



# Are You Ready for HITECH?

A benchmark study of healthcare covered entities & business associates

---

---

**Sponsored by Crowe Horwath** LLP

Independently conducted by Ponemon Institute LLC

Publication Date: November 10, 2009

## Are You Ready for HITECH?

### A Benchmark Study of Healthcare Covered Entities and Business Associates

Prepared by Ponemon Institute, November 10, 2009

#### I. Executive Summary

*Are You Ready for HITECH: A Benchmark Study of Healthcare Covered Entities and Business Associates* was conducted by Ponemon Institute and sponsored by Crowe Horwath. The purpose of the study is to determine the readiness of healthcare companies to comply with the privacy and security provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act. The Act extends the Health Insurance Portability and Accountability Act's (HIPAA) rules for security and privacy safeguards, including increased enforcement, penalties and audits.

To determine readiness for HITECH, our study covered privacy, data protection, information security and risk management activities being deployed by companies in response to present and emerging regulatory requirements. In addition to readiness, the benchmark results assess potential gaps to compliance that companies need to resolve. Specific areas of the benchmark instrument include:

- Policies and standard operating procedures (SOPs)
- Training, awareness
- Downstream communications
- Program management activities
- Data security methods and tools
- Compliance monitoring, assessment and audit
- Redress and enforcement

A total of 260 healthcare organizations were identified and contacted by the researcher. This resulted in 77 completing the benchmark survey instrument over a seven-week period ending in October 2009. Of these responding companies, 42 are covered entities (including hybrid organizations) and 35 are business associates, according to HIPAA classification.

The sample of responding companies varied in size from less than 100 full-time employees to more than 25,000 full-time employees. Participating healthcare organizations were located in all major regions of the United States. A detailed description of the participating organizations is presented in the methods section of this paper.

Benchmark methods utilized a standardized survey instrument that was completed by each responding organization. Individuals deemed to be most responsible for ensuring HIPAA and HITECH compliance were asked to field the instrument within their organizations. In a majority of cases, the researcher re-contacted or visited the responding organization to verify certain responses or to resolve potential inconsistencies.

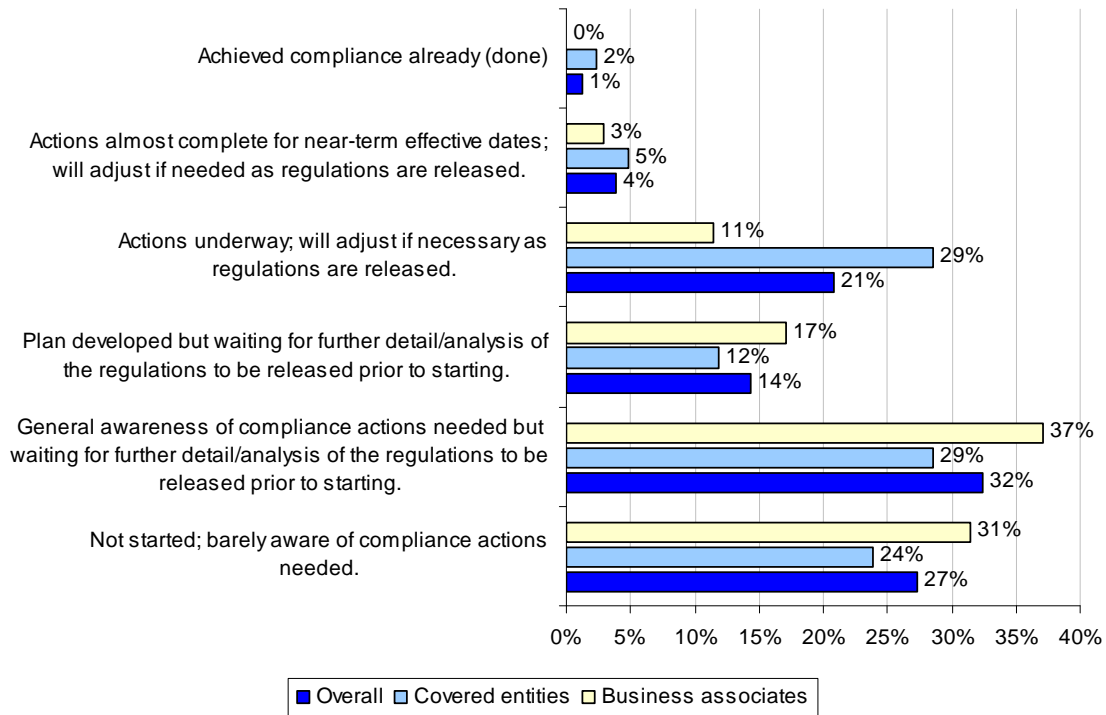
As shown in Bar Chart 1, 94 percent of the healthcare organizations in our study are not in substantial compliance with HITECH.<sup>1</sup> This was determined from participants' responses to six levels of preparedness for HITECH. Bar Chart 1 also shows that covered entities report a much higher level of compliance readiness than business associates.

Overall responses are as follows: 27 percent have not started and are barely aware of what they need to do, 32 percent are waiting for more detail, 14 percent have a plan but are waiting for more detail and 21 percent are just starting to act. Only 1 percent of organizations are ready and 4 percent are almost ready to meet the deadlines for near-term effective dates.

---

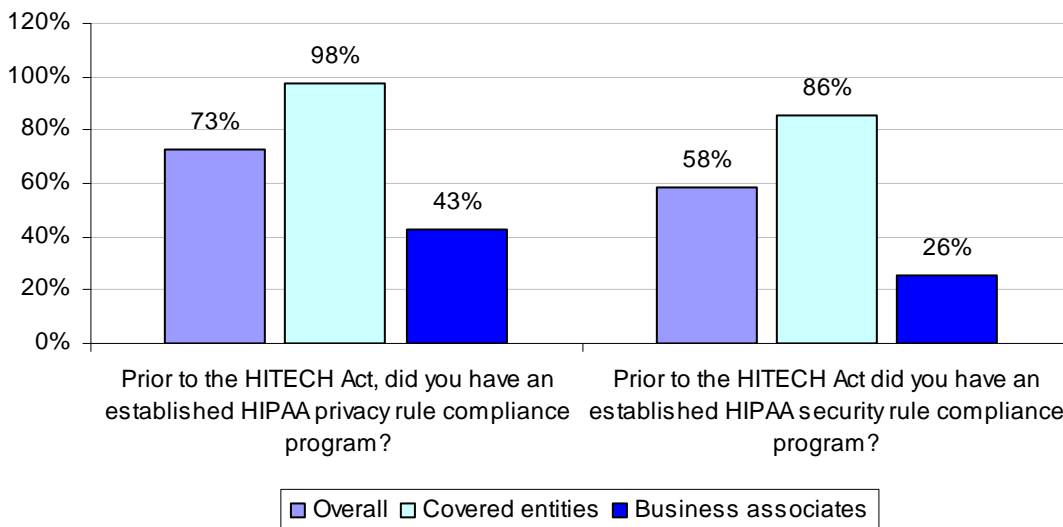
<sup>1</sup> Please note that at the time of this study, organizations had approximately four months remaining until HITECH requirements will go into effect (February 2010).

