



Electronic Health Information at Risk: A Study of IT Practitioners

Sponsored by LogLogic

Conducted by Ponemon Institute LLC

October 15, 2009

Electronic Health Information at Risk

Ponemon Institute, October 15, 2009

Executive summary

The *Electronic Health Information at Risk* study was conducted by Ponemon Institute and sponsored by LogLogic. The purpose of the study is to determine from IT practitioners¹ in healthcare organizations how secure they believe electronic patient health records are — especially those records stored in databases.

This topic is timely because of the new Health Information Technology for Economic and Clinical Health Act (HITECH). The Act offers incentives to encourage adoption of electronic health record (EHR) systems. It also expands the Health Insurance Portability and Accountability Act (HIPAA) rules for data security and privacy safeguards, including increased audits, enforcement and penalties. Among the provisions are the mandatory breach notification requirements that went into effect September 15, 2009.²

To better understand the risk to patient health records, we surveyed 542 IT practitioners (termed respondents) from healthcare organizations that collect patient health information in both paper and electronic format. Sixty-one percent of respondents are employed by healthcare providers, plans or insurance companies (HIPAA covered entities). The remaining 39 percent are employed by HIPAA business associates or hybrid organizations.

The majority of IT practitioners in our study believe their organizations do not have adequate resources to protect patients' sensitive or confidential information. Following are the most salient findings of this survey research. Please note that most of the results are displayed in bar chart or table formats. The actual data utilized in each figure and referenced in the paper can be found in the percentage frequency tables attached in Appendix 1.

The survey addressed the following topics:

- The adequacy of the organization's approach to the security of health information.
- Senior management's views about the importance of securing health information.
- How electronic health information is used by the organization.
- The database applications that cause the most risk to health information and the difficulty in securing health information in databases.
- Steps taken to secure health information in databases and their effectiveness.
- The impact of compliance on the security of electronic health information.

Lack of resources and support from senior management is putting electronic health information at risk.

Bar Chart 1 shows 61 percent of IT practitioners surveyed believe they do not have enough resources to ensure privacy and data security requirements are met. In addition, 70 percent say senior management does not view privacy and data security as a top priority.

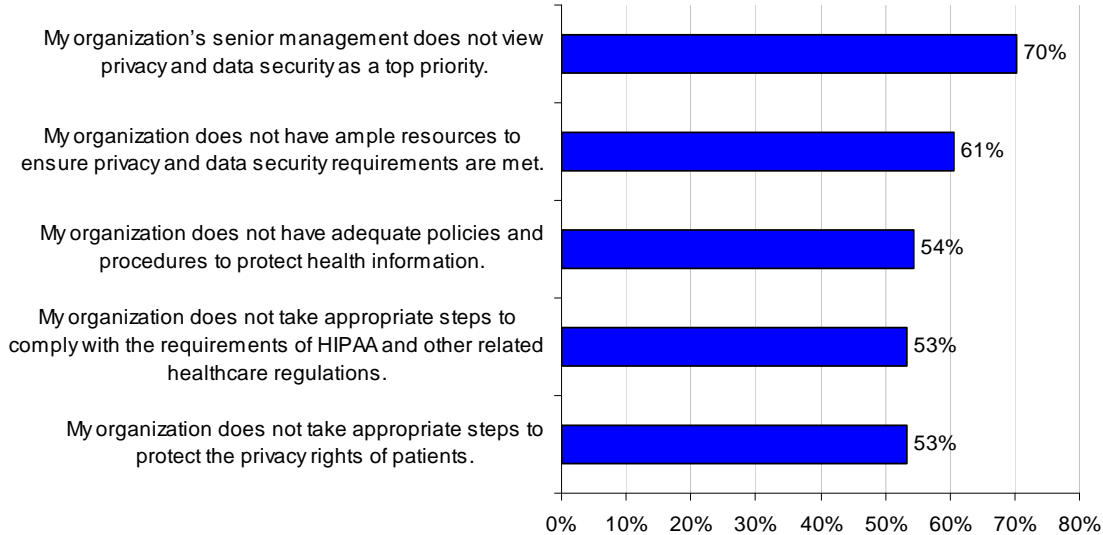
Perhaps given resource constraints and the lack of executive support, it is understandable that 53 percent of respondents do not believe their organization takes appropriate steps to protect the privacy rights of patients and to comply with the requirements of HIPAA and other related

¹ IT practitioners included in the sample include those individuals responsible for HIPAA programs. The sample also included security practitioners who are mostly located in their organization's IT department.

² Federal Trade Commission, 16 CFR Part 318, Health Breach Notification Rule, August 25, 2009.

healthcare organizations. Fifty-four percent believe they have adequate policies and procedures to protect health information.

Bar Chart 1
Attributions about participating healthcare organizations



Attributions are reverse scored. Each bar reflects the strongly agree, agree and unsure response using a five point adjective scale.

