Part I
Ponemon Institute Study:
Data Security in Small Healthcare Organizations

Part II (Starting on Page 34)
MegaPath White Paper:
Managed Network Security for Healthcare

Data Security in Small Healthcare Organizations

Sponsored by MegaPath

Independently conducted by Ponemon Institute LLC

Publication Date: November 30, 2011

Data Security in Small Healthcare Organizations

Ponemon Institute, November 30, 2011

Part 1. Introduction

Small healthcare organizations such as offices of physicians and dentists, home healthcare services, health clinics and nursing care facilities are obligated to protect patient health information and comply with the requirements of U.S. Health Insurance Portability and Accountability Act (HIPAA) and other related healthcare regulations. Failure to comply with HIPAA can result in fines ranging from $100 to $50,000 per violation up to an annual maximum of $1.5 million, depending on the organization's lack of reasonable diligence and the nature of harm resulting from the violation.

In achieving compliance with regulations, the challenge these small providers face is that they are less likely to have dedicated personnel, such as a chief security officer or chief information security officer, to manage the development and implementation of the security and privacy policies and procedures for the organization. Further, they may not have the budget to purchase the enabling technologies critical to safeguarding patient information.

A Small Healthcare Horror Story

A speculator bid $4,000 for the patient records of a family practice in South Carolina. Among the businessman's uses of the purchased records was selling them back to the former patients.

Source HHS: 65 Fed. Reg.82467 (28 Dec.2000)

Data Security in Small Healthcare Organizations was conducted by Ponemon Institute and sponsored by MegaPath to understand the unique problems faced by smaller organizations and their ability to safeguard patient health information. The study surveyed 708 IT and administrative practitioners working in organizations with 250 or fewer employees. All organizations represented in this study use and have access to patient health information and are required to comply with HIPAA. Respondents in our study have an average of 10.5 years of relevant experience.

The following are some of the most salient findings from this study:

- Ninety-one percent have had at least one data breach and 23 percent say their organizations experienced at least one patient medical identity theft incident.
- Seventy percent of respondents agree that their organizations do not have or are unsure their organizations have sufficient funding to achieve proper governance, risk management and compliance requirements.
- Thirty-five percent of respondents say no one person has overall responsibility for protecting patient health information.
- Patient information is most often in paper documents as opposed to electronic storage.
- Governance and control procedures are considered more effective than the technologies they currently use.
- Approximately half of respondents (48 percent) say less than 10 percent of their organizations' budget or annual spending is dedicated to data security technologies.

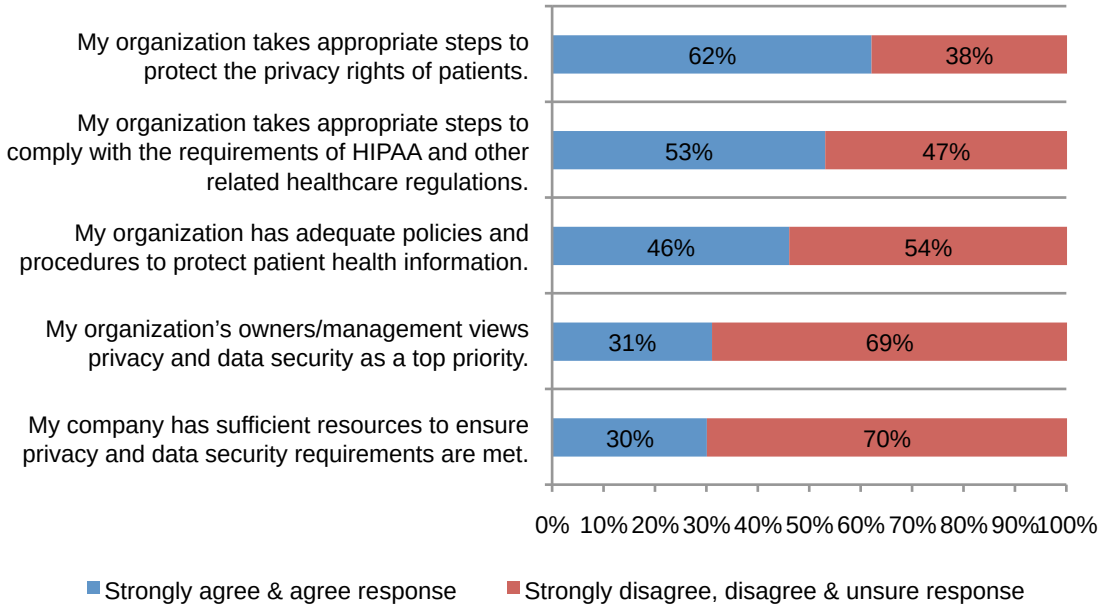
In the following section, we discuss the key findings. They are organized according to the following four topics: perceptions about organizations' ability to safeguard patient information, barriers to achieving a strong security posture, patient data most at risk, technology and control activities to mitigate data security threats and frequency of data breaches and medical identity theft.

Part 2. Key Findings

We have organized the key findings according to the following four topics: perceptions about organizations' ability to safeguard patient information and barriers to achieving a strong security posture, patient health data used and what puts it at risk, effectiveness of technology and control activities to mitigate data security threats and the affect data breaches and medical identity theft have on small healthcare organizations.

Respondents' hold unfavorable perceptions about patient security in their organizations.[1] As shown in Bar Chart 1, the majority of respondents agree their organization takes appropriate steps to protect the privacy rights of patients and that it takes the appropriate steps to comply with the requirements of HIPAA and other related healthcare regulations. However, less than one-third (31 percent) agrees that their organizations' management views privacy and data security as a top priority and 70 percent agree that it does not have sufficient resources to ensure privacy and data security requirements are met.

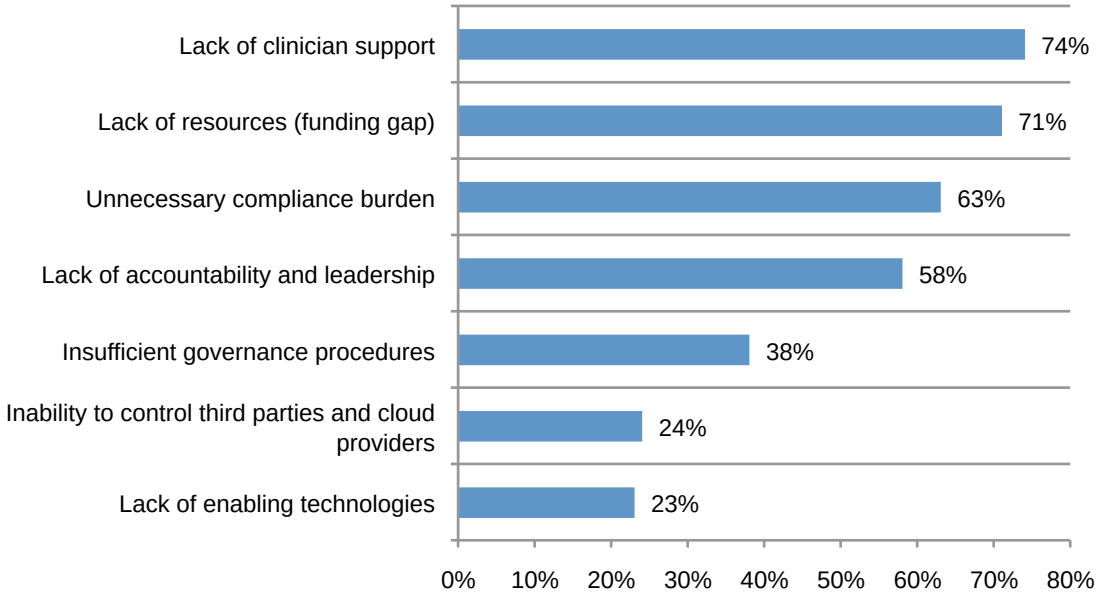
Bar Chart 1. Perceptions about patient privacy and security in small healthcare organizations
Five-point scale from strongly agree to strongly disagree



[1]Attributions are framed using a five-point adjective scale from strongly agree to strongly disagree. An unfavorable response is defined as a combined strongly agree and agree response that is less than 50 percent.