**Bar Chart 1**  
**State of HITECH Act compliance readiness**



Bar Chart 2 shows that nearly all of the participating covered entities (98 percent) versus only 43 percent of business associates report they have a formally implemented HIPAA privacy compliance program. Similarly, 86 percent of covered entities and only 26 percent of business associates say they have a formally implemented HIPAA security compliance program.

**Bar Chart 2**  
**HIPAA programs prior to HITECH**  
Percentage Yes response



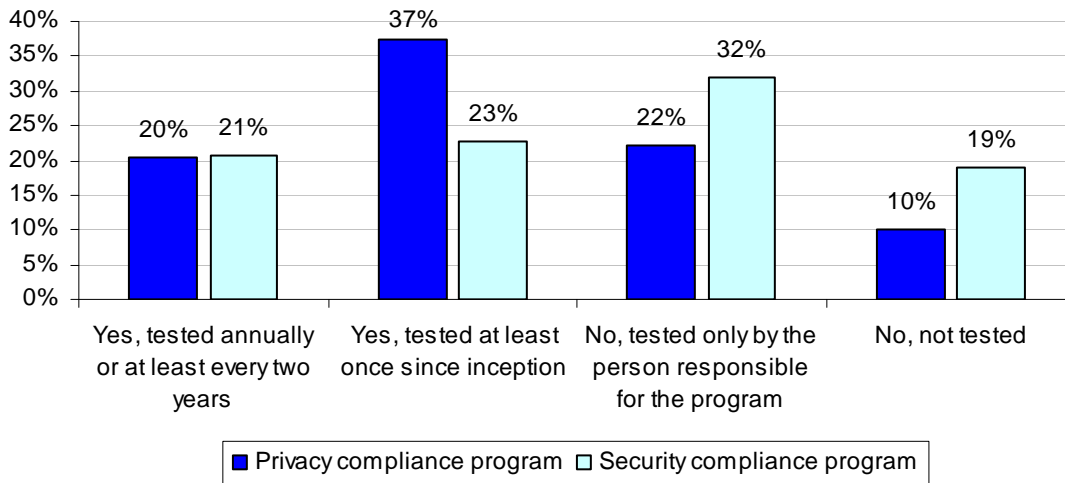
## II. Key Findings

### 1. HIPAA compliance programs have deficiencies, according to most organizations.

We asked organizations to comment on the actions they have taken to comply with the major provisions of HIPAA and HITECH. Of those organizations that have a privacy and security compliance program in place, 20 and 21 percent, respectively, have an independent party test the program for adequacy annually or at least every two years (see Bar Chart 3).

**Bar Chart 3**  
Testing the adequacy of the HIPAA compliance program

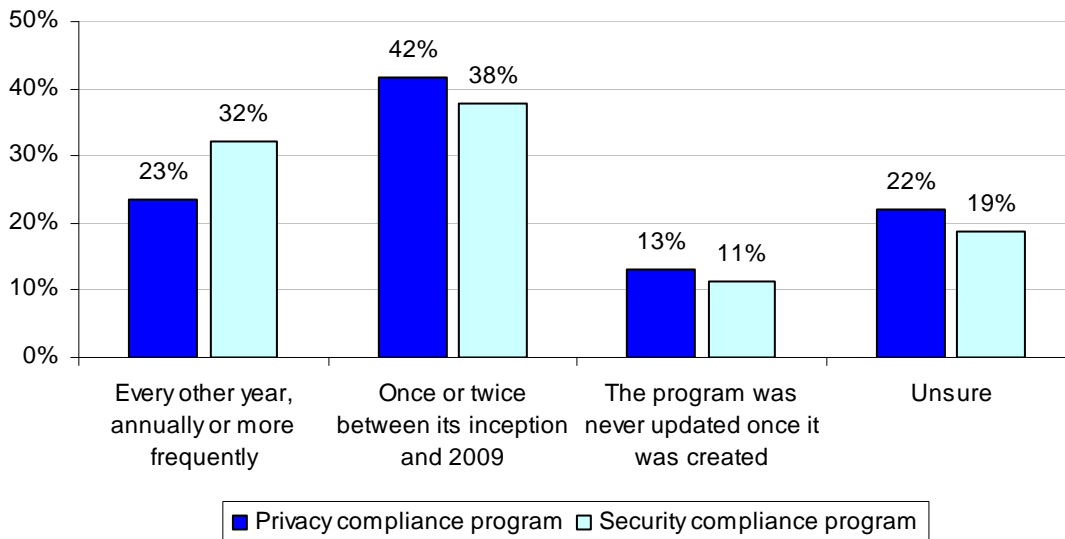
Has your HIPAA compliance program been tested for adequacy by an independent party (internal or external) not responsible for program management?



As shown in Bar Chart 4, 42 percent of participating organizations have updated their privacy programs at least once since inception, and 38 percent have similarly updated their security compliance program.

**Bar Chart 4**  
Updating the HIPAA compliance program

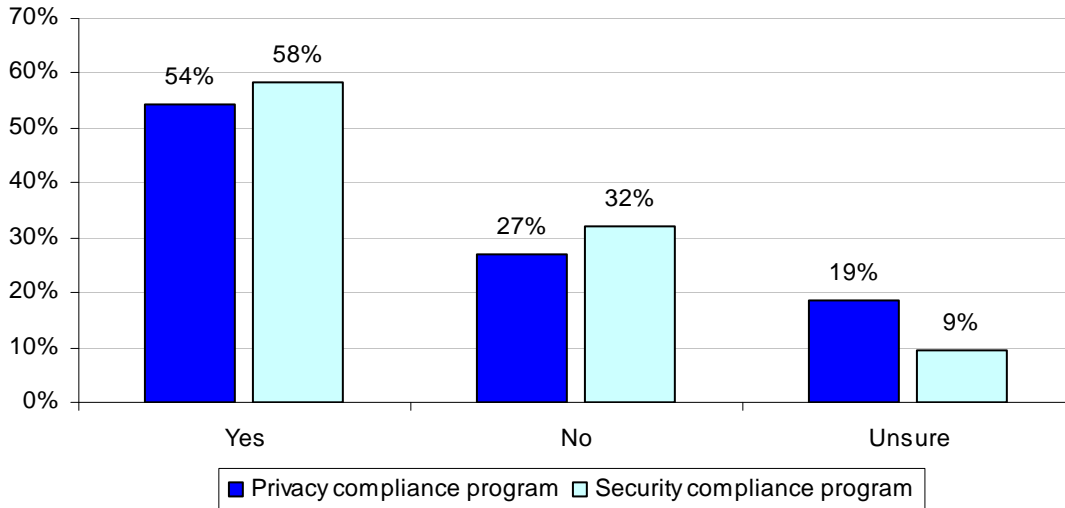
How frequently has your HIPAA compliance program been updated?