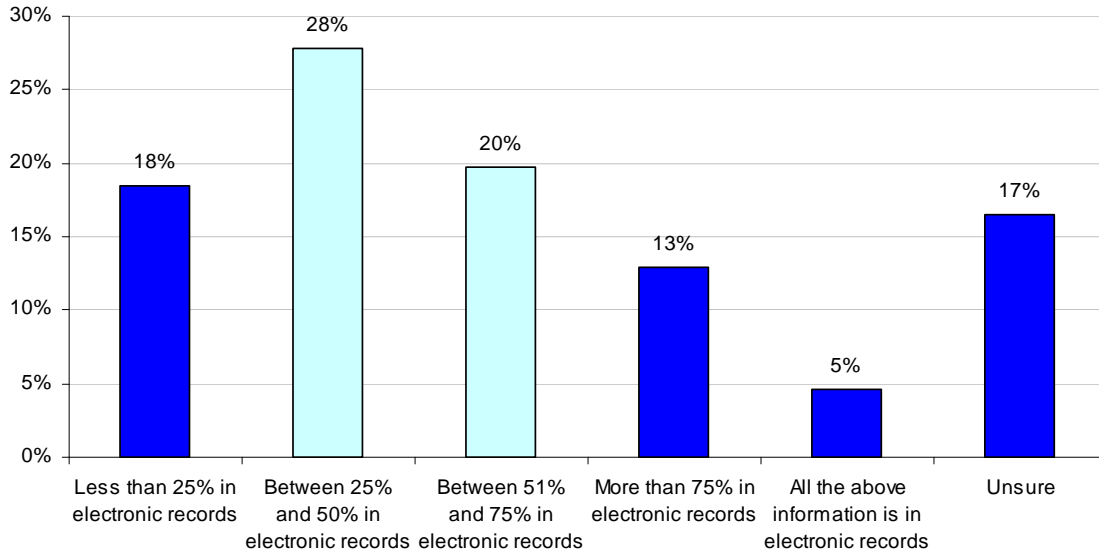
Databases contain more than half of organizations' electronic health information.

The following table reports the types of personal data routinely collected by healthcare organizations. As can be seen, the most frequently collected personal data are the patient's name, address, telephone, age, gender, certain physical characteristics, personal health history and family health history. Less frequently collected personal data elements include credit history, religion and ethnicity.

Table 1: Twenty-six data elements that healthcare organizations may collect and store about patients in electronic files or records.			
Data types	Pct%	Data types	Pct%
Name	99%	Health insurance information	58%
Gender	98%	Social Security Number	52%
Address	96%	Prescription drugs	38%
Telephone	96%	Educational background	34%
Personal health history	95%	Race	31%
Family health history	92%	Addictions	31%
Age	92%	Interest in clinical trial research	29%
Physical characteristics	90%	Sexual preferences	26%
Employer	80%	Photo	23%
Guardian or next of kin	76%	Diet	20%
Marital status	75%	Credit history	16%
Credit card or bank payment information	74%	Religion	15%
Names of primary health care provider	62%	Ethnicity	13%

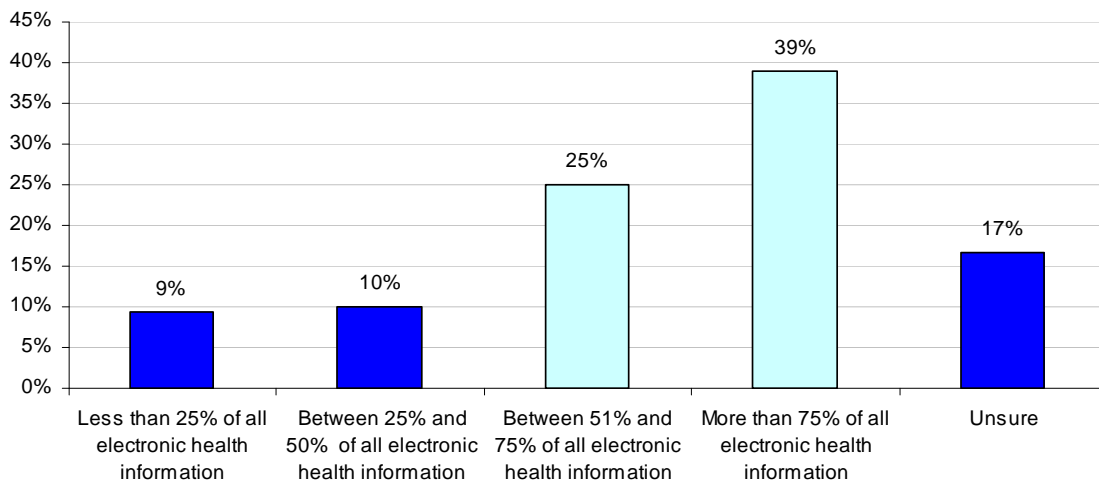
Bar Chart 2 shows that almost half (48 percent) report that between 25 percent and 75 percent of the data collected by healthcare companies is in electronic format versus paper documents.

Bar Chart 2
Percentage of electronic vs. paper documents containing patient health information



Bar Chart 3 shows 64 percent of respondents report that more than half of their organization's electronic health information is stored in databases rather than unstructured data files such as documents, spreadsheets, emails and so forth. Thus, while unstructured data and insecure endpoints present high risk to healthcare organizations, the prime culprit of major data breaches in the healthcare space is likely to result from insecure database activities.