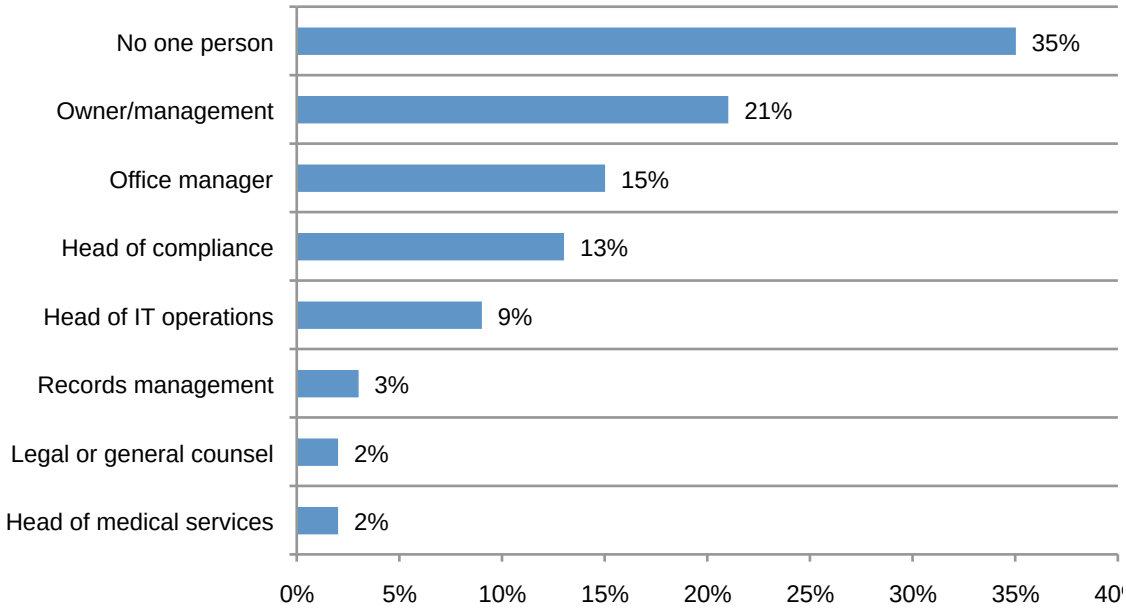
Barriers to a strong security posture. The most significant barriers to achieving a strong privacy and data security posture with respect to patient health information collected, used and retained by organizations according to Bar Chart 2 are a lack of clinician support, lack of resources and unnecessary compliance burdens to achieve the goal of safeguarding patients' sensitive and confidential information. However, a lack of enabling technologies and inability to control third parties, including cloud-computing providers are not considered by the majority of respondents to be as significant a barrier.

Bar Chart 2. What are the most significant barriers to achieving a strong privacy and data security posture with respect to patient health information collected, used and retained by your organization?
Check all that apply



Who is in charge of the security of patient information? While small healthcare providers are less likely to have dedicated security and privacy personnel, HIPAA does require each entity to identify the individual who is ultimately responsible for the development and implementation of the security and privacy policies and procedures for the organization. According to Bar Chart 3, 35 percent of respondents say no one person has overall responsibility for protecting patient health information. Twenty-one percent say the owner or key management of the organization is responsible. Only 9 percent say the head of IT operations has responsibility.

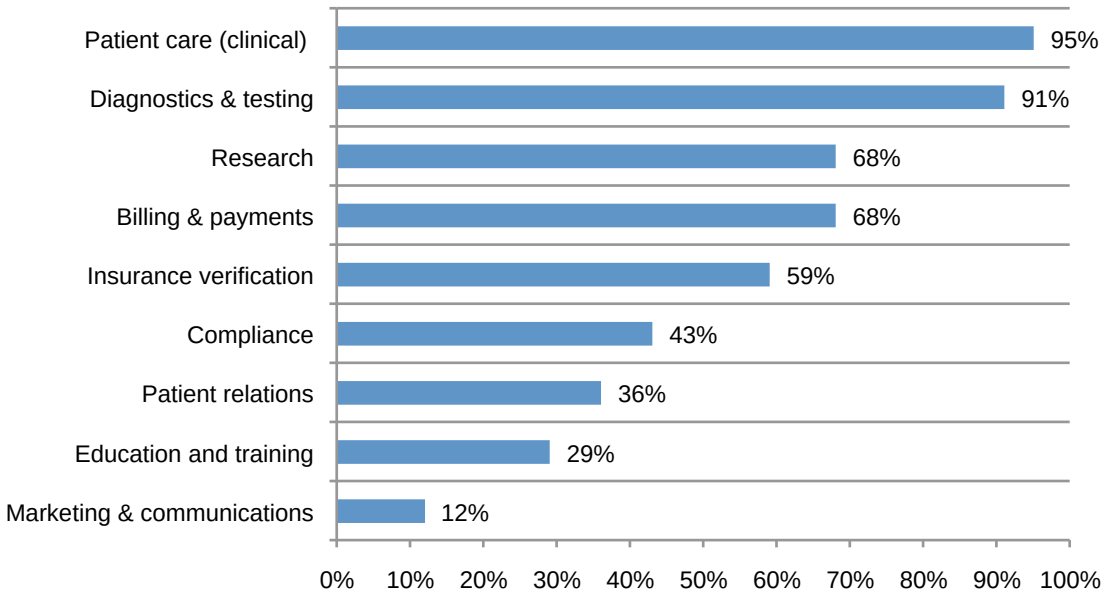
Bar Chart 3. Who within your organization is most responsible for protecting of patient health information?



Patient health information used by organizations and what puts this information at risk. Medical information is among the most sensitive types of personal information. The small healthcare organizations participating in the study agree and have ranked what they consider to be the most sensitive information that may be collected and stored about patients in files or records. These include information about addictions, participation in clinical trials, medications, sexual orientation and health history. A complete listing of the types of sensitive information is shown in the Appendix to this paper.

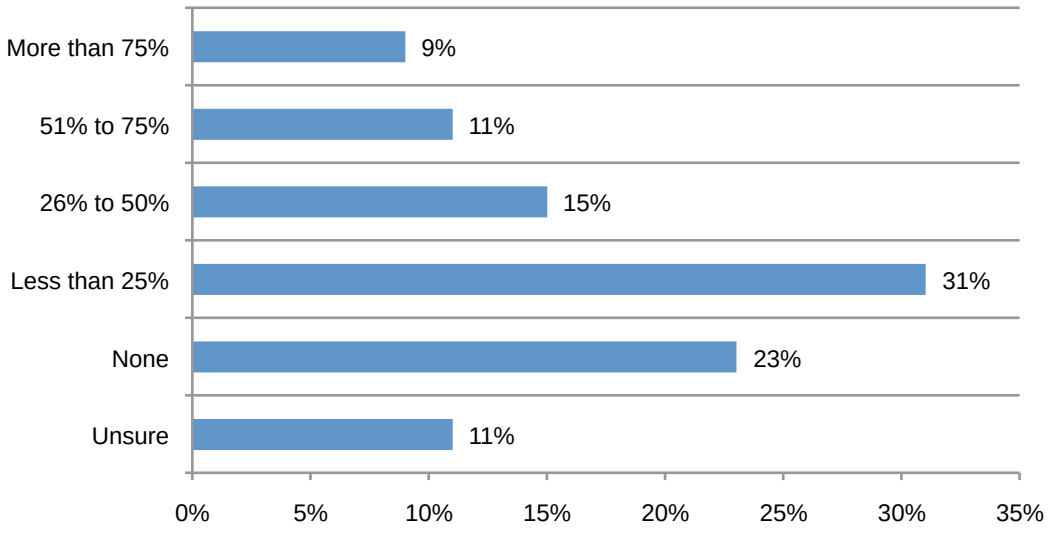
As shown in Bar Chart 4, this extremely sensitive information is mostly used in patient care and diagnostics and testing, billing and payments and research.