Fifty-four and 58 percent of participating organizations, respectively, report that they are aware of deficiencies in their privacy compliance and security compliance programs respectively (see Bar Chart 5).

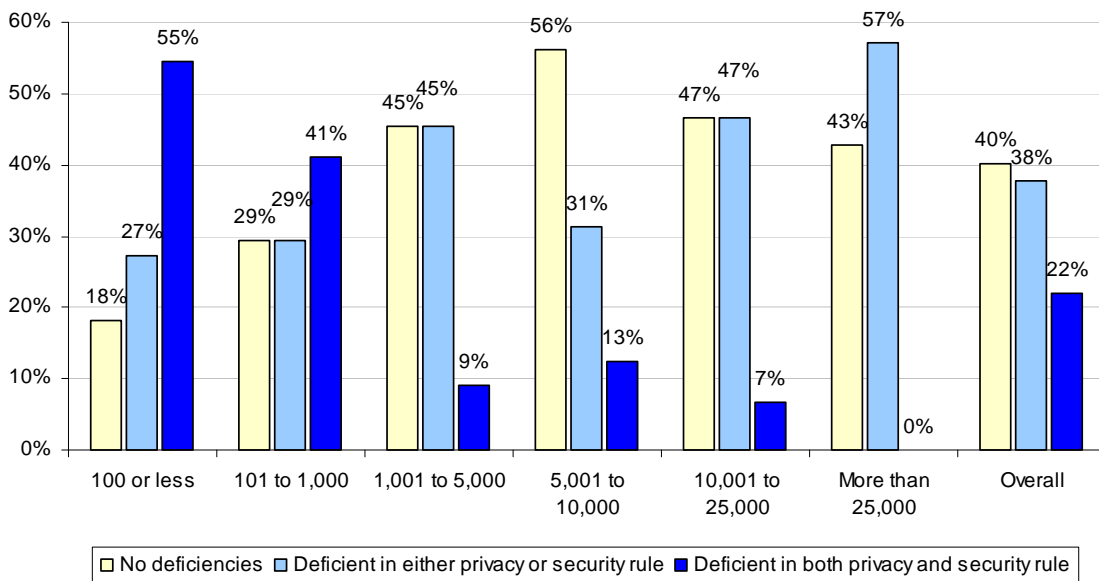
**Bar Chart 5**  
**Known deficiencies in the HIPAA compliance program**

Were there known deficiencies in your HIPAA compliance program?



As shown in Bar Chart 6, cross-tabulations revealed smaller-sized healthcare organizations are more likely to report deficiencies in their HIPAA privacy rule and/or security rule compliance programs, respectively. Very small organizations – those with less than 100 employees – are most likely to acknowledge deficiencies in both their privacy and security programs.

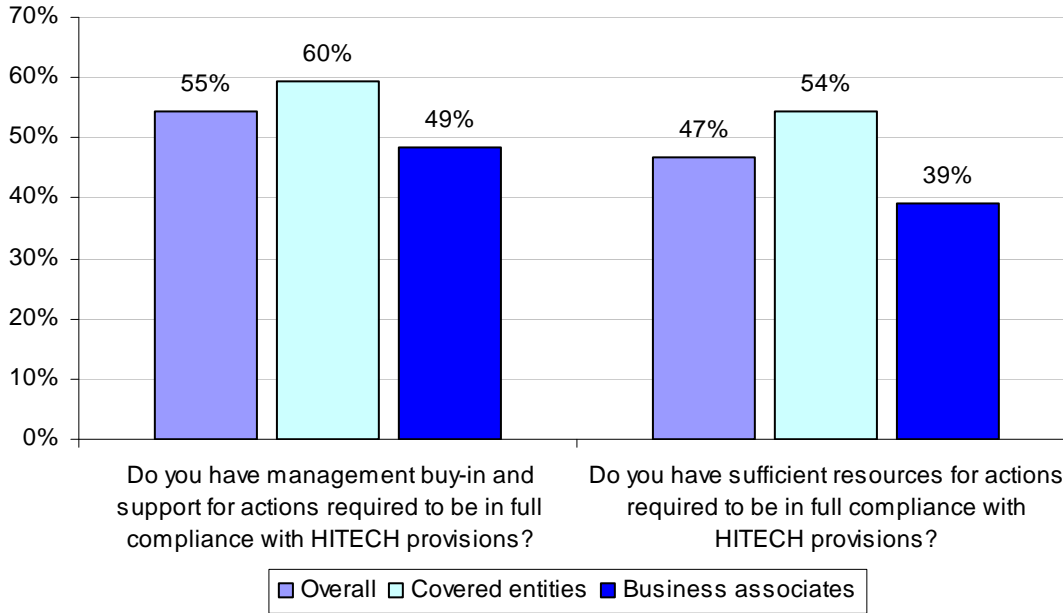
**Bar Chart 6**  
**HIPAA deficiencies by organizational size (headcount)**



**2. Lack of management buy-in and support may stymie compliance goals.**

As already stated, most healthcare organizations in our study readily admit to compliance gaps. Fifty-five percent reports there is management buy-in for compliance with HITECH. Forty-seven percent of respondents say they have sufficient resources to achieve compliance with HITECH provisions (see Bar Chart 7).

**Bar Chart 7**  
**Management buy-in and sufficiency of resources**  
 Percentage Yes response



There are, however, differences between covered entities and business associates as shown in the above chart. Accordingly, more than 60 percent of covered entities say they have sufficient support from management to achieve compliance goals. On the other hand, only 49 percent of business associates state they have management support. With respect to the sufficiency of budgets to achieving compliance goals, 54 percent of covered entities and 39 percent of business associates believe they have the necessary funding and resources.

**3. Despite HIPAA mandatory regulatory requirements, both covered entities and business associates report significant gaps in their privacy and security programs.**

Our benchmark methods revealed that more than 32 percent of respondents believe their organizations do not provide adequate staff training for both privacy and security. Twenty-one percent believe their organizations have not formally implemented a risk-based assessment program for protecting the privacy of protected health information. Another 21 percent believe their organizations have not effectively developed a privacy policy that clearly summarizes appropriate use and sharing of protected health information.