Bar Chart 3
Percentage of electronic health information stored in databases

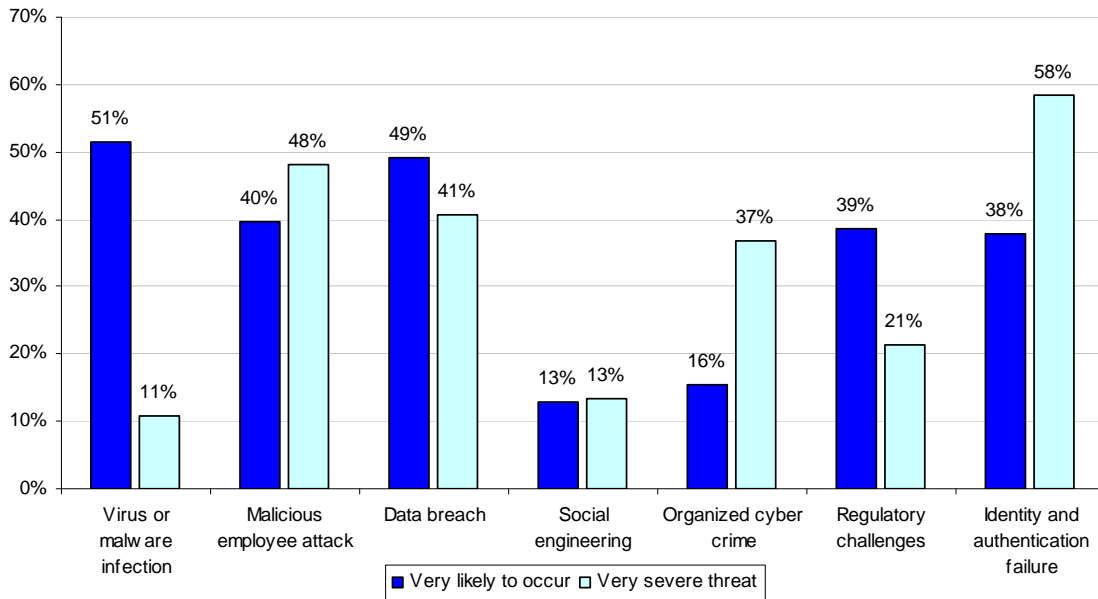


Respondents are concerned about their organization's ability to safeguard electronic health information in databases.

According to the IT practitioners in our study, the top three emerging threats affecting an organization's ability to secure electronic health information are: virus or malware infections, the

loss of patient data (a.k.a. data breach), and malicious employee attacks. Of these threats that are most likely to occur and most severe are: identity and authentication failures, data breach and malicious employee attacks.³ Threats that do not appear to cause significant concerns for respondents are: social engineering, regulatory challenges and organized cyber crime.

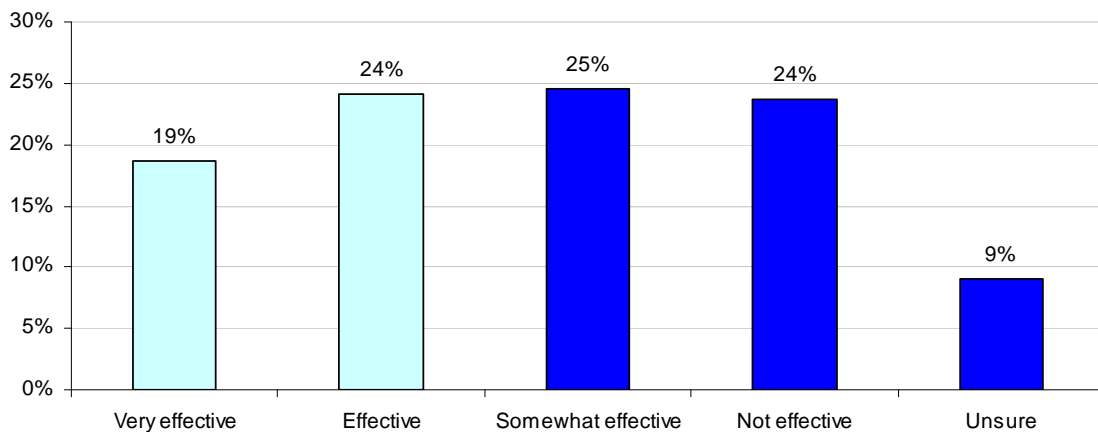
Bar Chart 4
Likelihood and severity of seven security threats to electronic health information



Protection of EPHI is focused on policies and procedures, anti-malware/anti-virus and training. Many do not think their approaches are effective.

Bar Chart 5 shows only 43 percent believe the measures their organizations have in place are either very effective or effective.

