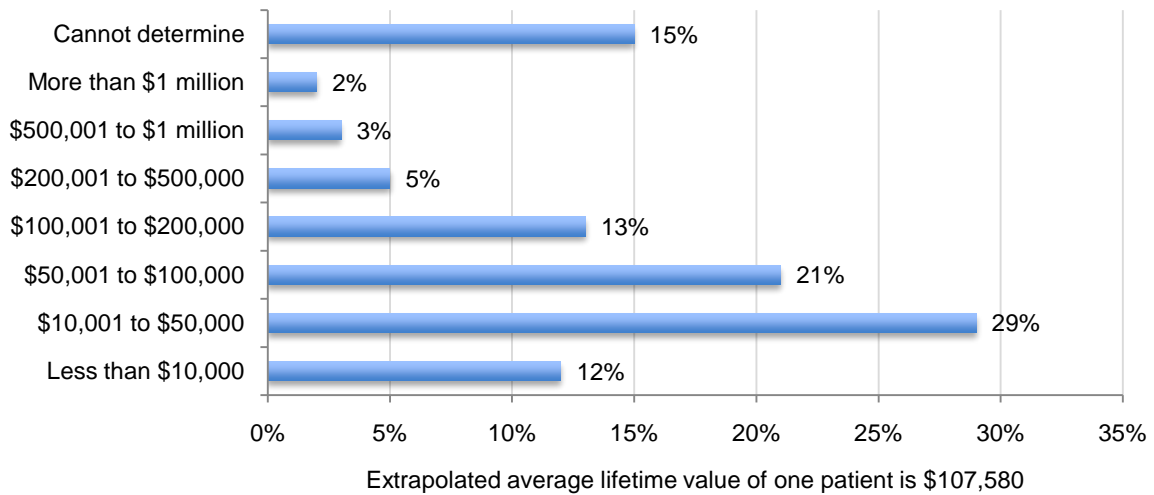
As shown in Bar Chart 15, very few respondents (15 percent) believe the breach had no negative impact on their organizations. Most respondents believe they have suffered brand or reputation diminishment (81 percent) followed by time and productivity loss (80 percent) and loss of patient goodwill (77 percent). The least negative results are lawsuits (23 percent) and poor employee morale (18 percent).

Bar Chart 15: The negative impact of data breach incidents



As mentioned above, the most negative result 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 Bar Chart 16, 29 percent of respondents see the lifetime value between 10,001 to \$50,000. The extrapolated average lifetime value of one lost patient (customer) is \$107,580.

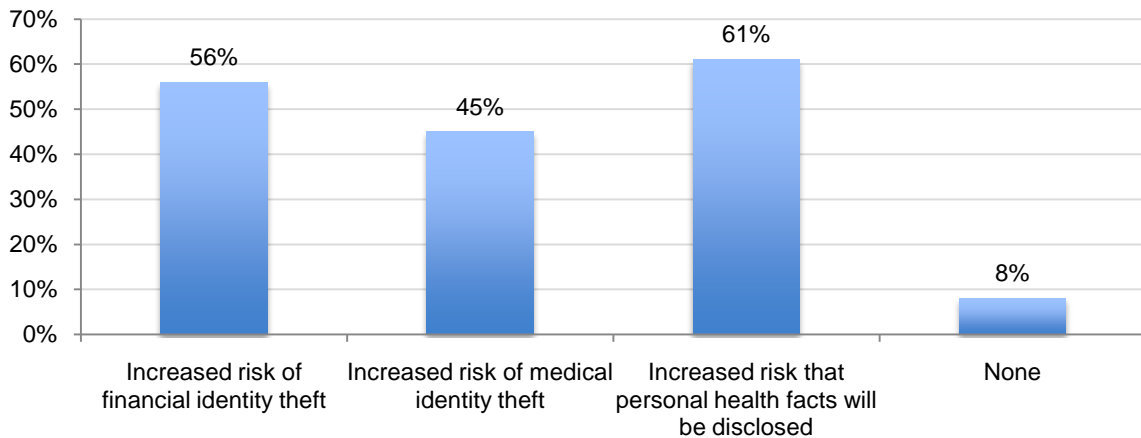
Bar Chart 16: Estimate of the lifetime value of one patient for participating organizations



Ponemon Institute's *2009 Annual Study: Cost of a Data Breach* calculates the abnormal customer/patient churn rate for the healthcare industry as six percent. When this churn rate is applied to the average number of data breach incidents experienced by survey participants over two years (2.4), the average number of lost or stolen records per breach (1,769) and percent that were fully notified (34 percent), the result is 87 patients lost to churn. The loss of 87 patients implies that organizations lose over \$9 million to patient churn just from data breach incidents experienced over a two-year period.²

Bar Chart 17 shows 61 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 (56 percent) and increased risk of medical identity theft (45 percent). Only eight percent say patients suffer no harms. A significant number of respondents (41 percent) are unsure whether or not the breach led to any cases of identity theft (financial or medical).

Bar Chart 17: Harms patients actually suffer as a result of data loss or theft

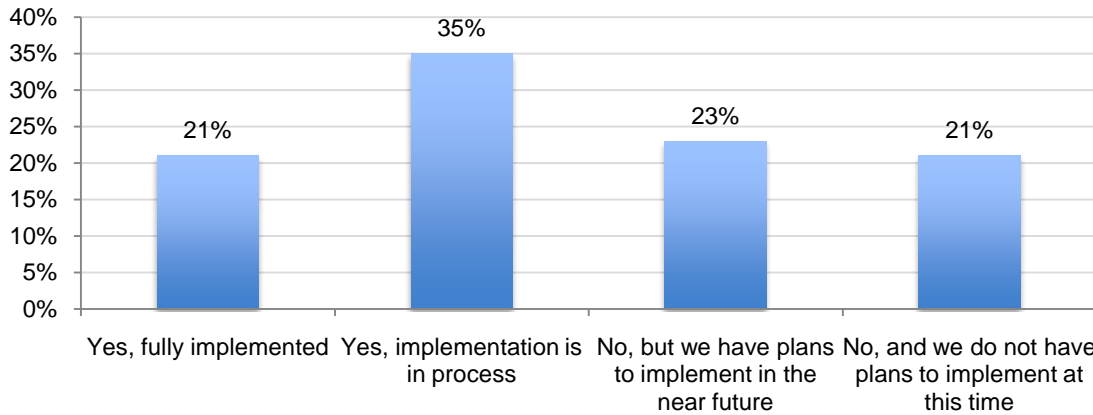


²87 patients multiplied by, the average lifetime value of one lost patient, \$107,580 equals \$9,317,530.