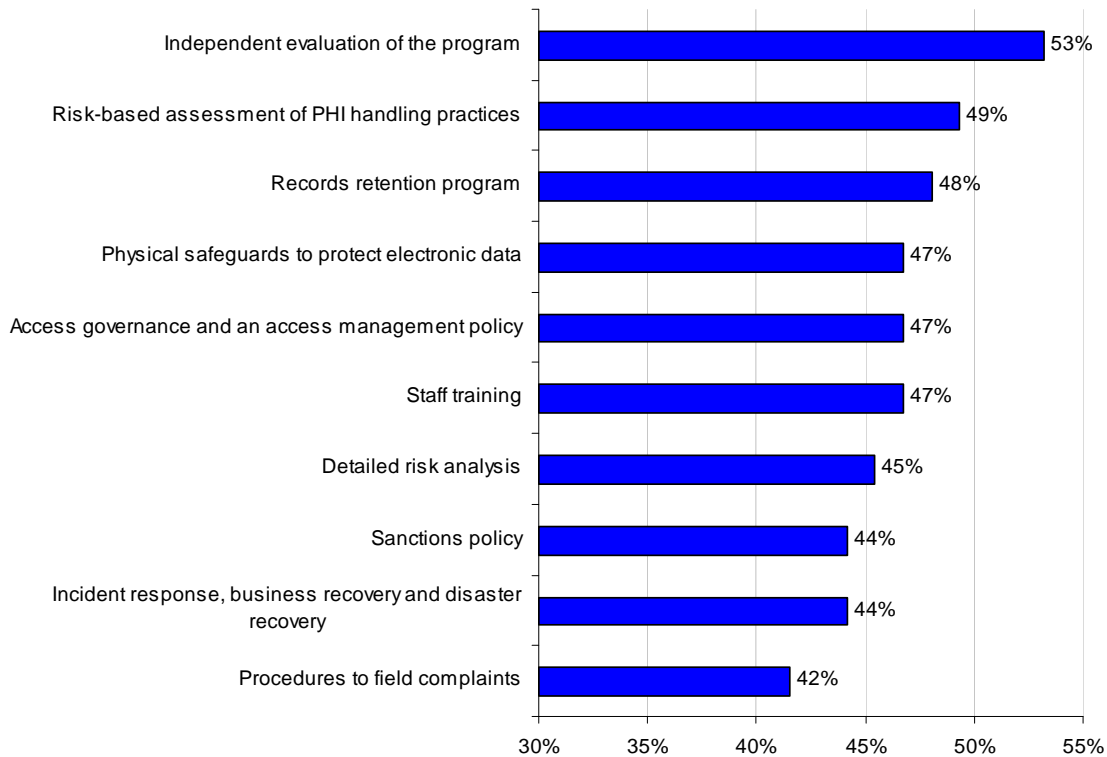
With respect to security, 34 percent of respondents state their organizations do not perform a periodic independent evaluation of their programs. Another 30 percent say their organizations do not conduct a detailed security risk analysis. And, 22 percent of respondents state their organizations have not formally assigned the role of security officer or CISO.

With respect to HITECH compliance requirements, 26 percent of respondents state they have not conducted a review of marketing activities to ensure secondary uses of information do not violate

HIPAA privacy requirements. Another 25 percent say their organizations have not performed any system review to determine their capabilities to provide accounting of disclosure and to address gap issues. Finally, 22 percent of respondents say their organizations have not taken any steps to ensure data collection procedures conform to the minimization principle (i.e., collect only that which is needed to fulfill a legitimate operation or task).

Bar Chart 8 summarizes the HIPAA privacy and security program requirements least likely to be implemented formally. Each bar shows the percentage of respondents who said the given requirement is either not implemented or only informally implemented within their organization.

**Bar Chart 8**  
**HIPAA compliance requirements that are not formally implemented**



Cross-tabulations show that compliance implementation is systemically related to organizational size. That is, smaller-sized healthcare companies appear to be less likely to have officially implemented key aspects of their HIPAA privacy and security programs. In addition, smaller companies are less likely to demonstrate readiness to comply with HITECH. In contrast, covered entities appear, on average, to have implemented more compliance program elements than business associates.

**4. Some respondents believe certain aspects of compliance will have a significant impact on their organization’s business and operations.**

Thirty percent of respondents say that staff training (which is a compliance deficiency area) and 40 percent of respondents say implementation of procedures to field complaints will have a significant impact on their organization’s business and operations. Another 25 percent believe that the assignment of a privacy leader (CPO) as well as the implementation of a sanctions policy will have a significant impact on business and operations.

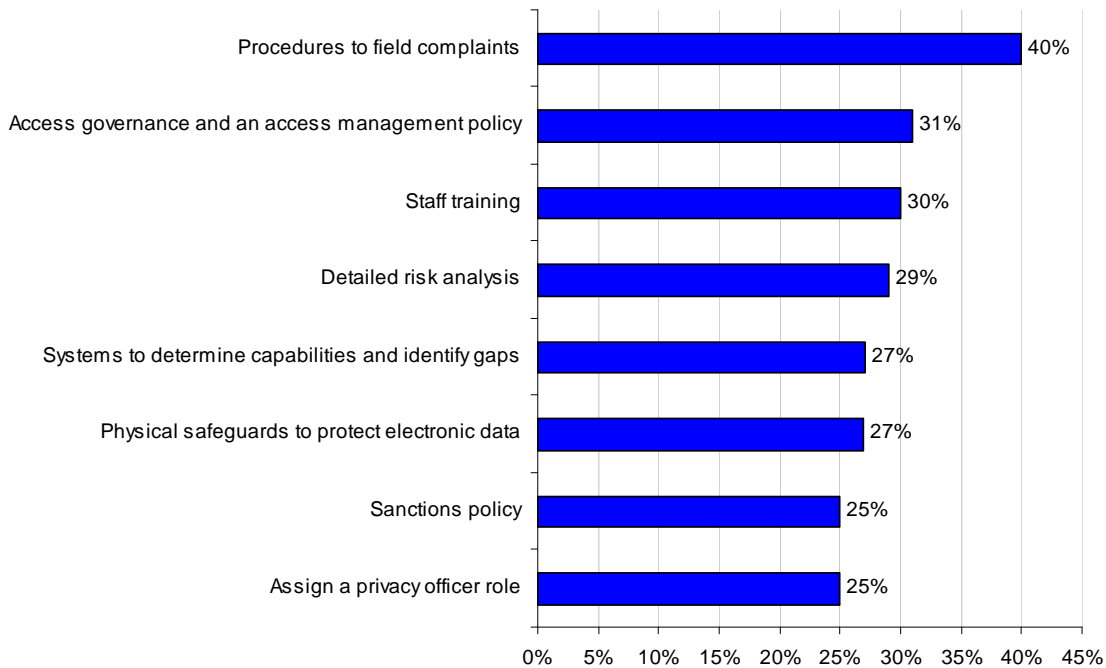
With respect to the security rule, 31 percent believe that implementing access management systems and information governance policies would significantly impact business and operations. Also, procedures to safeguard physical access to electronic data storage would significantly impact business and operations.

With respect to HITECH, 27 percent of respondents believe system level reviews and the review of marketing activities to mitigate secondary uses of protected health information would significantly impact their organization’s business and operations.