Bar Chart 4. How is the above patient health information marked as extremely sensitive used by your organization?
Check all that apply



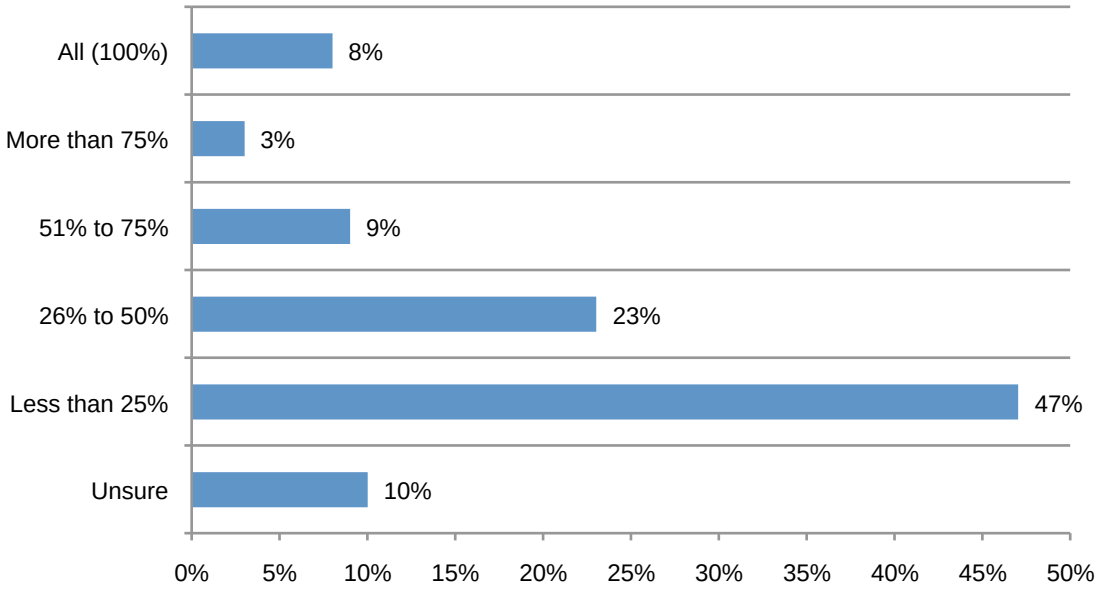
Patient health information used by small healthcare providers is most often onsite and in paper format. Bar Chart 5 reveals that less than 25 percent of patient health information (PHI) is stored offsite or at a managed services provider (including cloud services), according to 54 percent of respondents.

Bar Chart 5. How much of patient health information (PHI) used in your organization is stored offsite or at a managed services provider (including cloud services)?



As shown in Bar Chart 6, most of the sensitive patient information collected and stored by these small healthcare providers is in paper and not stored in electronic files.

Bar Chart 6. What percentage of the above information is in electronic versus paper files?

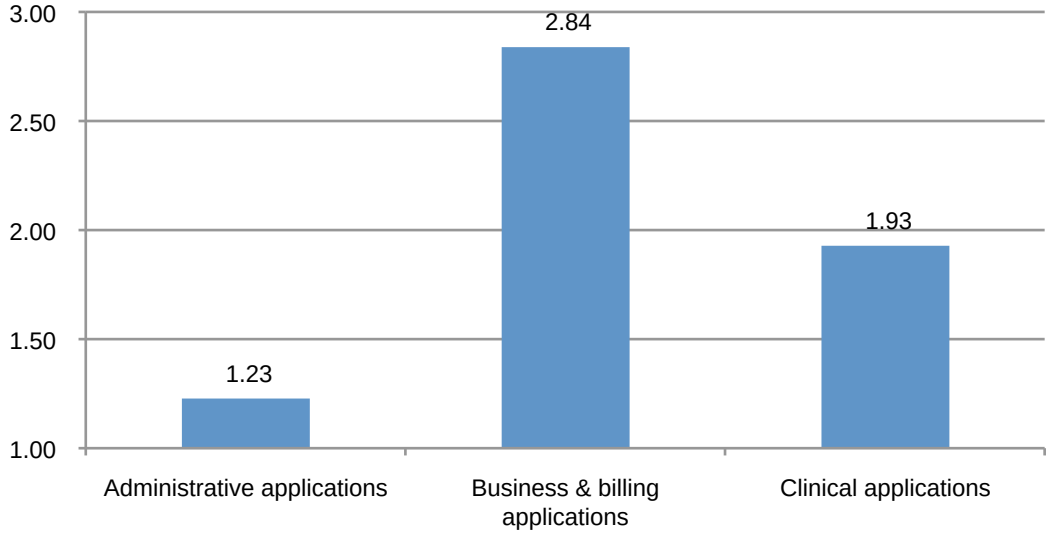


Sensitive information and risky practices increase the likelihood of a data breach. Activities that are putting PHI most at risk, according to respondents are: business applications, cloud computing, mobile computing and social media.

Business applications. Bar Chart 7 details what respondents believe to be the types of applications that present the highest risk of patient data leakage. These are such business applications as billing and insurance processes followed by clinical applications such as physician notes, prescriptions or diagnostic reports.

Bar Chart 7. What types of applications or activities present the highest risk of patient data leakage?

Three choices ranked from 3 = highest risk to 1 = lowest risk.



Cloud computing. According to Pie Chart 1, approximately one-third (34 percent) of respondents say their organization uses cloud computing. The primary cloud applications in use, as shown in Table 1 are scheduling, email and document management followed by business applications such as accounting, billing and insurance processing**.** The latter applications are considered to have extremely sensitive information.

Pie Chart 1. Does your organization use cloud computing?

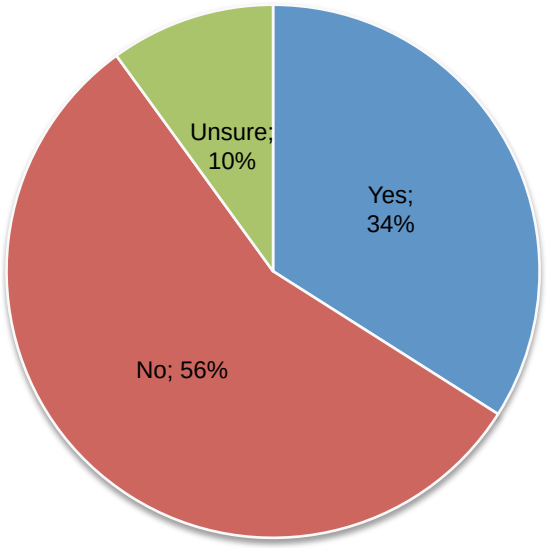


Table 1. If yes, what types of cloud applications does your organization use?

Types of cloud applications used	Pct%
Administrative applications such as scheduling, email and document management	85%
Business applications such as accounting, billing and insurance processing	41%
Clinical applications such as physician notes, prescriptions or diagnostic reports	38%
Managed security services	14%
Other	9%

Concerns about security seem to be keeping small healthcare organizations from processing data in the cloud. Bar Chart 8 reveals that 77 (45+21+11) percent of respondents say that less than half of their organization's total data processing activities are presently performed in the cloud. To address the risks, organizations most often only use leading cloud providers and rely upon informal or word of mouth referrals.