Providers' perceptions about their organizations' privacy and security environment

Bar Chart 18 shows 56 percent (21 and 35 percent) of respondents have either fully implemented or are in the process of implementing an electronic health records (EHR) system. Only 21 percent have no plans to do so at this time.

Bar Chart 18: Has your organization implemented electronic health records (EHR) systems?



Bar Chart 19 shows that the overwhelming majority (74 percent) of those who have implemented an EHR system say it has made patient data more secure.

Bar Chart 19: What impact do you think it has had on privacy and security of patient data?

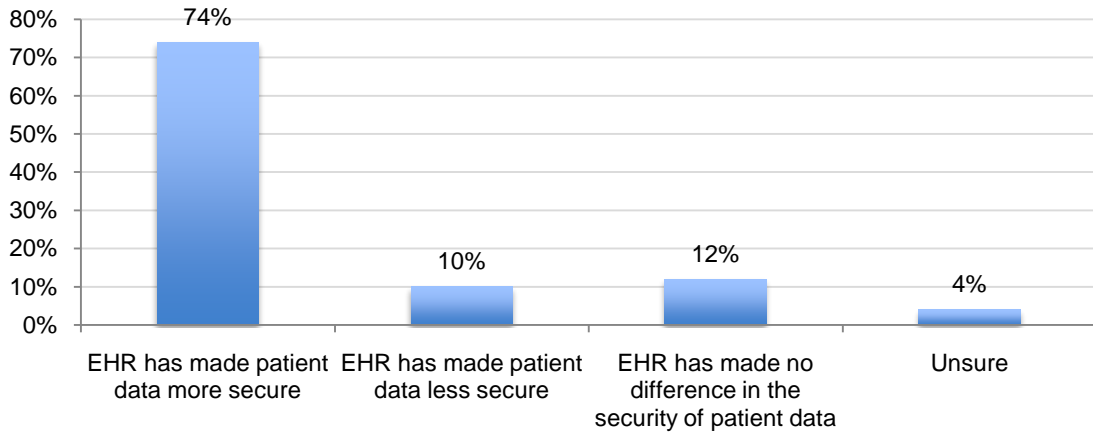


Table 1 provides 26 attributes that describe the information security environment within most companies. The percentage next to each attribute represents the confidence rating that each attribute is presently accomplished. Only the average very confident and confident response are reported.

The pattern of results suggests respondents are not very confident about their organization's security environment. They appear to be most confident about standard agreements with business associates that clearly explain the requirements for data protection, training and awareness program for all system users and compliance with legal requirements and policies, including privacy laws and statutes.

While 85 percent believe they comply with the legal requirements of HIPAA, only 10 percent are confident that they are able to protect patient information when used by outsourcers and cloud computing providers. Only 23 percent of respondents believe they can curtail physical access to data storage devices and servers.

Table 1: Attributes that describe the information security environment in healthcare organizations in descending order of confidence.	Very confident & Confident response*
Comply with legal requirements and policies including privacy laws and statutes (i.e., HIPAA)	85%
Enforce corporate policies, including the termination of employees or contractors who pose a serious insider threat	72%
Training and awareness program for all system users	71%
Have standard agreements with business associates that clearly explain the requirements for data protection	66%
Ensure minimal downtime or disruptions to systems resulting from security problems	65%
Conform with leading self-regulatory requirements such as ISO, NIST, HITRUST and others	61%
Prevent or curtail viruses and malware infections	56%
Attract and retain high quality IT security personnel	55%
Perform timely updates for all major security patches	53%
Security program administration is consistently managed	52%
Secure endpoints to the network	51%
Secure patient data in motion	47%
Know where patient information is physically located	47%
Identify system end-users before granting access rights to patient information	45%
Conduct independent audits of the system	45%
Secure patient data at rest	42%
Control all live data used in systems development activities	39%
Prevent or curtail cyber attacks	39%
Prevent or curtail cyber attacks that attempt to acquire patient information	37%
Identify major data breaches involving patient information	32%
Prevent or curtail major data breaches involving patient information	31%
Determine the root causes of major data breaches involving patient information	30%
Protect patient information used by business associates	29%
Limit physical access to data storage devices containing patient information	23%
Demonstrate the economic value or other tangible benefits of the company's security program	17%
Protect patient information used by outsourcers including cloud computing vendors	10%

*Four-point scale from very confident to not confident.

Table 2 lists 20 enabling security technologies that may be deployed by participating healthcare organizations to secure and protect information assets. Each cell of this table provides the average frequency for all respondents ranging from 0 to 100. An average value near 100 points suggests the given technology has a significant impact on data breach prevent or compliance with HIPAA, and an average value near 0 implies the opposite.

As reported, firewalls are the top choice for both data breach prevention and compliance with HIPAA. Also popular for accomplishing both are access governance systems and privileged user management. Respondents favor anti-virus and anti-malware for data breach prevention and for compliance with HIPAA they favor encryption for data at rest.

While the average values for data breach prevention and compliance with HIPAA are close, there are some significant differences between these categories. For instance, ID and credentialing systems appears to be more important for compliance than data breach prevention. In contrast, intrusion prevention systems are more important for breach prevention than compliance.