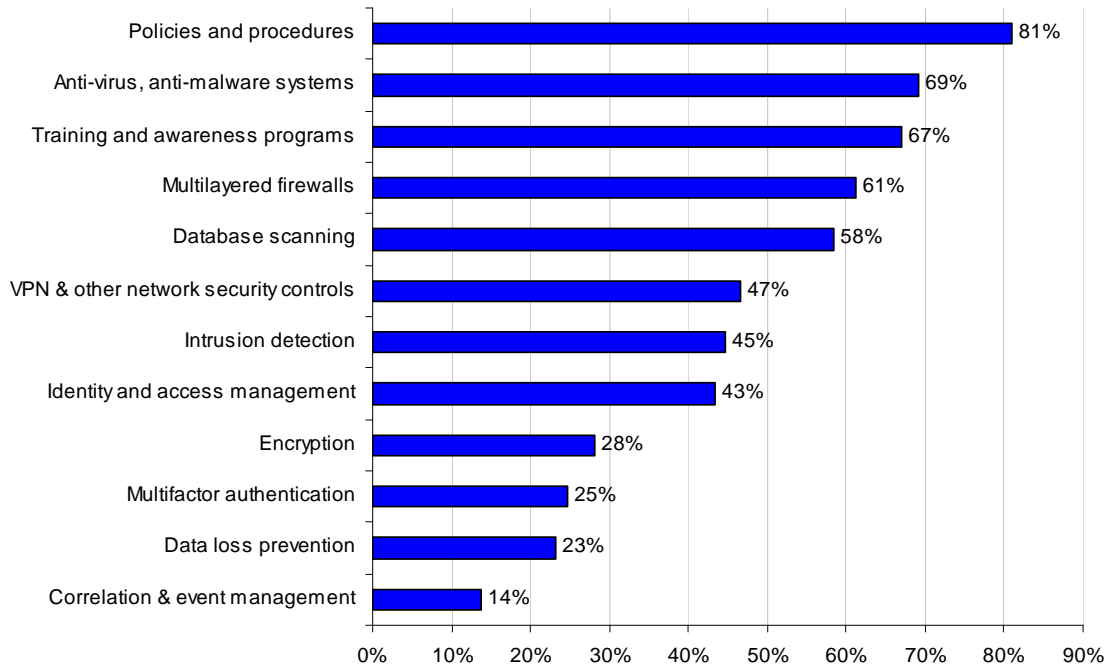
Bar Chart 5
Effectiveness of existing security measures



³ It is interesting to see that virus or malware infections, while high on the likelihood scale, score low on severity. See Ponemon Institute's recent report entitled *Anatomy of Data-Stealing Malware* (October 2009), which shows that the malware threat may be significantly underestimated by IT and IT security practitioners.

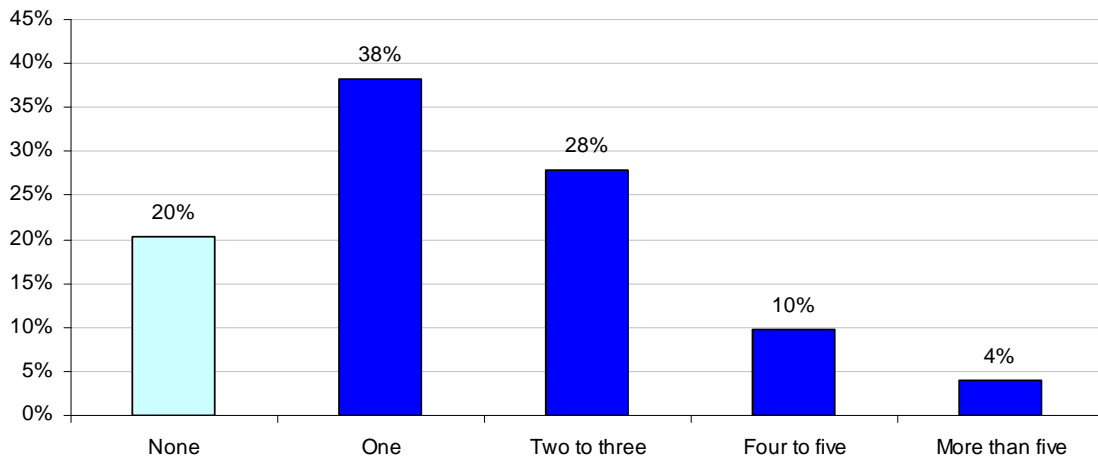
Bar Chart 6 shows the ways organizations attempt to secure and protect electronic health information. The most frequently cited security measures are: policies and procedures, anti-virus and anti-malware systems, training and awareness programs and perimeter controls such as multilayered firewalls. Least used are correlation and event management systems and data loss prevention solutions (DLP). Given that one of the most significant threats concerns data breach, it is surprising to see that DLP solutions are so infrequently used by healthcare organizations.

Bar Chart 6
Security measures used by healthcare organizations



A majority of respondents say their organizations had one or more data breaches that involved the loss of patient health information.