Bar Chart 8. What percentage of your organization's total data processing activities are presently performed in the cloud?

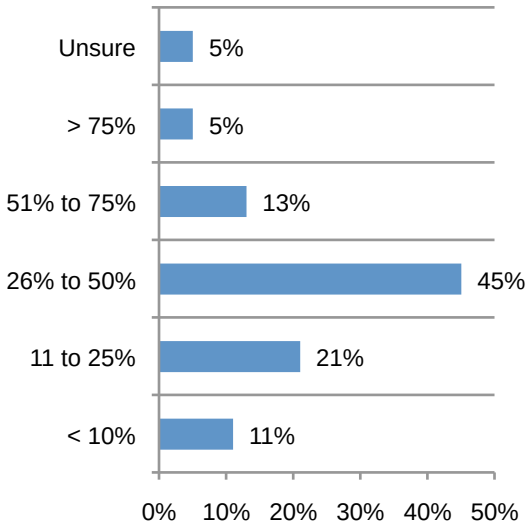
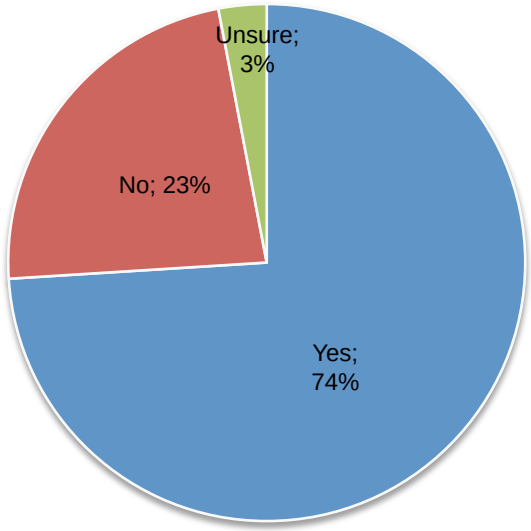
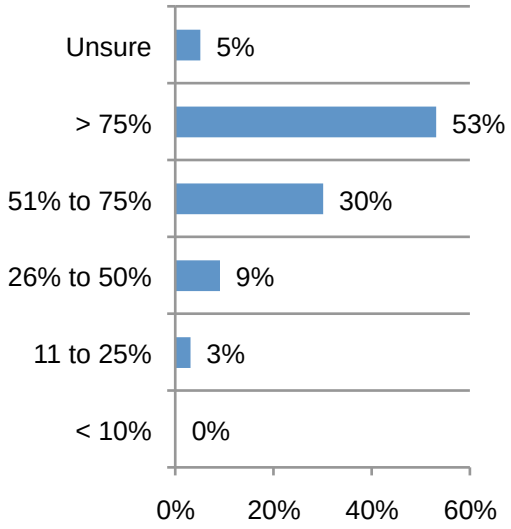


Table 2. If yes, what steps does your organization take to ensure cloud service providers are safe and secure (more than one response allowed)?

Steps taken to ensure cloud services are safe and secure	Pct%
Only use leading cloud provides	56%
Informal or word of mouth	47%
None of the above	32%
Indemnification in legal agreements	25%
Perform reference checks	21%
Obtain proof of security/operational certifications such as a SAS 70 II	9%
Other (please specify)	5%
Use of cloud security services	4%
Vetting and background checks	3%
Total	202%

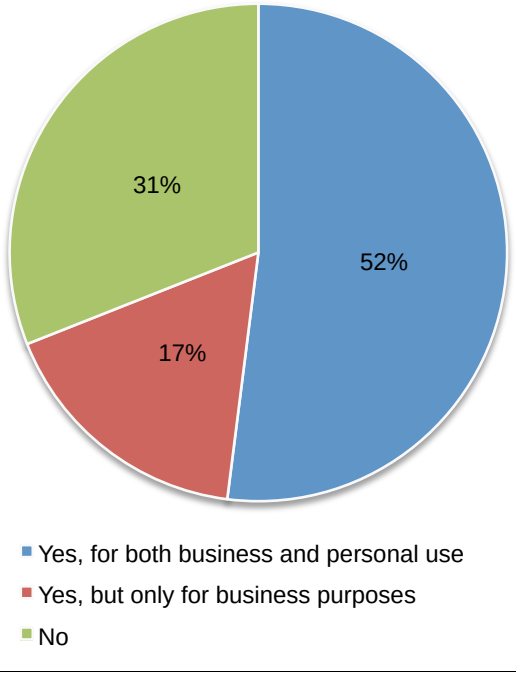
Mobile computing. Pie Chart 2 shows 74 percent of respondents say their organization allows employees to access business or clinical applications from mobile devices, including laptops, netbooks, smartphones, iPads and other tablets they own.

Bar Chart 9 reports that 53 percent of respondents say that almost all employees use mobile devices in the workplace. To address the risk, 48 percent say their organizations mostly rely on policies governing the proper use of mobile devices and 45 percent say they don't do anything to protect these mobile devices.

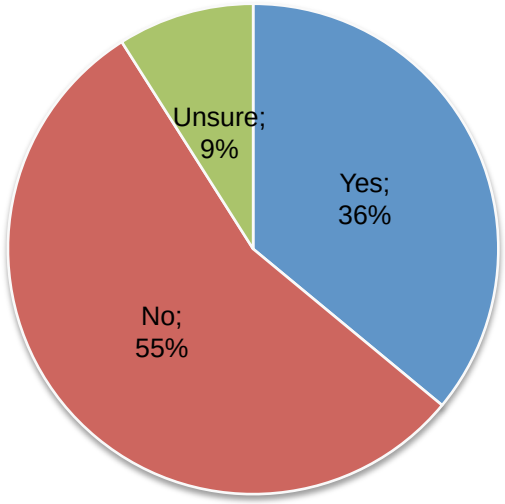
Pie Chart 2. Does your organization allow employees to access business or clinical applications from mobile devices?	**Bar Chart 9. If yes, what percent of your employees use mobile devices in the workplace?**
	

Social media. According to Pie Chart 3**,** more than half (52 percent) of respondents say their organization allows employees to access social networks or social media tools during the workday for both business and personal use. However, Pie Chart 4 shows 55 percent of respondents admit their organizations do not have an acceptable use policy for the use of social networks in the workplace.

Pie Chart 3. Does your organization allow employees to access social networks or social media tools during the workday?