Table 2: Enabling security technologies and their impact on breach prevention and compliance with HIPAA	Data breach prevention	Compliance with HIPAA
Firewalls	83	78
Access governance systems	73	73
Encryption for data at rest	60	72
Privileged user management	75	72
Data loss prevention (DLP)	48	69
Database scanning and monitoring	65	67
Anti-virus & anti-malware	70	65
Encryption for data in motion	65	57
Virtual private network (VPN)	64	56
Log management	65	55
Web application firewalls (WAF)	45	49
Endpoint security solutions	56	47
Security intelligence & event manager (SIEM)	35	43
ID & credentialing systems	16	40
Code review tools	31	33
Intrusion detection systems	35	33
Network intelligence systems	25	27
Perimeter or location surveillance	39	27
Intrusion prevention systems	32	18
Service oriented architecture (SOA)	19	9
Average	50.05	49.5
Scale: 0 = No impact to 100 = Maximum impact		

Table 3 lists 19 manual control practices that may be deployed by participating healthcare organizations to secure and protect information assets. Similar to the above table, each cell of this table provides the average frequency for all respondents ranging from 0 to 100. An average value near 100 points suggests the given control area has a significant impact on data breach prevent or compliance with HIPAA, and an average value near 0 has an opposite meaning.

Respondents appear to favor the following controls and governance for both data breach prevention and compliance with HIPAA: control self-assessment, training of patient or customer data handlers and training of end users. Respondents also favor annual (periodic) risk assessments and upstream communications for compliance with HIPAA. They favor vetting and monitoring of third parties, including business associates for data breach prevention.

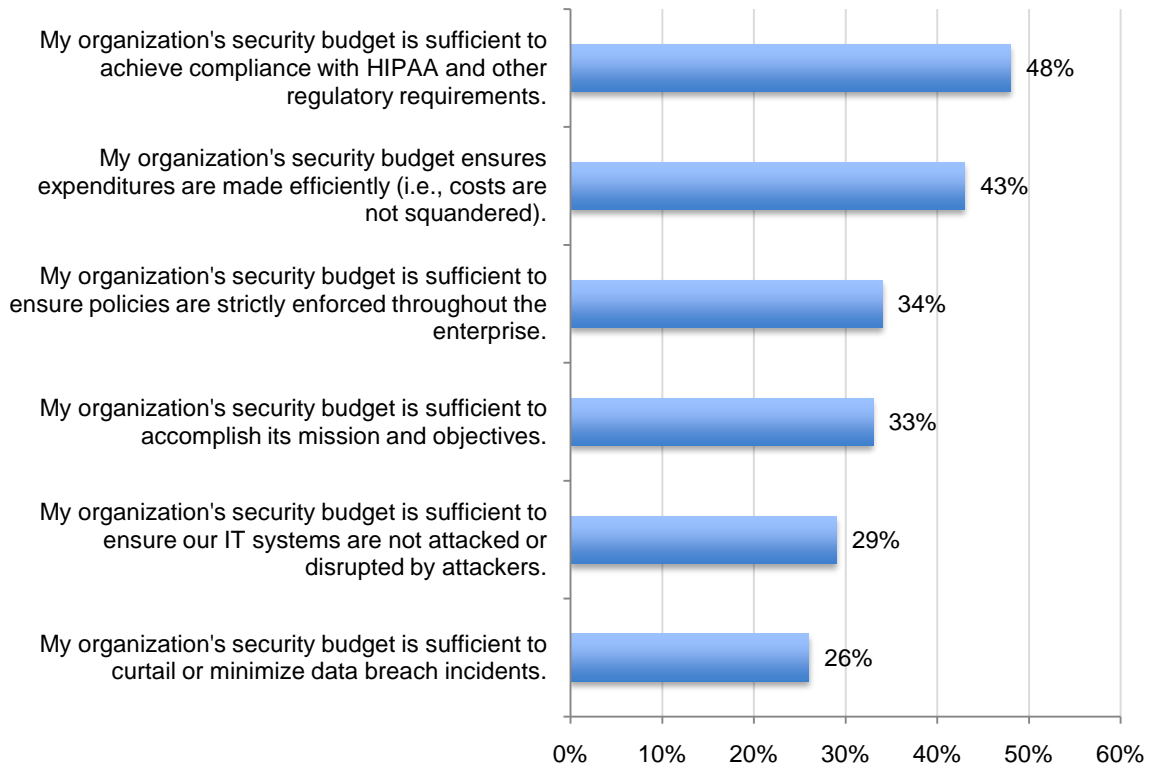
Table 3: Manual control practices and their impact on breach prevention and compliance with HIPAA	Data breach prevention	Compliance with HIPAA
Training of patient or customer data handlers	90	89
Control self-assessment	89	90
Vetting & monitoring of third parties including business associates	89	88
Training of end users	82	84
Incident response plans	69	66
Annual (periodic) risk assessments	65	89
Record retention & archive management	65	61
Business continuity plans	61	56
External audits	57	40
Redress & enforcement	56	56
Workplace surveillance	56	77
Certification of security staff	54	65
Disposal of paper documents	49	43
Background checks of privileged users	45	55
Disposal of electronic data-bearing devices	24	23
Helpdesk activities	17	14
Monitoring regulatory change	16	66
Upstream communications	16	43
Quality assurance	2	12
Average	53	59
Scale: 0 = No impact to 100 = Maximum impact		

Table 4 lists 11 governance practices that may be deployed by participating healthcare organizations to secure and protect information assets. Direct budgetary authority for data protection, appointment of a data protection executive and upstream data breach incident reporting channel to chief executive are the most popular data governance practices for both data breach prevention and compliance with HIPAA.

Table 4: Information security governance practices and their impact on breach prevention and compliance with HIPAA	Data breach prevention	Compliance with HIPAA
Appointment of a data protection executive	79	76
Board involvement in data protection efforts	22	19
Board understanding of data protection risks	64	61
Direct budgetary authority for data protection	83	82
Community outreach on patient privacy issues	15	16
Cross-functional steering committee	24	25
Metrics or measures used to define success	17	19
A security department that is officially sanctioned with charter	32	35
Participation in benchmark program (with reference to peer group of healthcare companies)	29	40
Segregation of duties between data protection and IT operations	33	39
Upstream data breach incident reporting channel to the chief executive	78	80
Average	43	45
Scale: 0 = No impact to 100 = Maximum impact		

As shown in Bar Chart 20, only 26 percent strongly agree or agree that their organization's security budget is sufficient to curtail or minimize data breach incidents. However, almost half (48 percent) believe their security budget is sufficient to achieve compliance with HIPAA and other regulatory requirements.