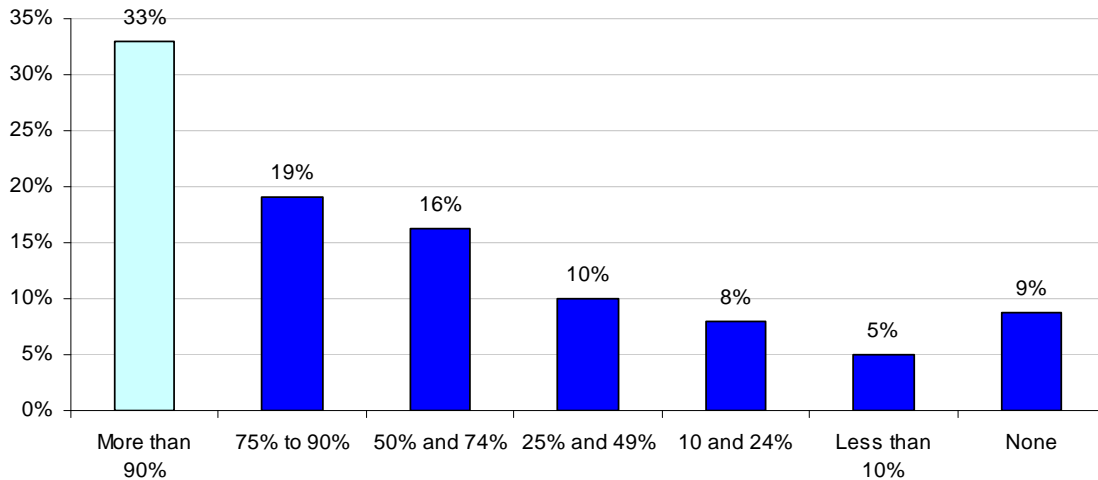
Bar Chart 7
Frequency of data breach experience



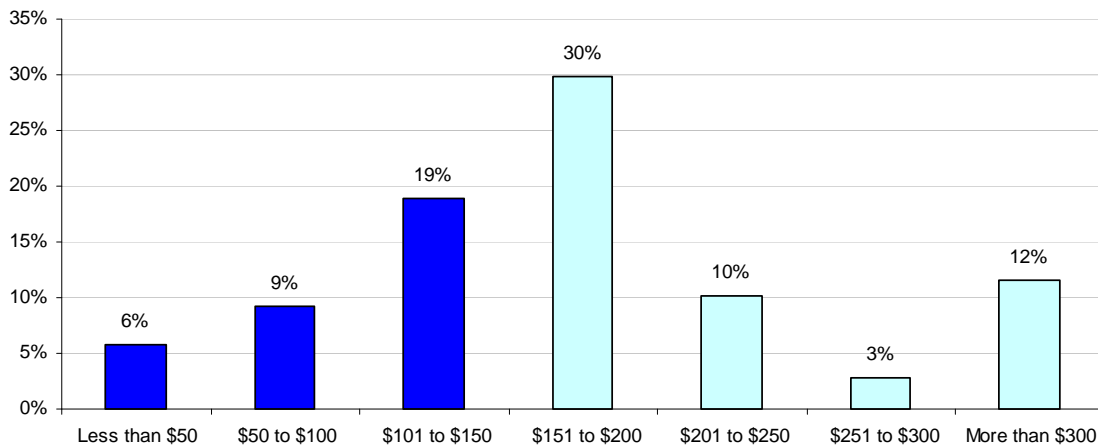
Bar Chart 7 shows that only 20 percent of respondents report their organizations did not have a data breach involving the loss or theft of electronic patient health information.

Of those that had a data breach, 33 percent of respondents say more than 90 percent of their organization's data breach involved electronic health information stored on databases.

Bar Chart 8
Percentage of data breaches involving electronic health information on databases



Bar Chart 9 shows the estimated value of the cost of a data breach on a per compromised record basis. As can be seen, 55 percent of respondents say the cost of a lost or stolen compromised record is more than \$150. The extrapolated average value (not shown in the graph) is \$211.⁴



⁴ This estimated average value is close to the \$202 average cost associated with a compromised record reported in Ponemon Institute's [Annual Cost of Data Breach](#) report (January 2009).

Method

A random sampling frame of 7,888 individuals employed in the healthcare industry who reside within the United States was used to recruit participants. Our randomly selected sampling frame was selected from national lists of IT practitioners. In total, 781 surveys were completed and 155 were rejected because of reliability criteria. The final sample includes 626 usable returns which represents a 4.9 percent net response rate.

Table 2: Sampling Frame	Freq	Pct%
IT, IT compliance and security panels (combined)	12,888	100.0%
Sent to subject	10,502	81.5%
Bounce backs	1369	10.6%
Returns	781	6.1%
Rejects	155	1.2%
Net returns	626	4.9%

Two screening questions were used to ensure respondents worked in organizations that routinely collected, used or stored electronic patient health information. The sample size after screening questions was 599 individuals.

Ninety-one percent of respondents completed all survey items within 15 minutes. Table 3 reports the respondent's organizational level. As can be seen, a majority of respondents are at or above the supervisory level. The average experience for respondents is 11.9 years.

Table 3: Organizational level that best describes the respondents' position	Pct%
Senior Executive	0%
Vice President	0%
Director	20%
Manager	31%
Supervisor	10%
Associate/Staff	14%
Technician	24%
Other	1%
Total	100%

Table 4 reports the respondents' primary reporting channels. As can be seen, a large number of respondents report through the IT organization (CIO or CTO) rather than compliance, security or risk management.