Cross tabulations reveal that smaller-sized healthcare organizations are more likely to see compliance requirements as a significant impact on business and operations than larger organizations. Similarly, covered entities are more likely to see privacy requirements as having a significant impact on business and operations than business associates. In contrast, business associates are more likely to see security requirements as having a significant impact on business and operations than covered entities.

Bar Chart 9 summarizes the HIPAA privacy and security program features with a significant impact on operations. Each bar shows the percentage of respondents who said the given feature will have a significant impact on operations within their organization.

**Bar Chart 9**  
**HIPAA compliance features that have a significant impact on business operations**



**5. Respondents agree that assistance from an expert source (third-party) is necessary for achieving certain compliance goals.**

Bar Chart 10 summarizes the HIPAA privacy and security program features most likely to require outside assistance from an expert. Each bar shows the percentage of respondents who said the given feature will likely require the assistance of a third-party vendor such as a consultant, lawyer, auditor or systems integrator.

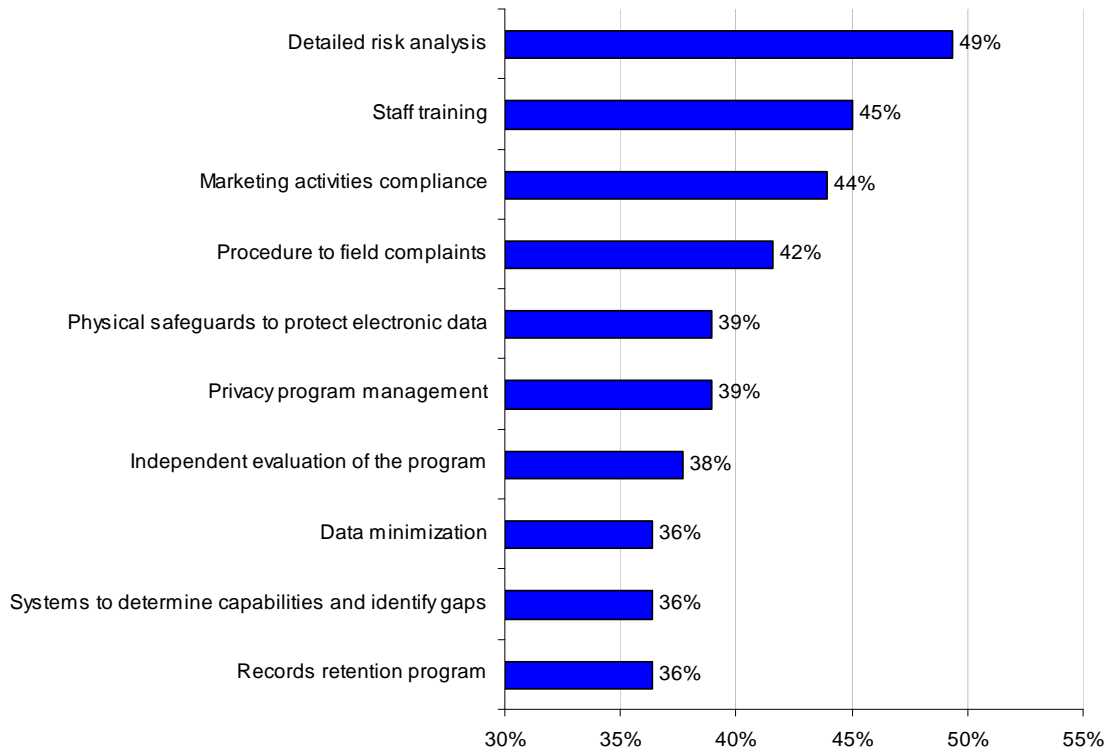
Many respondents say their organizations require assistance from a bona fide third-party such as a consultant, attorney, auditor or systems integrator. Forty-nine percent say they need outside support to conduct a detailed risk analysis, and 45 percent need outside support for staff training.

Forty-four percent say they will engage third-parties to ensure marketing activities conform to compliance requirements. Forty-two percent say that assistance from a third-party may be necessary to implement procedures for fielding complaints. Thirty-nine percent of respondents say their organizations may need third-party assistance in developing physical safeguards to protect electronic data. And, another 39 percent say they will need assistance with privacy program management.

In addition, 38 percent see the need to hire third-parties to perform independent audits of the compliance program. Finally, 36 percent of respondents see the need to: hire third-parties for data minimization, to help implement systems to determine capabilities and identify gaps, and records retention programs.

Cross-tabulations reveal smaller-sized healthcare organizations are less likely to engage consultants or legal experts to help implement key features of HIPAA or HITECH. Similarly, covered entities appear to be less likely to engage third parties to assist on privacy compliance issues. Business associates appear to be less likely to engage third parties to implement HIPAA security compliance requirements, but more likely to hire consultants to implement HITECH.

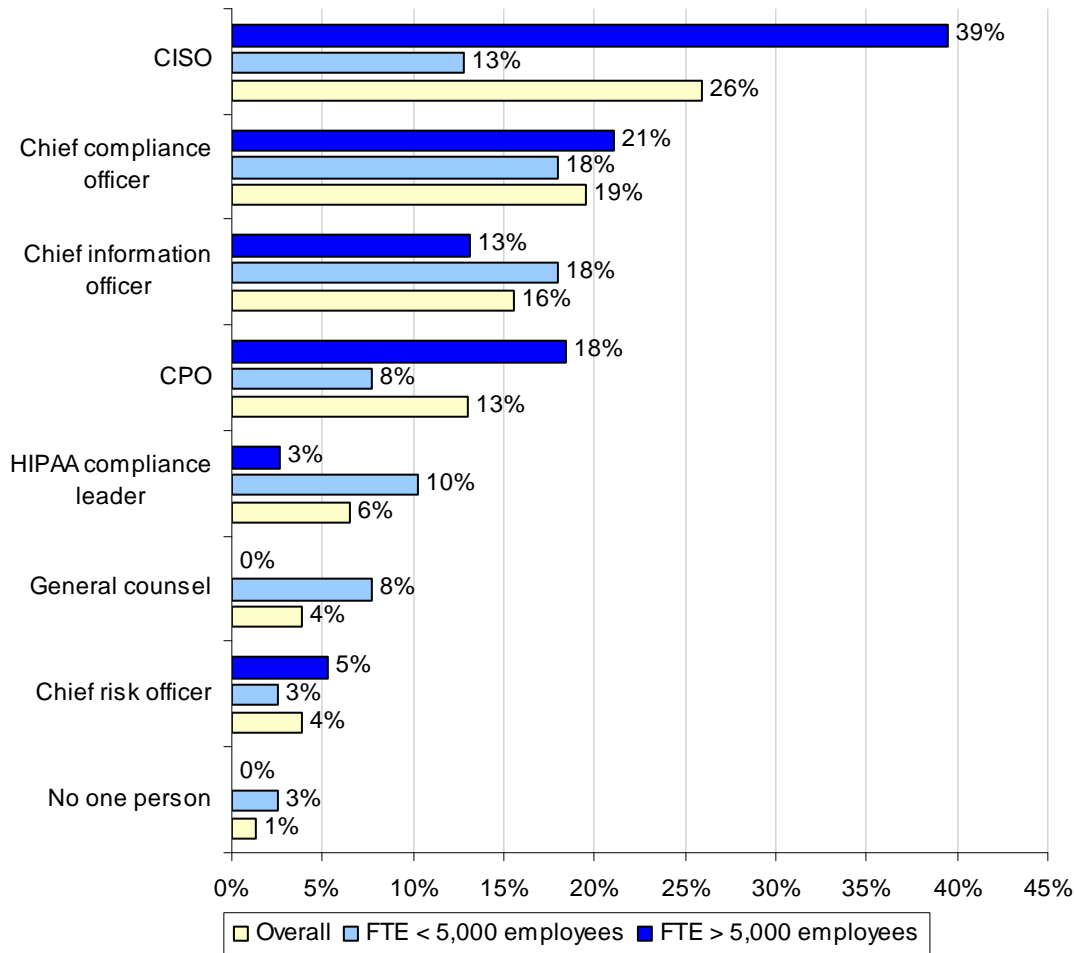
**Bar Chart 10**  
**HIPAA compliance features most likely to require third-party (expert) assistance**