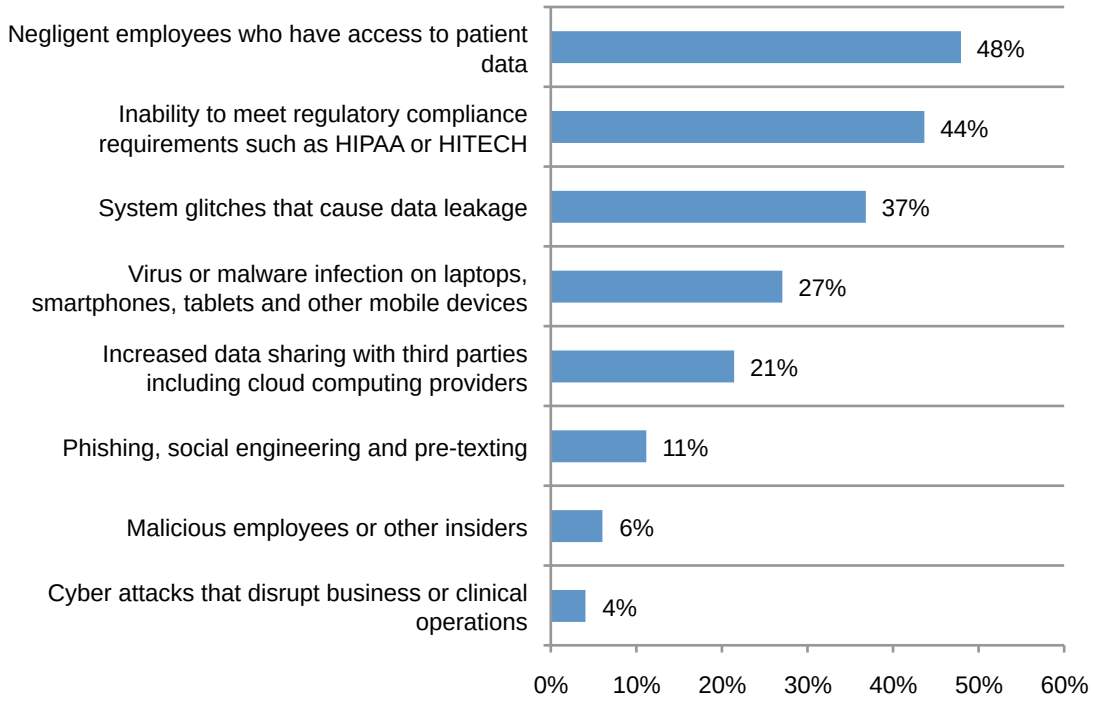


Pie Chart 4. Does your organization have an acceptable use policy for social networks?



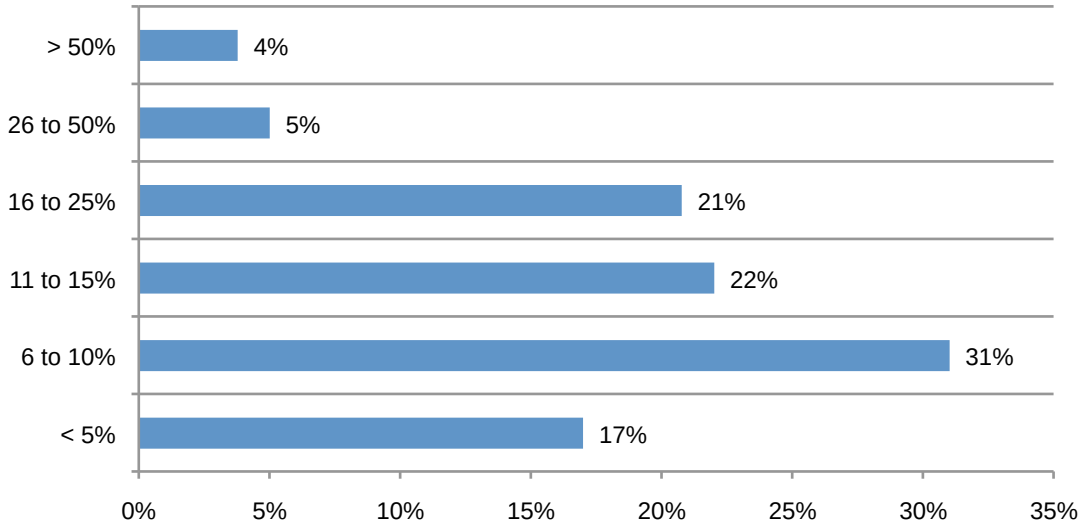
Employee negligence and noncompliance are the greatest threats to these healthcare organizations. The greatest data security risks, according to respondents and shown in Bar Chart 10, are negligent employees who have access to patient data and the inability to meet regulatory compliance requirements such as HIPAA or HITECH. Malicious employees or other insiders and cyber attacks are not considered as significant a risk.

Bar Chart 10. What do you see as the data security threats that present the highest risk to your organization?
Top two choices



Sixty percent of respondents say governance and control procedures are considered very effective or effective in securing patient health information. Forty-eight percent of respondents say the security technologies they use are very effective or effective**.** Bar Chart 11 shows that approximately half of respondents (48 percent) say less than 10 percent of their organization's IT budget or annual spending is dedicated to data security technologies**.**

Bar Chart 11. What percentage of your organization's IT budget or annual spending is devoted to data security technologies and related activities?



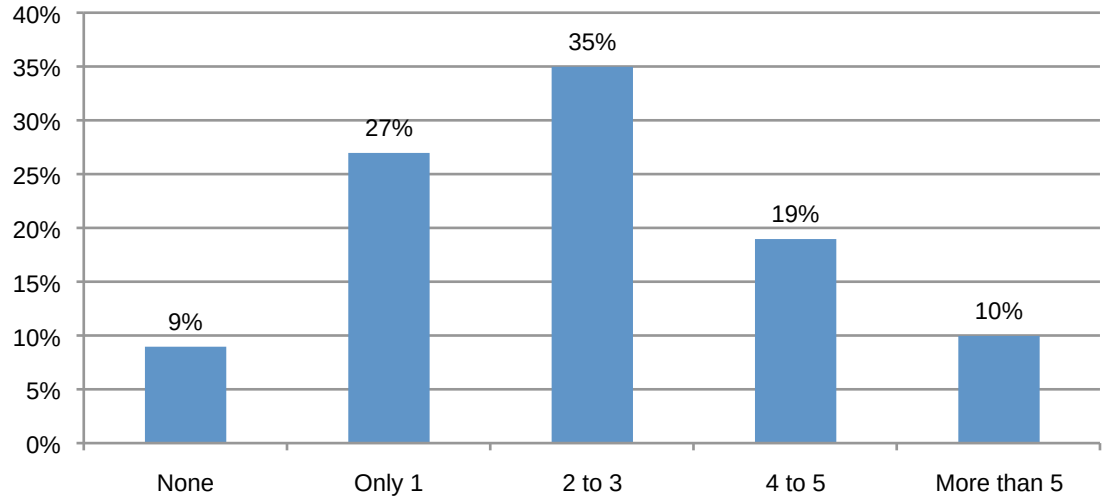
Encryption or tokenization of data in storage followed by data loss prevention tools and multilayered firewalls are the most popular technologies managed in-house. The most popular technologies managed by a security services provider are intrusion prevention and detection systems, SEIM or other network intelligence systems and access governance systems.

In contrast, 60 percent of respondents say their organizations' governance and control practices are very effective or effective. The most popular governance or control practices in place are shown in Bar Chart 12. They are: training and awareness activities for end-users, adherence to standardized security requirements and backup and disaster recovery plans.

Bar Chart 12. Please check all the data governance or control practices that your organization has in-place today.

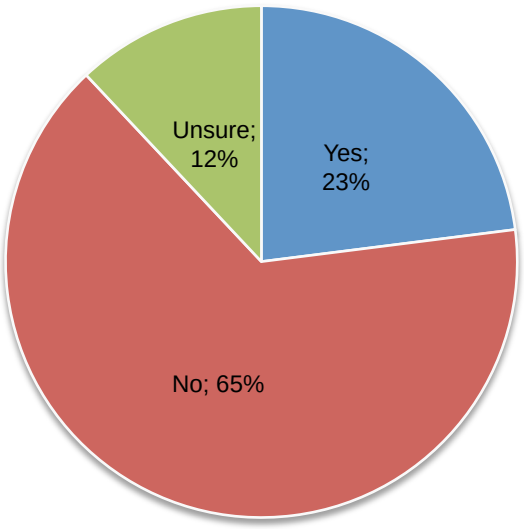
Data breaches and medical identity theft are occurring in small healthcare organizations. Similar to the large healthcare providers, the organizations featured in this study are experiencing data breaches. In fact, 91 (27+35+19+10) percent of respondents report that their organizations have had a data breach involving the loss or theft of patient health information in the past 12 months as revealed in Bar Chart 13. Fifty-five percent were required to notify the individuals who had their patient information lost or stolen. Sixty-three percent say the data breach involved less than 500 records.