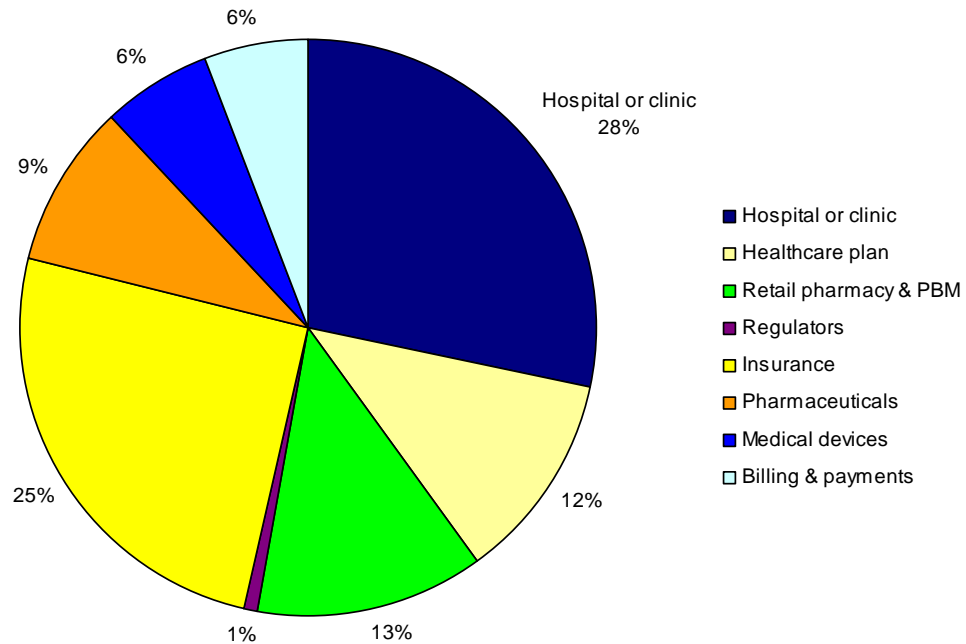
Table 4: Respondent's reporting channel or chain of command.	Pct%
Chief Financial Officer	3%
Legal or General Counsel	12%
Chief Information Officer (CIO)	40%
Compliance Officer	16%
Medical Officer	2%
Chief Technology Officer (CTO)	8%
Human Resources VP	5%
Chief Security Officer	10%
Chief Risk Officer	4%
Total	100%

Table 5 reports the respondent organization's headcount. As shown, a majority of respondents work within companies with more than 1,000 employees.

Table 5: Headcount of respondents' organizations	Pct%
Less than 100 people	10%
101 to 500 people	9%
501 to 1,000 people	13%
1,001 to 5,000 people	20%
5,001 to 10,000 people	14%
10,001 to 25,000 people	23%
More than 25,000 people	11%
Total	100%

Pie Chart 1 reports the percentage distribution of respondents by healthcare organization type. As shown below, 28 percent of respondents work for hospitals or clinics. More than 25 percent of respondents are employed by insurance organizations.

Pie Chart 1
Percentage distribution of respondents by organizational type



Caveats to this study

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

- **Non-response bias**: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.
- **Sampling-frame bias**: The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT practitioners involved in their organization's HIPAA program. We also acknowledge that the results may be biased by external events such as media coverage. We also acknowledge bias caused by compensating subjects to complete this research within a holdout period. Finally, because we used a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would result in a different pattern of findings.
- **Self-reported results**: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that respondents did not provide truthful responses.

Conclusion

Many healthcare organizations are facing new rules and regulations for the protection of electronic health information. However, IT practitioners' responses to this survey suggest they are skeptical that these regulations will affect the security of electronic patient data. According to our findings, the lack of resources and support from senior management may be putting electronic health information at risk.

While much of the recent security focus has been on insecure endpoints and networks, our study suggests that databases contain much of the electronic personal health information that puts healthcare organizations at risk. Further, many healthcare organizations have had a data breach that involved health information stored in a database. Respondents acknowledge that the cost of these data breaches can be very costly and possibly harmful to their reputation.

Securing electronic health information from a variety of threats including malicious employees and data breach is likely to be a challenge for many healthcare organizations. While these organizations seem to focus on policies and procedures, training and perimeter controls, without resources and support from senior management, preventing the loss of data may be very difficult. We recommend that organizations pursue a strategy of assigning accountability for the protection of electronic health information, appropriate technology to prevent the insider threat (such as DLP solutions) and senior management buy-in for the necessary resources to get the job done right.

Appendix 1: Percentage Survey Responses

Audited Findings Presented by Dr. Larry Ponemon. Fieldwork ended on August 28, 2009

The following table summarizes the sample results. As can be seen, 626 individuals participated in the study (or a 4.9% response rate).

Sampling Frame	Freq	Pct%
IT, IT compliance and security panels (combined)	12,888	100.0%
Sent to subject	10,502	81.5%
Bounce backs	1369	10.6%
Returns	781	6.1%
Rejects	155	1.2%
Net returns	626	4.9%

Respondents were asked to respond to two screening questions, defined as S1a and S1b. The final sample was reduced to 542 individuals, which includes those who said "Yes" to S1a and who did not select "Only paper" in S1b.