Bar Chart 20: Respondents' response to attributions about the organization's budget
Strongly agree and agree response combined

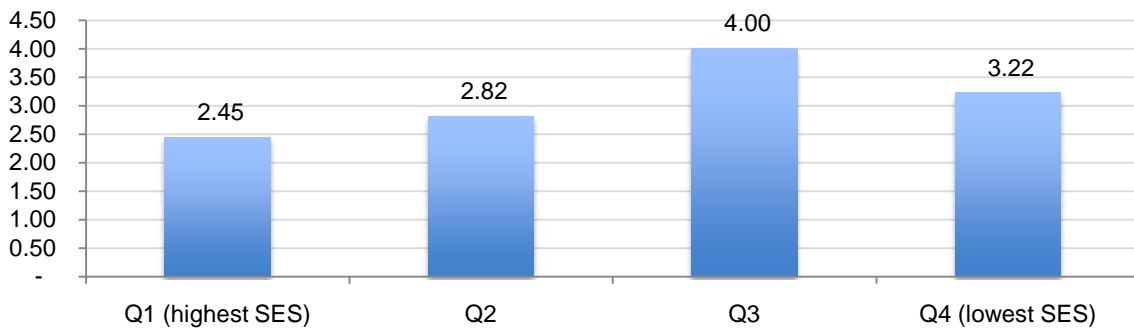


Does a strong security posture impact the frequency and magnitude of data breach?

To answer the above question, we utilize a statistic known as the Security Effectiveness Score (SES), which measures an organization’s ability to meet reasonable security objectives.³ The attributes that describe the information security environment in healthcare organizations are shown in Table 1 on page 12 of this report. The higher the SES score, the more effective the organization is in achieving its security objectives. The attributes used to compile the SES for the present benchmark sample of 65 organizations are listed in Table 1. The mean SES for the present benchmark sample of 65 companies is +.12 with a high of +1.78 to a low of -1.30.

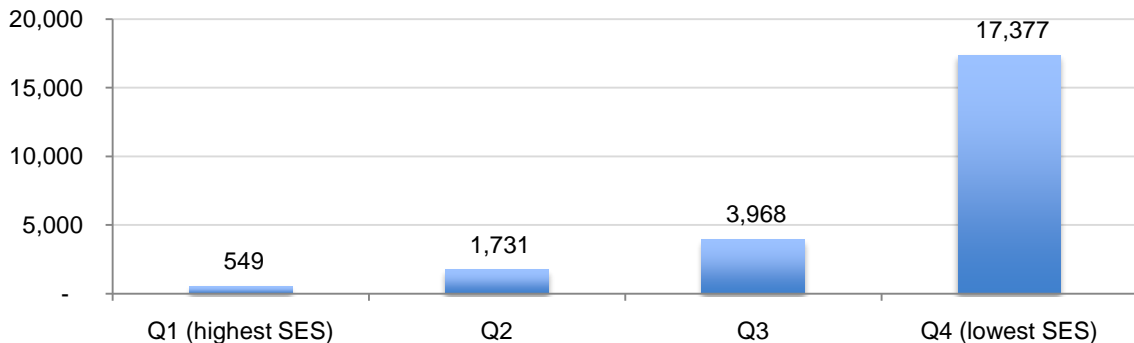
We segmented the overall benchmark sample into four SES quartile subgroups, ranging from Q1 (highest scores) to Q4 (lowest scores). Bar Chart 21 reports the average frequency of data breach incidents for healthcare organizations over a two-year period. Albeit not a linear relationship, organizations in the first and second quartiles (top half) experienced a lower number of data breach then organizations in the third and fourth quartile (bottom half) over two years.

Bar Chart 21: Extrapolated average frequency of data breach according to SES quartile



Bar Chart 22 reports the extrapolated average number of lost or stolen records (i.e., magnitude) as a result of data breach incidents according to SES quartile subgroups. This analysis shows a marked difference in the magnitude of data breach based on the organization’s security posture, wherein organizations in the lowest quartile subgroup average over 17,000 records in comparison to only 549 records in the highest quartile subgroup.

Bar Chart 22: Extrapolated average number of lost or stolen records according to SES quartile



³PGP Corporation and Ponemon Institute developed the Security Effectiveness Score (SES) for its annual encryption trends survey to define the security posture of responding organizations. The SES is derived from the rating of security features or practices (see Table 1). This method has been validated from more than 30 independent studies conducted since June 2005. The SES provides a range of +2 (most favorable) to -2 (least favorable). Hence, a result greater than zero is viewed as net favorable.

Part 3. Healthcare privacy 2010 year in review

2010 has been a pivotal year in the area of healthcare data privacy. September marked the end of the first twelve months that the Health Information Technology for Economic and Clinical Health (HITECH) Act took effect and that data breach incidents have been publicly reported to the Department of Health and Human Services (HHS). This past year we have also seen the first fines assessed for violations of the HIPAA privacy regulations. These events have provided a “window” into healthcare privacy that had not existed until passage of the HITECH Act.

HITECH Act and implications

The HITECH Act was passed as a component of the American Recovery and Reinvestment Act of 2009 (ARRA), also known as the Stimulus Bill, by Congress in February 2009. Under this bill, there were substantial new provisions for the safeguarding of protected health information (PHI) by healthcare organizations as well as their business associates.

These provisions require affected patients, HHS and sometimes the media to be notified in the event of an unauthorized disclosure of patient PHI. HITECH also included new requirements for securing and maintaining privacy of sensitive patient information and imposed penalties for violations. Under the Act, negligent compliance practices can result in fines up to \$1.5 million per incident, and state Attorneys’ General now have the authority to prosecute organizations that experience breaches.

As of September 30, 2010, there were 166 data breach incidents involving over 500 individuals reported to HHS and posted on their website. These incidents involved 4,905,768 individuals who had their PHI exposed. The largest of these incidents includes AvMed, Inc.’s exposure of 1,220,000 PHI records in December 2009 resulting from theft of an unencrypted laptop, Blue Cross Blue Shield of Tennessee’s exposure of 998,442 individual’s personal information in October 2009 and South Shore Hospital’s disclosure of 800,000 records in February 2010.