**6. Responsibility for ensuring HITECH compliance varies considerably among participating organizations.**

While no one function dominates responsibility for HITECH compliance, security leaders (CISOs) and chief compliance officers are the most likely roles to lead this compliance effort. Other roles or functions important for HITECH compliance include the chief information officer (CIO) and chief privacy officer (CPO). Our findings also show role differences based on organizational size. As can be seen, organizations with more than 5,000 employees are much more likely to see a CISO as having primary responsibility than smaller-sized companies.

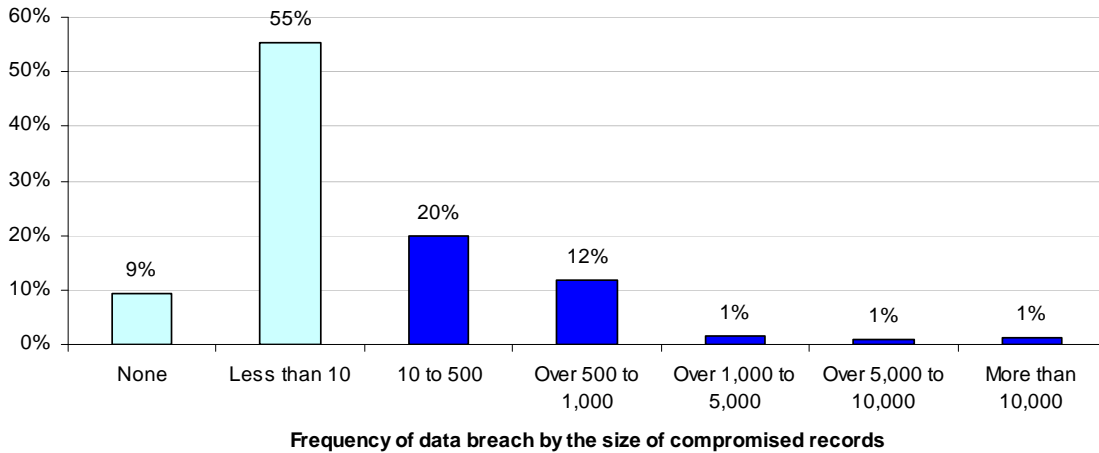
**Bar Chart 11  
Most responsible for HITECH compliance**



**7. Most respondents report their organizations experienced one or more data breach incidents involving the loss or theft of patient information during the past two years.**

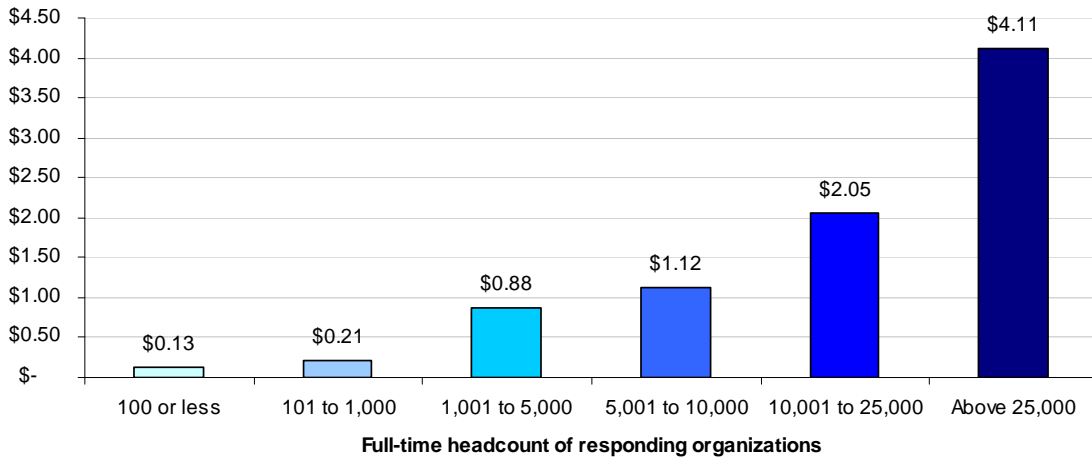
Ninety percent of respondents admit their organizations experienced one or more data breaches over the past two years involving the loss or theft of patient information. All covered entities in our study say their organizations had at least one breach involving one or more compromised records. Similarly, 80 percent of business associates admit to experiencing a data breach involving at least one or more compromised records. As noted in Bar Chart 12, the vast majority of data breach incidents involve small numbers of lost or stolen records – that is, a breach involving less than 10 records.

**Bar Chart 12**  
**Frequency of data breach incidents over a two-year period**



Bar Chart 13 reports the estimated cost of data breach incidents experienced by participating organizations according to full time equivalent headcount (as a surrogate for size). As expected, the estimated cost of data breach varies by organizational size. As shown, organizations with less than 100 employees experienced an average cost of \$130,000 and organizations with more than 25,000 employees experienced an average cost of \$4.1 million.