Bar Chart 13. How many data breaches involving the loss or theft of patient health information has your organization experienced in the past 12 months?

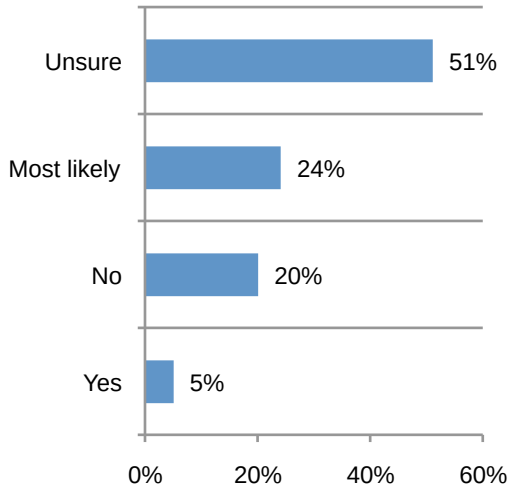


Medical ID theft. Almost half of respondents (49 percent) say they are very familiar or familiar with medical identity theft and, according to Pie Chart 3, 23 percent of respondents say that their organization experienced at least one actual or attempted medical identity theft incident sometime over the past 12 months.

Pie Chart 3. Has your organization ever experienced a patient medical identity theft incident?



Bar Chart 14. Was the root cause of the medical identity theft incident the result of your organization's data breach incidents?



For respondents who say their healthcare organization experienced a medical identity theft incident, 51 percent are uncertain whether the root cause of this incident (or attempted incident) was the result of a data breach. Bar Chart 14 shows only 5 percent of respondents who are certain that a breach was the root cause of a medical identity theft.

Part 3. Methods

A random sampling frame of 20,212 adult-aged individuals who reside within the United States was used to recruit and select participants to this survey. Our randomly selected sampling frame was built from proprietary lists of experienced individuals with bona fide credentials in the healthcare fields.

As shown in Table 3, 844 respondents completed the survey. Of the returned instruments, 41 surveys failed reliability checks. A total of 803 surveys were available before screening. Two screening questions were used to remove respondents who did not have relevant experience or knowledge to rate their organizations' data protection activities. This resulted in a final sample of 708 individuals.

Table 3. Survey response	Freq.	Pct%
Sample frame	20,212	100.0%
Total responses	844	4.2%
Rejected surveys	41	0.2%
Sample before screening	803	4.0%
Final sample	708	3.5%

Table 4 reports the respondent's organizational role within participating smaller sized healthcare organizations. Twenty-three percent of respondents say they are the medical office manager, and 18 percent say they are head of administration. The approximate experience level of respondents is 9.88 years and 5.09 years in their present position.

Table 4. Respondents' current position	Pct%
Owner/manager	12%
Office manager	23%
Head of medical services	9%
Head of administration	18%
Head of IT	15%
Head of compliance	8%
Billing manager	5%
Records manager	7%
Other (please specify)	3%
Total	100%

Table 5 reports the U.S. region where participants are located. As can be seen, the largest geographical regions include the Northeast (20 percent) and the Pacific-West (19 percent).

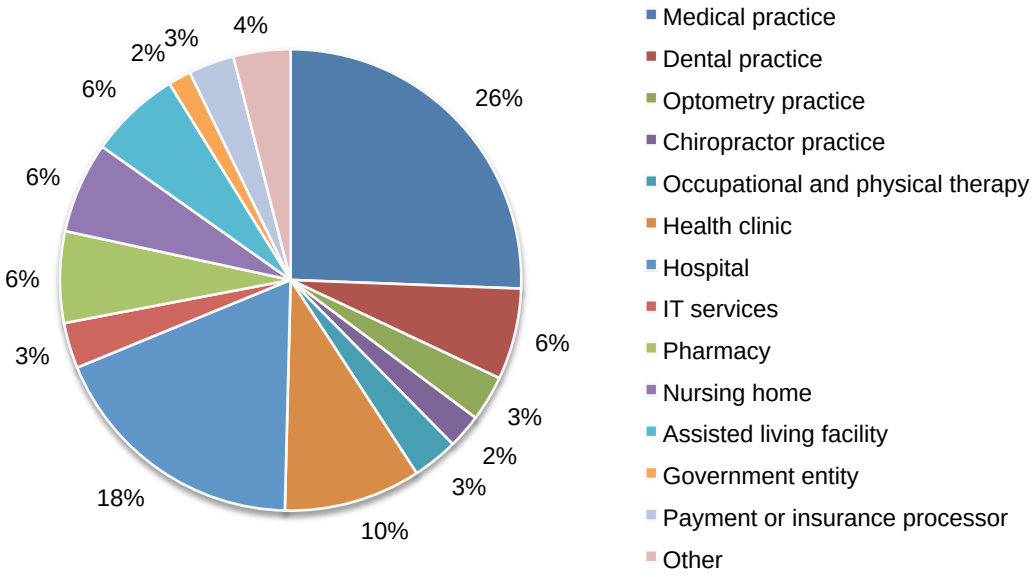
Table 5. U.S. regional location of respondents' organizations	Pct%
Northeast	20%
Mid-Atlantic	18%
Midwest	17%
Southeast	16%
Southwest	13%
Pacific-West	19%
Total	100%

Table 6 reports the number of medical professionals (a.k.a. clinicians) residing in participants' organizations.

Table 6. Number of clinicians in respondents' healthcare organizations	Pct%
None	6%
1 to 10	35%
11 to 25	40%
26 to 50	19%
More than 50	100%

Pie Chart 4 reports the type of healthcare organization represented by participants. As can be seen, the largest segment include medical offices (28%) and small-sized hospitals.

Pie Chart 4. Distribution of respondents' healthcare organizations



Part 4. Concluding thoughts

The findings of the study show that smaller healthcare organizations face the same challenges as larger organizations. Almost every organization has had a data breach and 23 percent believe their organizations had a medical identity theft incident.

The biggest threats are considered to be negligent employees and inability to meet compliance requirements. As a result, these organizations seem to rely upon governance and control activities such as training and awareness programs.

An area that also seems to be vulnerable is employees' use of mobile computing and social media. A recommendation for these organizations is to create policies and guidelines to incorporate in their training and awareness programs about the appropriate use of these devices and applications. They should also consider technologies that specifically address the risks associated with the use of mobile devices.

Limitations

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 located smaller-sized healthcare organizations in the United States. It is always possible that individuals who did not participate are substantially different in terms of underlying beliefs or perceptions about data protection activities from those who completed the instrument.
- Sampling-frame bias: The accuracy is based on contact information and the degree to which the sample is representative of individuals employed by smaller-sized healthcare organizations. We also acknowledge that the results may be biased by external events.

  We also acknowledge bias caused by compensating respondents 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 certain respondents did not provide accurate responses.

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured over a three-week period ending in November 2011.