Enforcement environment, penalties and rules

While there have been no fines assessed in any of these three cases, there have been several high profile incidents where fines have been assessed. Connecticut Attorney General Richard Blumenthal settled the state’s lawsuit against Health Net in July 2010 regarding a breach of the personal information of 470,000 individuals for \$250,000. And in California, the Lucile Salter Packard Children’s Hospital at Stanford University was fined \$250,000 in September 2010 for not promptly reporting a data breach to the State of California Department of Public Health, as required by state law. These fines are an indicator of a much more aggressive enforcement posture across the country for the growing number of healthcare data privacy incidents.

The greatest controversy this past year has centered on HHS’ “harm threshold” provision that’s supposed to assist covered entities and business associates determine whether or not to report a breach. HHS has mandated post-incident risk assessments be used to determine the level of risk to the affected patients. If the assessment determined that there was substantial “risk of financial, reputational or other harm” as a result of the incident, the organization would be required to notify the affected individuals (as well as HHS and possibly the media).

The “harm threshold” created concern among privacy advocates that this self-monitoring approach would lead to inconsistent reporting and potentially intentional non-reporting of serious data privacy exposures. As a result of this uproar, HHS took an unprecedented step and withdrew their final rule for further consideration. It remains unclear whether their final rule will contain a “harm threshold” for data breach notification.

What's coming?

So what should we all expect to see in terms of healthcare data privacy in the near future? Obviously, we will see whether a harm threshold is used as a basis for determining whether notification is required for data privacy incidents. We will also see whether the aggressive postures of Connecticut and California on enforcement and fines for privacy violations will be replicated in other states, as well as by HHS. And, we will see whether national data privacy and data breach legislation will be passed that covers organizations outside of healthcare. Stay tuned.

Part 4. Implications and recommendations

Healthcare providers are at risk of non-compliance with regulations based on practices revealed in this study. They also risk severe economic consequences based on the data breach experience of organizations in this study.

The majority of respondents seem to be aware of the reasons why patient data is at risk. These include a lack of adequate staff, lack of resources to prevent or quickly detect patient data loss or theft, and a dearth of knowledge about compliance with healthcare regulations. Because of this awareness, more than half (56 percent) would appreciate help assessing their risks and procedures to make sure they are in compliance.

How does an organization's security posture and governance practices influence its ability to detect data breaches or prevent them and what the implications are for other healthcare organizations? As shown in the SES score presented in this paper, the healthcare organization's security posture is key to protecting patient privacy and safeguarding sensitive data. We believe this report can be helpful to healthcare organizations concerned about their privacy and data security practices. The findings in this report can assist organizations benchmark their own practices and determine how best to allocate their resources to strengthen their security posture.

Part 5. Benchmark Methods

Table 5 summarizes the sample response completed in October 2010. A total of 457 healthcare organizations were selected for participation and contacted by the researcher. Ninety-nine organizations agreed to complete the benchmark survey; however, 67 completed the benchmark instrument. Two instruments were incomplete and, hence, removed from the final benchmark sample. A final sample of 65 organizations was used in our analysis.

Table 5: Benchmark sampling response	Freq.	Pct%
Total healthcare organizations contacts made	457	100%
Total healthcare organizations recruited	99	22%
Total healthcare organizations participating	67	15%
Total healthcare organizations providing incomplete responses	2	0%
Final benchmark sample	65	14%

Pie Chart 1 reports the type of healthcare providers that participated in this research, with 54 percent representing private organizations. Pie Chart 2 shows the size of organizations with respect to the number of patient beds. Forty-five percent of participating healthcare providers have a 301 to 600-bed capacity, while 32 percent have 101 to 300 beds.

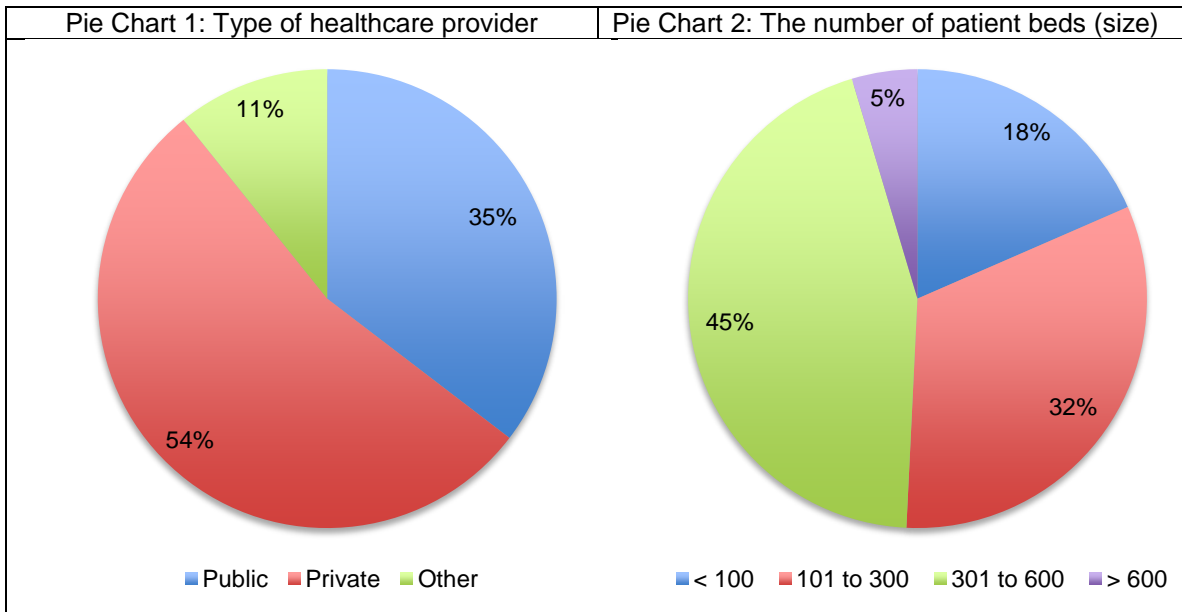


Table 6 provides a detailed breakdown of our final sample by US region. It shows the Northeast and mid-Atlantic regions as having the highest frequency of responding organizations.