**Bar Chart 13**  
**Estimated cost of data breach incidents by organization headcount**  
 Cost figures reported with \$000,000 omitted

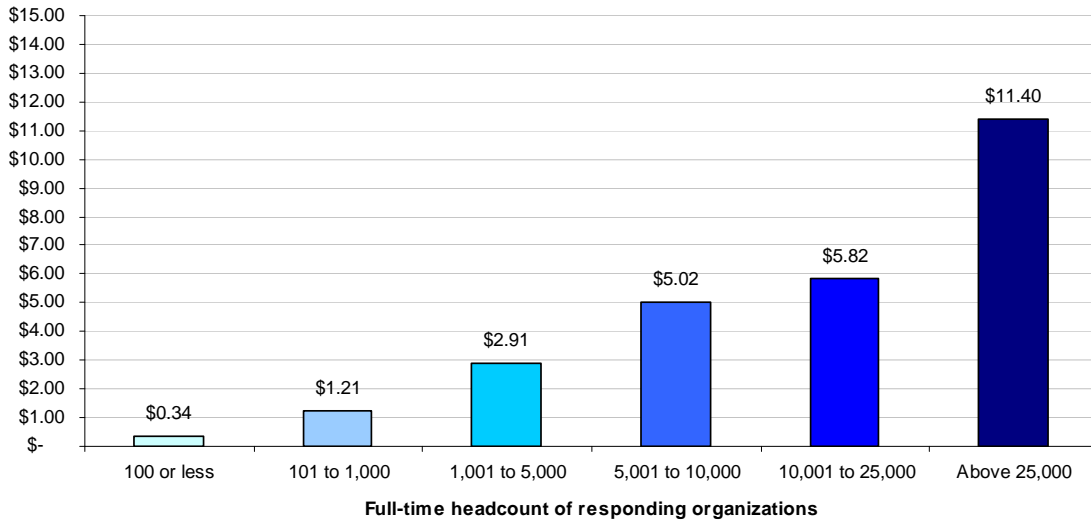


**8. Budgetary resources for HITECH compliance may be limited.**

Thirty-five percent of respondents believe that financial/budgetary pressures will significantly impact HIPAA/HITECH compliance requirements. Despite the importance of compliance in the healthcare industry, our results suggest that resources allocated may not be sufficient to achieve compliance goals. Specifically, the estimated average 2009 budget earmarked for all compliance efforts is \$3.9 million – of which HIPAA and HITECH is only a small portion (see Bar Chart 15).

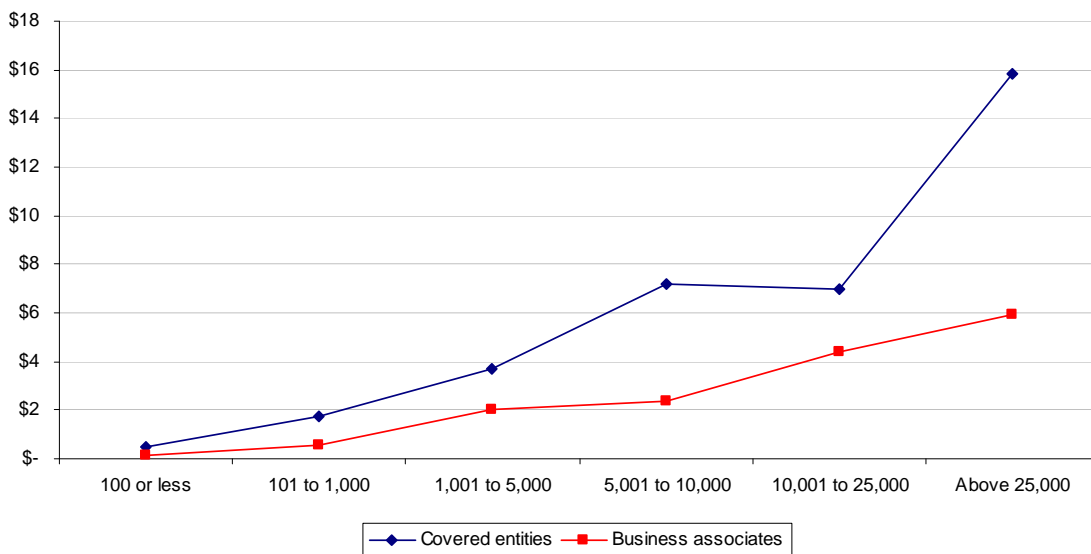
Bar Chart 14 reports the extrapolated compliance budget for 2009 according to organizational headcount. As can be seen, the average budget varies considerably from less than \$340,000 for organizations with less than 100 employees to \$11.4 million for organizations with more than 25,000 employees.

**Bar Chart 14**  
**Estimated cost of compliance budgets by organization headcount**  
 Cost figures reported with \$000,000 omitted



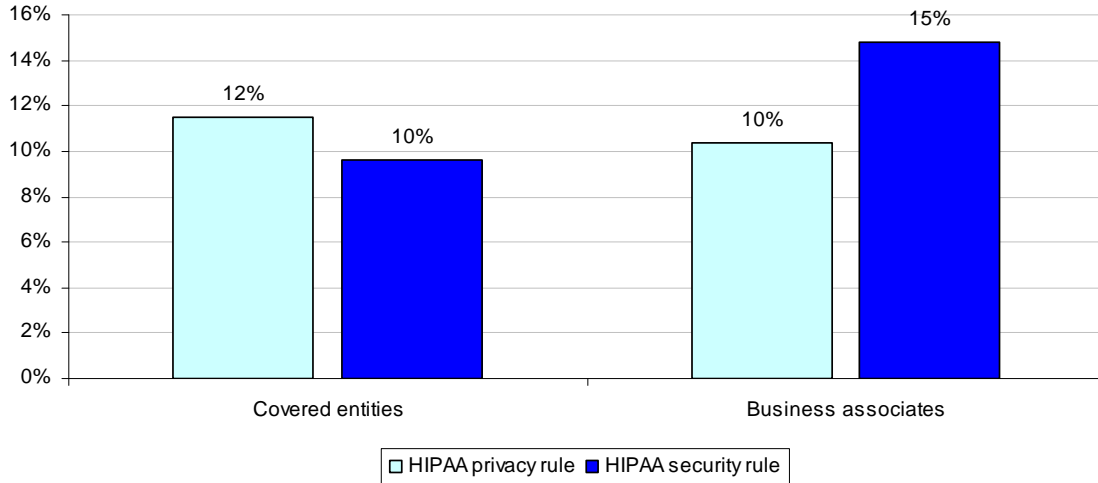
The following graph shows the differences between average budget amounts earmarked for compliance for covered entities and business associates by organizational headcount. As shown below, covered entities allocate considerably more resources for compliance than comparably sized business associates.

**Line Graph 1**  
**Extrapolated cost of compliance budgets for covered entities vs. business associates**  
 Cost figures reported with \$000,000 omitted



Approximately 11 percent of the 2009 compliance budget for the overall benchmark sample is earmarked to HIPAA privacy rule compliance requirements, and 12 percent is earmarked to HIPAA security rule compliance requirements. Bar Chart 15 shows differences in the percentage allocations to privacy and security compliance efforts. The chart shows business associates allocating a larger percentage of their budget to security rule compliance issues than covered entities (15 percent vs. 10 percent). In contrast, covered entities are allocating more resources to privacy compliance than business associates (12 percent vs. 10 percent).