Survey response	Freq.	Pct%
Sample frame	20,212	100.0%
Total responses	844	4.2%
Rejected surveys	41	0.2%
Sample before screening	803	4.0%
Final sample	708	3.5%

Part 1. Screening questions

S1. Does your organization use or have access to patient health information?	Freq.	Pct%
Yes	788	98%
No (stop)	15	2%
Total	803	100%

S2. Is your organization required to comply with the U.S. Health Insurance Portability & Accountability Act (a.k.a. HIPAA)?	Freq.	Pct%
Yes	780	99%
No (stop)	8	1%
Total	788	100%

S3. What is the approximate number of employees in your organization?	Freq.	Pct%
Less than 10	93	12%
11 to 25	178	23%
26 to 100	265	34%
101 to 250	172	22%
More than 250 (stop)	72	9%
Total	780	100%

Final sample	708

Part 2. Survey questions

Q1. Please respond to each statement using the following five-point scale to express your opinion: Strongly agree and agree responses shown.	Strongly agree	Agree	Combined
My organization has adequate policies and procedures to protect patient health information.	18%	28%	46%
My organization takes appropriate steps to protect the privacy rights of patients.	30%	32%	62%
My organization takes appropriate steps to comply with the requirements of HIPAA and other related healthcare regulations.	25%	28%	53%
My organization's owners/management views privacy and data security as a top priority.	14%	17%	31%
My company has sufficient resources to ensure privacy and data security requirements are met.	15%	15%	30%

Q2. Following is a list of 29 data elements that healthcare organizations may collect and store about patients in files or records. Please use the following three-point scale to denote the patient data elements viewed as the **most sensitive or confidential** by your organization: 1 = Not sensitive, 2 = Sensitive and 3 = Extremely sensitive. Please leave blank if your organization does not collect a stated data element.	Not sensitive	Sensitive	Extremely sensitive
Name	73%	22%	5%
Address	72%	24%	4%
Telephone	69%	30%	1%
Age	53%	45%	2%
Gender	71%	25%	4%
Race	21%	73%	6%
Religion	23%	39%	38%
Ethnicity	21%	34%	45%
Sexual orientation	20%	15%	65%
Physical characteristics such as weight, height	50%	22%	28%
Family health history	37%	22%	41%
Martial status	60%	38%	2%
Guardian or next of kin	68%	22%	10%
Health history	15%	25%	60%
Present illnesses	5%	21%	74%
Photo, x-ray or MRI	9%	69%	22%
Medications	5%	28%	67%
Surgeries	12%	77%	11%
Diet & exercise	36%	31%	33%
Addictions	2%	10%	88%
Employer	36%	60%	4%
Participation in clinical trials	8%	7%	85%
Names of health care providers	28%	50%	22%
Social Security Number	34%	55%	11%
Health insurance information	31%	53%	16%
Educational background	57%	38%	5%
Credit card or bank payment information	43%	40%	17%
Credit or payment history	39%	33%	28%
Doctor-patient voice communications (VOIP)	2%	54%	44%

Q3. How is the above patient health information marked as **extremely sensitive** used by your organization? Please check all that apply.	Pct%
Billing & payments	68%
Insurance verification	59%
Patient care (clinical)	95%
Diagnostics & testing	91%
Marketing & communications	12%
Patient relations	36%
Research	68%
Compliance	43%
Education and training	29%
Other (please specify)	2%

Q4. Approximately, what percentage of the above information is in electronic versus paper files?	Pct%
Less than 25% in electronic records	47%
Between 25% and 50% in electronic records	23%
Between 51% and 75% in electronic records	9%
More than 75% in electronic records	3%
All the above information is in electronic records	8%
Unsure	10%
Total	100%

Q5. Approximately, how much of patient health information (PHI) used in your organization is stored offsite or at a managed services provider (including cloud services)?	Pct%
None	23%
Less than 25% of all patient health information	31%
Between 26% and 50% of all patient health information	15%
Between 51% and 75% of all patient health information	11%
More than 75% of all patient health information	9%
Unsure	11%
Total	100%

Q6. What types of applications or activities present the highest risk of patient data leakage? Please rank the following three selections from 3 = highest risk to 1 = lowest risk.	Average rank
Administrative applications such as patient scheduling systems	1.23
Business applications such as billing and insurance processing	2.84
Clinical applications such as physician notes, prescriptions or diagnostic reports	1.93
Average	2.00

Q7a. Does your organization use cloud computing?	Pct%
Yes	34%
No	56%
Unsure	10%
Total	100%

Q7b. If yes, what types of cloud applications does your organization use? Please check all that apply.	Pct%
Administrative applications such as scheduling, email and document management	85%
Business applications such as accounting, billing and insurance processing	41%
Clinical applications such as physician notes, prescriptions or diagnostic reports	38%
Managed security services	14%
Other (please specify)	9%
Total	187%

Q7c. If yes, what percent of your organization's total data processing activities are presently performed in the cloud?	Pct%
Less than 10%	11%
Between 11 to 25%	21%
Between 26% and 50%	45%
Between 51% and 75%	13%
More than 75%	5%
Unsure	5%
Total	100%

Q7d. If yes, what steps does your organization take to ensure cloud service providers are safe and secure?	Pct%
Vetting and background checks	3%
Only use leading cloud provides	56%
Indemnification in legal agreements	25%
Perform reference checks	21%
Obtain proof of security/operational certifications such as a SAS 70 II	9%
Use of cloud security services	4%
Informal or word of mouth	47%
None of the above	32%
Other (please specify)	5%
Total	202%

Q7e. Do you believe there is some patient data too sensitive to be processed or stored in the cloud?	Pct%
Yes	65%
No	31%
Unsure	4%
Total	100%

Q8. What do you see as the data security threats that present the **highest risk** to your organization? Please select only your top two choices.	Pct%
Cyber attacks that disrupt business or clinical operations	4%
Inability to meet regulatory compliance requirements such as HIPAA or HITECH	44%
Negligent employees who have access to patient data	48%
System glitches that cause data leakage	37%
Phishing, social engineering and pre-texting	11%
Malicious employees or other insiders	6%
Virus or malware infection on laptops, smartphones, tablets and other mobile devices	27%
Increased data sharing with third parties including cloud computing providers	21%
Other (please specify)	3%
Total	200%

Q9a. Please check all the data security technologies that your organization either manages in-house or is managed by an outside security services provider.	Do not use	Managed in-house	Managed by a security services provider
Multilayered firewalls	23%	68%	32%
Anti-virus, anti-malware systems	21%	64%	36%
VPN or other secure gateway	31%	41%	59%
Encryption of data on computers and other mobile devices	54%	63%	37%
Encryption or tokenization of data in storage	86%	80%	20%
Encryption of data when transferred or in-motion	55%	65%	35%
Data loss prevent tools	54%	78%	22%
SIEM or other network intelligence systems	71%	25%	75%
Identity and access management systems	43%	45%	55%
Access governance systems	43%	33%	67%
Multifactor or single sign-on authentication	61%	54%	46%
Mobile security management suite	80%	50%	50%
Database security tools including scanning	48%	62%	38%
Intrusion prevention and detection systems	70%	25%	75%
Average	53%	54%	46%

Q9b. Please rate the overall effectiveness of the above mentioned security technologies you have in-place for securing patient health information using a 5-point scale. Very effective and effective responses are shown.	Very effective	Effective	Combined
Rating	20%	28%	48%

Q9c. Approximately, what percentage of your organization's IT budget or annual spending is devoted to data security technologies and related activities?	Pct%
Less than 5%	17%
6 to 10%	31%
11 to 15%	22%
16 to 25%	21%
26 to 50%	5%
More than 50%	4%
Total	100%

Q10a. Please check all the data governance or control practices that your organization has in-place today.	Pct%
Appointment of a security leader	12%
Formalized process for policy review	38%
Process for reviewing employee or patient complaints about security operations	5%
Process for self-reporting compliance violations to appropriate authorities	19%
Clearly defined security policies and procedures (a.k.a. standard operating procedures)	49%
Backup and disaster recovery plans	63%
Background checks of all privileged users	37%
Training and awareness activities for the organization's end-users	83%
Monitoring of business partners, vendors and other third-parties	21%
Audits of security and other related IT compliance practices	10%
Segregation of duties	45%
Control self-assessment	25%
Adherence to standardized security requirements	64%
Other (please specify)	5%
Average	34%