Table 6: Regions of the United States where healthcare organization is located or headquartered.	Freq	Pct%
Northeast	15	23%
Mid-Atlantic	13	20%
Midwest	10	15%
Southeast	8	12%
Southwest	9	14%
Pacific	10	15%
Total	65	100%

Table 7 reports the department locations of individuals who responded to benchmark questions. As can be seen, compliance and IT are the most frequently cited functional areas. In total, 211 individuals from 65 organizations completed the diagnostic interview with the researcher (for an average of 3.25 per participating company).

Table 7. Department locations participating on organizations	Freq	Pct%
Compliance	59	91%
Information technology (IT)	31	48%
Records management	29	45%
Legal	13	20%
Medical informatics	13	20%
Finance	4	6%
Risk management	11	17%
Human resources	10	15%
Privacy	25	38%
Medical staff	6	9%
Patient services	6	9%
Other	5	8%
Development – foundation	4	6%
Marketing	13	20%
Planning	0	0%
Total	211	
Average number of interviews per HC organization	3.25	

Part 6. Caveats

The presented findings are based on self-reported benchmark survey returns.⁴ Usable returns from 65 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 healthcare providers.

⁴ 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.

Appendix 1: Detailed Results

The following tables provide the frequency and percentage frequency of all benchmark survey questions completed by participating companies. The field research was completed in October 2010.

Benchmark sampling response	Freq.	Pct%
Total healthcare organizations contacts made	457	100%
Total healthcare organizations recruited	99	22%
Total healthcare organizations participating	67	15%
Total healthcare organizations providing incomplete responses	2	0%
Final benchmark sample	65	14%

Part 1: Organizational Characteristics

Q1a. What best describes your organization:	Freq	Pct%
Public healthcare provider	23	35%
Private healthcare provider	35	54%
Other (please specify)	7	11%
Total	65	100%

Q1b. How many patient beds (capacity) does your healthcare facility or organization have?	Freq	Pct%
Less than 100	12	18%
101 to 300	21	32%
301 to 600	29	45%
More than 600	3	5%
Total	65	100%

Q1c. What best describes its operating structure?	Freq	Pct%
Integrated Delivery System	23	35%
Hospital or clinic that is part of a healthcare network	30	46%
Standalone hospital or clinic	11	17%
Other (please specify)	1	2%
Total	65	100%

Q1d. Please indicate the region of the United States where you are located.	Freq	Pct%
Northeast	15	23%
Mid-Atlantic	13	20%
Midwest	10	15%
Southeast	8	12%
Southwest	9	14%
Pacific	10	15%
Total	65	100%

Q1f. What best describes your role or the role of your supervisor?	Freq*	Pct%
Chief security officer	15	7%
Chief information security officer	20	9%
Chief information officer	12	6%
Chief privacy officer	9	4%
Chief compliance officer	24	11%
Chief medical officer	2	1%
Chief clinical officer	1	0%
Chief finance officer	12	6%
Chief development officer	4	2%
General counsel	13	6%
HIPAA compliance leader	25	12%
Billing & administrative leader	31	15%
Medical records management leader	28	13%
Human resources leader	10	5%
Clinician	2	1%
Other	3	1%
Total	211	100%
Average number of interviews per HC organization	3.25	

Q1g. What best describes your department?	Freq	Pct%
Compliance	59	91%
Privacy	9	14%
Information technology (IT)	31	48%
Legal	13	20%
Finance	12	18%
Marketing	3	5%
Medical informatics	13	20%
Medical staff	6	9%
Patient services	6	9%
Records management	29	45%
Risk management	11	17%
Development – foundation	4	6%
Planning	0	0%
Human resources	10	15%
Other	5	8%
Total	211	
Average number of interviews per HC organization	3.25	

Part 2. Organizational Experience

Attributions about your healthcare provider	Strongly agree	Agree
Q2. My organization has sufficient policies and procedures that effectively prevent or quickly detect patient data loss or theft.	18%	23%
Q3. My organization has sufficient technologies that effectively prevent or quickly detect patient data loss or theft.	15%	22%
Q4. My organization has sufficient resources to prevent or quickly detect patient data loss or theft.	11%	18%
Q5. My organization has personnel who have sufficient technical expertise to be able to identify and resolve data breaches involving the loss or theft of patient data.	18%	24%
Q6. My organization has personnel who are knowledgeable about compliance with healthcare regulations including data breach notification and risk assessment requirements.	23%	25%
Q7. In my organization, medical practitioners understand the importance of patient data protection.	27%	21%
Q8. In my organization, administrative personnel understand the importance of patient data protection.	30%	30%
Q9. In my organization, medical billing personnel understand the importance of patient data protection.	19%	22%
Q10. In my organization, IT personnel understand the importance of patient data protection.	18%	25%
Q11. In my organization, the prevention of patient data loss or theft is a top priority.	11%	19%
Q12. In my organization, new federal regulations have significantly changed patient records management practices.	15%	14%

Q13. Has your department suffered a data breach involving the loss or theft of patient data in the past two years?	Freq.	Pct%
No	9	14%
Yes, 1 incident	17	26%
Yes, 2 to 5 incidents	20	31%
Yes, more than 5 incidents	19	29%
Total	65	100%
Extrapolated number of data breaches for the benchmark sample	191	

Q14. How confident are you that your organization has the ability to detect all patient data loss or theft?	Pct%
Very confident	11%
Confident	31%
Little confidence	35%
No confidence	23%
Total	100%

Q15. Up to five separate data breach incidents over the past 2 years.	
Number of incidents reported	157
Average number of incidents for the benchmark sample	2.42

15a. Approximate number of records	Freq.	Pct%
10 – 100	95	61%
101 - 1,000	31	20%
1,000 - 5,000	19	12%
5,001 - 10,000	8	5%
10,001 – 100,000	3	2%
Over 100,000	1	1%
Total	157	100%
Average number of lost or stolen records per breach	1,769	