S1a. Does your organization collect, use, store or share health information?	Freq	Pct%
Yes	599	95%
No (stop)	32	5%
Total	631	100%

S1b. If yes, in what format is this information collected?	Freq	Pct%
Only paper (stop)	57	10%
Only electronic	141	24%
Both	401	67%
Total	599	100%

The following tables summarize the results of all survey questions in a percentage frequency format. The tables that sum to more than 100 percent pertain to questions that permitted more than one response.

Q1. Please respond to each statement about <u>your</u> organization using this five-point scale to express your opinion: ⁵ 1=Strongly agree, 2=Agree, 3=Unsure, 4=Disagree, 5=Strongly disagree.	Strongly agree & Agree (Combined)
My organization has adequate policies and procedures to protect health information.	46%
My organization takes appropriate steps to protect the privacy rights of patients.	47%
My organization takes appropriate steps to comply with the requirements of HIPAA and other related healthcare regulations.	47%
My organization's senior management views privacy and data security as a top priority.	30%
My company has ample resources to ensure privacy and data security requirements are met.	39%
Average	42%

⁵ Please note that the Q1 responses are reverse scored in the analysis of survey findings.

Q2. Following is a list of 26 data elements that healthcare organizations may collect and store about patients in electronic files or records. Please select all the data elements your organization routinely collects.	Pct%
Name	99%
Address	96%
Telephone	96%
Age	92%
Gender	98%
Race	31%
Religion	15%
Ethnicity	13%
Sexual preferences	26%
Physical characteristics such as weight, height	90%
Family health history	92%
Guardian or next of kin	76%
Personal health history	95%
Photo	23%
Prescription drugs	38%
Diet	20%
Addictions	31%
Employer	80%
Marital status	75%
Interest in clinical trial research	29%
Names of primary health care provider	62%
Social Security Number	52%
Health insurance information	58%
Educational background	34%
Credit card or bank payment information	74%
Credit history	16%
Average	58%

Q3. How is the above electronic health information used by your organization? Please check all that apply.	Pct%
Billing & payments	67%
Insurance verification	60%
Patient care (clinical)	53%
Diagnostics & testing	40%
Marketing & communications	58%
Patient relations	54%
Research	36%
Compliance	24%
Education and training	10%
Other (please specify)	4%
Average	41%

Q4. Approximately, what percentage of the above information is in electronic versus paper files?	Pct%
Less than 25% in electronic records	18%
Between 25% and 50% in electronic records	28%
Between 51% and 75% in electronic records	20%
More than 75% in electronic records	13%
All the above information is in electronic records	5%
Unsure	17%
Total	100%

Q5. Approximately, how much of the electronic health information used in your organization is stored in a database?	Pct%
Less than 25% of all electronic health information	9%
Between 25% and 50% of all electronic health information	10%
Between 51% and 75% of all electronic health information	25%
More than 75% of all electronic health information	39%
Unsure	17%
Total	100%

Q6. What kinds of database applications cause the most risk to electronic health information? Please rank the following three selections from 3 = most risk to 1 = least risk.	Average Rank
Administrative applications such as patient scheduling systems	1.9
Business applications such as billing and insurance processing	2.5
Clinical applications such as physician notes, prescriptions or diagnostic reports	1.6
Average	2.0

Q7a. What do you see as emerging data security threats that may affect your organization's ability to secure electronic health information contained in databases over the next 12 to 24 months?	Very likely	Likely	Not likely
Inability to prevent attacks by organized cyber criminals	16%	17%	67%
Inability to meet regulatory compliance requirements	39%	50%	11%
Loss of patient trust because of a data breach	49%	37%	14%
Increased social engineering or pre-texting	13%	19%	68%
Malicious employee attacks	40%	34%	27%
Virus or malware infection and infiltration into databases	51%	37%	12%
Inability to manage identity and authentication	38%	60%	2%
Average	35%	36%	29%

Q7b. How severe are the data security threats mentioned above with respect to your organization's ability to secure electronic health information contained in databases?	Very severe	Severe	Not severe
Inability to prevent attacks by organized cyber criminals	37%	52%	11%
Inability to meet regulatory compliance requirements	21%	36%	43%
Loss of patient trust because of a data breach	41%	53%	6%
Increased social engineering or pre-texting	13%	40%	46%
Malicious employee attacks	48%	50%	2%
Virus or malware infection and infiltration into databases	11%	42%	47%
Inability to manage identity and authentication	58%	32%	10%
Average	33%	44%	23%

Q8a. What is your organization doing today to protect electronic health information contained in databases?	Pct%
Training and awareness programs for everyone who accesses the database	67%
Policies and procedures including an incident response plan	81%
VPN, gateway or other network security controls	47%
Encryption for data at rest and data in motion	28%
Perimeter controls such as multilayered firewalls	61%
Data loss prevention tools	23%
Intrusion detection systems	45%
Anti-virus, anti-malware systems	69%
Correlation and event management systems	14%
Database scanning solutions	58%
Identity and access management solutions	43%
Multifactor authentication	25%
Other (please specify)	2%
Total	564%