**Bar Chart 15**  
**Privacy rule and security rule budget allocation for covered entities & business associates**



### III. Caveats

The presented findings are based on self-reported benchmark survey returns.<sup>2</sup> Usable returns from 77 organizations – or about 30 percent of those organizations 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 HIPAA compliance and readiness for the new HITECH Act.

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 organizations subject to HIPAA and the HITECH Act.

---

<sup>2</sup> The survey was developed with the assistance and input of Crowe Horwath. The final survey was reviewed by Fellows of Ponemon Institute as well as certain members of the RIM Council.

#### IV. Benchmark Methods

Table 1 summarizes the sample response over a seven-week period ending in October 2009. A total of 260 organizations were selected for participation and contacted by the researcher. Eighty-five organizations completed the benchmark survey, but eight of these instruments were incomplete and, hence, removed from the final benchmark pool. A final sample of 77 organizations (30% response rate) was used in our analysis.

Table 1: Description of the sample response	Freq.	Pct%
Healthcare providers	125	48%
Healthcare business associates	113	43%
Other organizations (including hybrids)	22	8%
Total organizations contacted	260	100%
Organizations completing the survey	85	33%
Incomplete surveys	8	3%
Benchmark sample	77	30%

Table 2 provides a detailed breakdown of our final sample. It shows the four largest segments: private healthcare providers (19 percent), public healthcare providers (19 percent), professional service companies (17 percent) and insurance companies (14 percent).

Table 2: Description of the benchmark sample	Freq.	Covered Entity	Business Associate
Private healthcare provider	15	15	
Public healthcare provider	13	13	
Professional services to healthcare organizations	13		13
Insurance company with health-related products	11	11	
Retail pharmacy	4		4
Vendors of public health record management systems	4		4
Other business associate	4		4
Public/government healthcare payer	3	3	
Employer with a self-funded health plan	3		3
Healthcare payment processor	3		3
Pharmaceutical	2		2
Medical device retailer and distributor	2		2
Total	77	42	35

Table 3 reports the approximate job titles of the primary individual representing the responding organization. As can be seen, the CISO is the most frequently cited job function or role.

Table 3: What is your approximate job title?	Freq.	Pct%
Chief information security officer	19	25%
Chief risk officer	11	14%
IT manager (general)	11	14%
Chief compliance officer	9	12%
Chief privacy officer	8	10%
Chief information officer	7	9%
HIPAA compliance leader	7	9%
Other	5	6%
Totals	77	100%

Pie Chart 1 reports the full-time equivalent headcount of organizations responding to the benchmark survey. As shown below, the largest segment includes healthcare organizations with headcount between 101 to 1,000 employees (23 percent). The second largest segment includes larger-sized organizations with headcount between 5,001 to 10,000 employees (21 percent).

**Pie Chart 1**  
**Headcount of participating healthcare organizations**

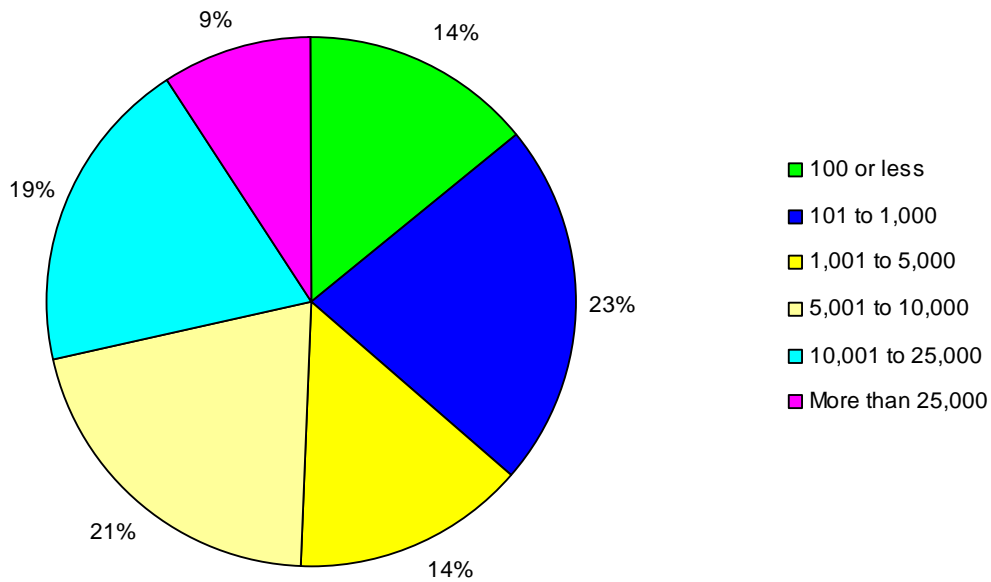


Table 4 reports the distribution of responding companies according to six geographic regions in the United States. The two largest regions are Northeast and Midwest, both at 27 percent of the overall sample, respectively.

Table 4: Geographic regions of participating organizations		
	Freq.	Pct%
Northeast	21	27%
Mid-Atlantic	9	12%
Midwest	21	27%
Southeast	7	9%
Southwest	9	12%
Pacific	10	13%
Total	77	100%

## V. Getting Ready for HITECH

Our study reveals that both covered entities and business associates face serious challenges in achieving substantial compliance with HIPAA privacy rule and security rule requirements. However, covered entities seem to be in a better position to achieve compliance with HIPAA and the new HITECH provisions.

Our study suggests HIPAA leaders in both privacy and security need to do a better job in making senior management aware of their organization's current program deficiencies. Accordingly, the lack of senior level support and buy-in is one reason why many organizations are unable to obtain sufficient resources for achieving compliance goals. In addition, respondents from participating organizations seem to be uncertain about what they need to do in order to achieve substantial compliance. Finally, many respondents are awaiting further analysis and guidance on new regulatory requirements before implementing program improvements.

This uncertainty can lead to difficulties in allocating resources appropriately and gaining senior management support. In addition to understanding HITECH compliance requirements, organizations need to determine specific gaps in their privacy and security compliance programs. Using the benchmark instrument in our study can help organizations make the right decisions as they get ready for HITECH.

In conclusion, our study suggests many healthcare organizations need to be more aggressive in managing compliance risk, in minimizing data breach of protected health information, and in avoiding regulatory risks. While many participating organizations appear to have mature HIPAA compliance programs (especially covered entities), there appears to be significant room for improvement especially on issues relating to risk assessment, training and policy dissemination.

We gratefully acknowledge the 77 healthcare organizations that participated in this inaugural benchmark study of HITECH Act readiness. We believe that this benchmark research will be helpful in identifying program gaps and areas for improvement among all organizations that are subject to the HIPAA privacy and security rules.

Please contact [research@ponemon.org](mailto: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.