15b. Approximate percentage of patients notified	Freq.	Pct%
None	60	38%
Below 10%	4	3%
11 to 25%	1	1%
26 to 50%	11	7%
51 to 75%	11	7%
75 to 90%	17	11%
Everyone	53	34%
Total	157	100%
Average percentage notified	50%	

15c. Nature of the data loss or theft	Freq.*	Pct%
Unintentional employee action	71	52%
Lost or stolen computing device	65	41%
Third-party snafu	54	34%
Technical systems glitch	49	31%
Criminal attack	29	20%
Malicious insider	23	15%
Intentional non-malicious employee action	16	10%
Total	319	203%
*More than one selection is permitted		

15d. How the data breach was discovered	Freq.*	Pct%
Employee detected	74	47%
Audit/assessment	65	41%
Patient complaint	64	41%
Accidental	33	21%
Legal complaint	30	19%
Loss prevention	14	9%
Law enforcement	13	8%
Total	293	187%
*More than one selection is permitted		

15e. Approximate length of time to resolve incident	Freq.	Pct%
Immediate	13	8%
One week	8	5%
One month	19	12%
Three months	45	29%
Six months	34	22%
One year or more	23	15%
Not resolved	15	10%
Total	157	100%
Average length of time to resolve incident (days)	161	

Q16. 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	81%
Time and productivity loss	80%
Loss of patient goodwill	77%
Loss of revenues	43%
Cost of outside consultants and lawyers	39%
Fines and penalties paid to regulators	37%
Lawsuits	23%
Poor employee morale	18%
No impact	15%
Other (please describe)	2%

Q17. 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	12%
\$10,001 to \$50,000	29%
\$50,001 to \$100,000	21%
\$100,001 to \$200,000	13%
\$200,001 to \$500,000	5%
\$500,001 to \$1 million	3%
More than \$1 million	2%
Cannot determine	15%
Total	100%
Average lifetime value of one lost patient (customer)	\$107,580

Q18. 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	4%
\$10,001 to \$50,000	1%
\$50,001 to \$100,000	4%
\$100,001 to \$200,000	11%
\$200,001 to \$500,000	25%
\$500,001 to \$1 million	19%
\$1 million to 10 million	23%
More than \$10 million	6%
Cannot determine	7%
Total	100%
Average economic impact of data breach over the past two years	\$2,060,174

Q19. In your opinion, what harms do patients actually suffer if their records are lost or stolen?	Pct%
Increased risk of financial identity theft	56%
Increased risk of medical identity theft	45%
Increased risk that personal health facts will be disclosed	61%
None	8%
Total	170%

Q20. 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	23%
No	36%
Unsure	41%
Total	100%

Q21. What type of data is most susceptible to data loss or theft within your department?	Pct%
Billing information	35%
Medical records	26%
Clinical trial data	2%
Employee records	12%
Non-patient related confidential information	20%
Other (please specify)	5%
Total	100%

Q22a. Has your organization implemented an electronic health records (EHR) system?	Pct%
Yes, fully implemented	21%
Yes, implementation is in process	35%
No, but we have plans to implement in the near future	23%
No, and we do not have plans to implement at this time	21%
Total	100%

Q22b, 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	74%
EHR has made patient data less secure	10%
EHR has made no difference in the security of patient data	12%
Unsure	4%
Total	100%

Part 3: Security Environment

Q23. The following table lists 26 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	17%	15%
Determine the root causes of major data breaches involving patient information	15%	15%
Know where patient information is physically located	16%	31%
Secure patient data at rest	15%	27%
Secure patient data in motion	16%	31%
Secure endpoints to the network	21%	30%
Identify system end-users before granting access rights to patient information	16%	29%
Protect patient information used by outsourcers including cloud computing vendors	0%	10%
Protect patient information used by business associates	10%	19%
Have standard agreements with business associates that clearly explain the requirements for data protection	37%	29%
Prevent or curtail major data breaches involving patient information	16%	15%
Prevent or curtail cyber attacks that attempt to acquire patient information	18%	19%
Limit physical access to data storage devices containing patient information	12%	12%
Demonstrate the economic value or other tangible benefits of the company's security program	5%	12%
Ensure minimal downtime or disruptions to systems resulting from security problems	34%	31%
Comply with legal requirements and policies including privacy laws and statutes (i.e., HIPAA)	34%	51%
Conform with leading self-regulatory requirements such as ISO, NIST, HITRUST and others	21%	40%
Prevent or curtail viruses and malware infections	18%	38%
Perform timely updates for all major security patches	14%	39%
Control all live data used in systems development activities	19%	20%
Enforce corporate policies, including the termination of employees or contractors who pose a serious insider threat	32%	40%
Attract and retain high quality IT security personnel	23%	32%
Training and awareness program for all system users	36%	35%
Conduct independent audits of the system	19%	26%
Security program administration is consistently managed	25%	27%
Prevent or curtail cyber attacks	18%	21%

Part 4: Enabling Security Technologies

Q24. Please review the following list of 20 enabling security technologies that may be deployed within your organization today. First, indicate whether the stated technology is presently deployed. Then use the following three-point scale to rate each technology in terms of its impact on data breach prevention and compliance with HIPAA.	Data breach prevention	Compliance with HIPAA
Access governance systems	73	73
Anti-virus & anti-malware	70	65
Code review tools	31	33
Security intelligence & event manager (SIEM)	35	43
Data loss prevention (DLP)	48	69
Database scanning and monitoring	65	67
Encryption for data at rest	60	72
Encryption for data in motion	65	57
Endpoint security solutions	56	47
Firewalls	83	78
ID & credentialing systems	16	40
Intrusion detection systems	35	33
Intrusion prevention systems	32	18
Log management	65	55
Network intelligence systems	25	27
Perimeter or location surveillance	39	27
Privileged user management	75	72
Service oriented architecture (SOA)	19	9
Virtual private network (VPN)	64	56
Web application firewalls (WAF)	45	49
Average	50.05	49.5
Scale: 0 = No impact to 100 = Maximum impact		