Q8b. How would you rate the effectiveness of the above mentioned data security measures you have in-place for securing electronic health information in databases?	Pct%
Very effective	19%
Effective	24%
Somewhat effective	25%
Not effective	24%
Unsure	9%
Total	100%

Q9a. How many data breaches involving the loss or theft of electronic health information has your organization experienced in the past 12 months?	Pct%
None	20%
One	38%
Two to three	28%
Four to five	10%
More than five	4%
Total	100%
Point estimate	1.75

Q9b. How many of the above data breaches experienced by your organization involved electronic health information stored in a database?	Pct%
More than 90%	33%
Between 75% to 90%	19%
Between 50% and 74%	16%
Between 25% and 49%	10%
Between 10 and 24%	8%
Less than 10%	5%
None	9%
Total	100%
Point estimate	0.63

Q9c. Was your organization required to publicly disclose the data breach to data breach victims?	Pct%
Yes, for all data breach incidents experienced	23%
Yes, for some data breach incidents experienced	45%
No, disclosure was not necessary	32%
Total	100%
Q9d. If your organization had a data breach involving the loss or theft of patient health information (say 1,000 or more records), what would this incident cost your company on a per lost record basis?	Pct%
Less than \$50	6%
Between \$50 to \$100	9%
Between \$101 to \$150	19%
Between \$151 to \$200	30%
Between \$201 to \$250	10%
Between \$251 to \$300	3%
Between \$301 to \$350	0%
Between \$351 to \$400	0%
Between \$401 to \$450	0%
Between \$451 to \$500	0%
Between \$501 to \$1,000	10%
More than \$1,000	2%
Don't know	12%
Total	100%
Point estimate (cost per compromised record)	\$ 211.30
Q10a. How familiar are you with the new HITECH Act?	Pct%
No knowledge	6%
Not familiar	30%
Familiar (Go to Q10b)	53%
Very familiar (Go to Q10b)	11%
Total	100%

Q10b. Approximately (gut feel is okay), what is the estimated cost range that best describes what your organization will incur to comply with the HITECH Act for protecting electronic health information?	Pct%
No cost required	3%
Less than \$1 million	10%
Between \$1 to 2 million	11%
Between \$2 to \$5 million	12%
Between \$5 to \$10 million	29%
Between \$10 to \$15 million	18%
Between \$15 to \$20 million	5%
Between \$20 to \$25 million	0%
Between \$25 to \$30 million	0%
Between \$35 to \$40 million	0%
Between \$45 to \$50 million	2%
Between \$55 to \$60 million	2%
More than \$60 million	0%
Don't know	7%
Total	100%
Point estimate	\$ 8.22

Q10c. Approximately (gut feel is okay), what percentage of the 2009-2010 data protection budget is dedicated to compliance with the HITECH Act?	Pct%
Less than 5%	25%
Between 5% to 10%	29%
Between 10% to 20%	32%
Between 20% to 30%	11%
Between 30% to 40%	2%
Between 40% to 50%	1%
Between 50% to 60%	1%
Between 60% to 70%	0%
Between 70% to 80%	0%
Between 80% to 90%	1%
More than 90%	0%
Total	100%
Point estimate	12%

Q10d. What statement best describes your belief about how compliance with HIPAA and the new HITECH Act affects the security of electronic health information in your organization?	Pct%
Compliance will increase the security of electronic health information	39%
Compliance will decrease the security of electronic health information	1%
Compliance will have no affect on the security of electronic health information	60%
Total	100%

Demographics and Organizational Characteristics

D1. What organizational level best describes your current position?	Pct%
Senior Executive	0%
Vice President	0%
Director	20%
Manager	31%
Supervisor	10%
Associate/Staff	14%
Technician	24%
Other	1%
Total	100%

D2. Is this a full time position?	Pct%
Yes	95%
No	5%
Total	100%

D3. Check the Primary Person you or your IT security leader reports to within the organization.	Pct%
Chief Financial Officer	3%
Legal or General Counsel	12%
Chief Information Officer (CIO)	40%
Compliance Officer	16%
Medical Officer	2%
Chief Technology Officer (CTO)	8%
Human Resources VP	5%
Chief Security Officer	10%
Chief Risk Officer	4%
Total	100%

D4. Total years of experience	Pct%
Total years of security experience	11.9
Total years in current position	5.2

D5. Gender:	Pct%
Female	40%
Male	60%
Total	100%

D6. What best describes your organization's healthcare industry focus?	Pct%
Hospital or clinic	48%
Healthcare plan	20%
Retail pharmacy & PBM	21%
Regulators	2%
Insurance	42%
Pharmaceuticals	16%
Medical devices	10%
Billing & payments	10%
Total	169%

D7. What is the worldwide headcount of your organization?	Pct%
Less than 100 people	10%
101 to 500 people	9%
501 to 1,000 people	13%
1,001 to 5,000 people	20%
5,001 to 10,000 people	14%
10,001 to 25,000 people	23%
More than 25,000 people	11%
Total	100%

Please contact research@ponemon.org or call us at 231.938.9900 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.