Part 5: Controls & Governance

Q25. Please review the following list of 19 control 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 and compliance with HIPAA.	Data breach prevention	Compliance with HIPAA
Background checks of privileged users	45	55
Annual (periodic) risk assessments	65	89
Business continuity plans	61	56
Incident response plans	69	66
Certification of security staff	54	65
Control self-assessment	89	90
Disposal of electronic data-bearing devices	24	23
Disposal of paper documents	49	43
External audits	57	40
Helpdesk activities	17	14
Monitoring regulatory change	16	66
Quality assurance	2	12
Record retention & archive management	65	61
Redress & enforcement	56	56
Workplace surveillance	56	77
Training of patient or customer data handlers	90	89
Training of end users	82	84
Upstream communications	16	43
Vetting & monitoring of third parties including business associates	89	88
Average	53	59
Scale: 0 = No impact to 100 = Maximum impact		

Q26. Please review the following list of 11 governance practices that may be performed in your organization today. First, indicate whether the stated control activity is presently performed. Then use the following three-point scale to rate each activity in terms of its impact on data breach prevention and compliance with HIPAA.	Data breach prevention	Compliance with HIPAA
Appointment of a data protection executive	79	76
Board involvement in data protection efforts	22	19
Board understanding of data protection risks	64	61
Direct budgetary authority for data protection	83	82
Community outreach on patient privacy issues	15	16
Cross-functional steering committee	24	25
Metrics or measures used to define success	17	19
A security department that is officially sanctioned with charter	32	35
Participation in benchmark program (with reference to peer group of healthcare companies)	29	40
Segregation of duties between data protection and IT operations	33	39
Upstream data breach incident reporting channel to the chief executive	78	80
Average	43	45
Scale: 0 = No impact to 100 = Maximum impact		

Part 6. Data protection and security budget

Q27. 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.	15%	18%
My organization's security budget is sufficient to ensure our IT systems are not attacked or disrupted by attackers.	9%	20%
My organization's security budget is sufficient to achieve compliance with HIPAA and other regulatory requirements.	19%	29%
My organization's security budget ensures expenditures are made efficiently (i.e., costs are not squandered).	18%	25%
My organization's security budget is sufficient to curtail or minimize data breach incidents.	11%	15%
My organization's security budget is sufficient to ensure policies are strictly enforced throughout the enterprise.	13%	21%
Average	14%	21%

Part 7. Other questions

Q28. What level of staffing do you have to manage data protection efforts throughout the enterprise?	Pct%
No dedicated staff	28%
Less than 2	35%
Between 3 and 5	8%
Between 6 and 10	6%
Between 11 and 15	5%
Greater than 15	18%
Total	100%

Q29. What best describes the process for preventing and detecting data breach incidents in your organization today? Please select one <u>best</u> choice.	Pct%
An "ad hoc" process	35%
Mostly a process that relies on policies and procedures	23%
Mostly a process that relies on security technologies	16%
A combination of manual procedures and security technologies	20%
None of the above	6%
Total	100%

Q30. Who is most responsible for preventing and detecting data breach incidents in your organization?	Pct%
Information technology department	12%
Information security department	11%
Compliance department	34%
Privacy office	5%
Legal department	2%
Business unit managers	9%
Human resource department	4%
No one person or department	23%
Other (please specify)	0%
Total	100%

Q31a. Do you have a clear written policy for employees to notify appropriate authority if they suspect a data breach has occurred?	Pct%
Yes	88%
No	12%
Total	100%

Q31b. If yes, do you think this policy is effective in curtailing or detecting most data breaches?	Pct%
Yes	44%
No	56%
Total	100%

Q32. Does your organization use external resources such as consultants, auditors and lawyers to help to prevent or detect data breach incidents?	Pct%
Yes	40%
No	60%
Total	100%

Q33. 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	Confident
	16%	15%

Q34. In your opinion, what are the key problems you face when dealing with patient data loss or theft? Please select only your top two choices.	Pct%
Insufficient knowledge about threats	32%
Insufficient security technologies	15%
Keeping pace with the rash of criminal attacks	8%
Keeping pace with new technologies that increase security risks (such as mobile devices)	41%
Lack of consistently applied control procedures	26%
Insufficient resources to get the job done right	45%
Lack of well trained or experienced personnel	30%
Other (please specify)	3%
Total	200%

Q35. How important are security technologies for your organization's ability to defend itself against patient data loss or theft.	Essential	Very important
	0.21	0.35

Q36. How important are controls and governance practices for your organization's ability to defend itself against patient data loss or theft.	Essential	Very important
	0.25	0.34

Q37. How important is it to your organization that a harms threshold standard exist in order to determine whether a data security incident requires notification to affected individuals?	Essential	Very important
	17%	41%

Q38a. Does your organization conduct HHS-mandated post data breach incident risk assessments?	Pct%
Yes, we have a formal process in-place	18%
Yes, we have an ad hoc process in-place	36%
No, but we are in the process of developing this	43%
No, we do not have plans to implement a process	3%
Total	100%

Q38b. Do you believe HHS-mandated risk assessments are effective in determining the risk of harm to individuals affected by data breaches?	Pct%
Yes	55%
No	45%
Total	100%

Q39. What do you believe is most effective in preventing a data breach incident within your organization? Please choose only two responses.	Pct%
Training and awareness programs	53%
Enabling security technologies	41%
Policies and procedures	9%
Governance & leadership	24%
Manual controls	19%
Risk assessments	45%
Independent audits	2%
Other (please specify)	0%
Total	193%

Q40. What do you think are your biggest weaknesses for a data breach to occur within your organization? Please choose only two responses.	Pct%
Lack of trained staff and end users	49%
Inadequate budget for security and privacy	51%
Lack of enabling security technologies	12%
Lack of manual controls	9%
Lack of governance and leadership	19%
Insufficient assessments for risk	43%
Lack of policies and procedures	16%
Other (please specify)	0%
Total	199%

Q41. Do you need help to assess your risks and procedures to make sure that you are compliant and doing everything you can?	Pct%
Yes	56%
No	26%
Unsure	18%
Total	100%

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.