Q10b. Please rate the overall effectiveness of the above-mentioned governance and control practices you have in-place for securing patient health information using a 5-point scale. Very effective and effective responses are shown.	Very effective	Effective	Combined
Rating	29%	31%	60%

Q10c. Approximately, what percentage of your organization's compliance activities is devoted to HIPAA requirements?	Pct%
Less than 5%	0%
6 to 10%	3%
11 to 15%	12%
16 to 25%	17%
26 to 50%	35%
More than 50%	33%
Total	100%

Q10d. Approximately, what percentage of your organization's compliance activities is devoted to PCI DSS requirements?	Pct%
Less than 5%	20%
6 to 10%	32%
11 to 15%	35%
16 to 25%	9%
26 to 50%	3%
More than 50%	1%
Total	100%

Q11. Does your organization have sufficient funding to achieve proper governance, risk management and compliance requirements with respect to the protection of patient health information?	Pct%
Yes	31%
No	34%
Unsure	35%
Total	100%

Q12. How many data breaches involving the loss or theft of patient health information has your organization experienced in the past 12 months?	Pct%
None	0.09
Only 1	0.27
2 to 3	0.35
4 to 5	0.19
More than 5	0.1
Total	1

Q13. Was your organization required to notify data breach victims (patients)?	Pct%
Yes, for all data breach incidents experienced	12%
Yes, for some data breach incidents experienced	43%
No, disclosure was not necessary	45%
Total	100%

Q14. Approximately, how many patient records were lost or stolen as a result of all data breaches experienced by your organization over the past 12 months (cumulative amount)?	Pct%
Less than 10 records	22%
10 to 499 records	41%
500 to 999 records	22%
1,000 to 9,999 records	10%
10,000 to 100,000 records	4%
More than 100,000 records	1%
Total	100%

Q15a. What best describes your level of familiarity with medical identity theft.	Pct%
Very familiar	24%
Familiar	25%
Not familiar	15%
No knowledge (to Q16)	36%
Total	1

Q15b. Has your organization ever experienced a patient medical identity theft incident?	Pct%
Yes	23%
No	65%
Unsure	12%
Total	100%

Q15c. If yes, how many medical identity theft incidents has your organization experienced over the past 12 months? Please include unsuccessful attempts in your frequency estimate.	Pct%
None	0%
Only 1	51%
2 to 3	42%
4 to 5	7%
More than 5	0%
Total	100%

Q15d. Was the root cause of the medical identity theft incident (or attempted incident) the result of your organization's data breach incidents?	Pct%
Yes, with certainty	5%
Yes, most likely	24%
Unsure	51%
No	20%
Total	100%

Q16. What statement best describes your belief about how compliance with HIPAA and HITECH affects the security of patient health information in your organization?	Pct%
Compliance increases the security of patient health information	45%
Compliance decreases the security of patient health information	9%
Compliance has no affect on the security of patient health information	46%
Total	100%

Q17. In your opinion, what are the **most significant** barriers to achieving a strong privacy and data security posture with respect to patient health information collected, used and retained by your organization? Please check all that apply.	Pct%
Lack of clinician support	74%
Lack of resources (funding gap)	71%
Lack of enabling technologies	23%
Lack of accountability and leadership	58%
Inability to control third parties, including cloud computing providers	24%
Insufficient governance procedures	38%
Unnecessary compliance burden	63%
Other (please specify)	3%
Total	354%

Q18. Who within your organization is **most** responsible for protecting of patient health information?	Pct%
Owner/management	21%
Records management	3%
Head of medical services	2%
Head of compliance	13%
Office manager	15%
Head of IT operations	9%
Legal or general counsel	2%
Human resources	0%
No one person has overall responsibility	35%
Unsure	0%
Total	100%

Q19a. Does your organization allow employees to access business or clinical applications from mobile devices including laptops, netbooks, smartphones, iPads, or other tablets owned by them?	Pct%
Yes	74%
No	23%
Unsure	3%
Total	100%

Q19b. If yes, what percent of your employees use mobile devices in the workplace?	Pct%
Less than 10%	0%
Between 11 to 25%	3%
Between 26% and 50%	9%
Between 51% and 75%	30%
More than 75%	53%
Unsure	5%
Total	100%

Q19c. If yes, what steps is your organization taking to safeguard information contained on these devices?	Pct%
Encryption solutions installed	31%
Passwords or keypad locks	34%
Anti-virus/anti-malware product installed	19%
Polices governing the proper use of mobile devices	48%
Other (please specify)	9%
We don't do anything to protect these mobile devices	45%
Total	186%

Q20a. Does your organization allow employees to access social networks or social media tools during the workday?	Pct%
Yes, for both business and personal use	52%
Yes, but only for business purposes	17%
No	31%
Total	100%

Q20b. Does your organization have an acceptable use policy for social networks?	Pct%
Yes	36%
No	55%
Unsure	9%
Total	100%

Part 3. What best describes your role?

D1. What organizational level best describes your current position?	Pct%
Owner/manager	12%
Office manager	23%
Head of medical services	9%
Head of administration	18%
Head of IT	15%
Head of compliance	8%
Billing manager	5%
Records manager	7%
Other (please specify)	3%
Total	100%

D2. Is this a full time position?	Pct%
Yes	97%
No	3%
Total	100%

D3. What best describes your organization's healthcare industry focus?	Pct%
Medical practice	26%
Dental practice	6%
Optometry practice	3%
Chiropractor practice	2%
Occupational and physical therapy	3%
Health clinic	10%
Hospital	18%
IT services	3%
Pharmacy	6%
Nursing home	6%
Assisted living facility	6%
Government entity	2%
Payment or insurance processor	3%
Other (please specify)	4%
Total	100%

D4. Total years of experience	Mean	Median
Total years of relevant experience	9.88	10.50
Total years in current position	5.09	5.00

D5. How many locations or offices does your organization have?	Pct%
Only 1	32%
2 to 3	19%
4 to 5	28%
More than 5	21%
Total	100%

D6. Where in the United States are you located?	Pct%
Northeast	20%
Mid-Atlantic	18%
Midwest	17%
Southeast	16%
Southwest	13%
Pacific-West	19%
Total	100%

D7. What is the total number of clinicians in your organization?	Pct%
None	6%
1 to 10	35%
11 to 25	40%
26 to 50	19%
More than 50	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.

MegaPath™
DATA · VOICE · SECURITY

Network Security

Managed Network Security for Healthcare

Network Security Challenges for Healthcare Organizations

Network security is a growing problem and business concern for healthcare organizations of all sizes and types. Today, healthcare IT managers must monitor and manage a broad range of security issues while keeping pace with expanding regulatory requirements and new network technologies. And of course, do all of this with limited budgets and staff.

Security Breaches Target Medical Identities

Perhaps the most worrisome network security threat for a healthcare organization is theft of a patient's medical identity. This information is becoming more attractive to organized crime, which can profit directly by sending fraudulent bills to insurers. A medical identity can also be sold to someone who can use it to obtain health care or prescription drugs.

A survey conducted by Ponemon Institute and sponsored by MegaPath uncovered some thought-provoking information about to the topic of medical identity theft:

- 91 percent of survey respondents had experienced a breach of private health information in the previous 12 months. Of those respondents, 55 percent had to notify patients of the breach and 24 percent said the breach likely resulted in medical identity theft.
- 43 percent of respondents had experienced at least one medical identity theft incident in the past.

More Network Threats

Healthcare networks are also experiencing the exponential growth in viruses, worms, and other malware attacks directed at business networks. Increased use of wireless networks, social media, and employees' personal mobile devices are bringing new data and IT security threats into the workplace. Yet, 52 percent of survey respondents rated their security technology plans as ineffective.

New Regulatory Requirements for Data Privacy

As both mandates and incentives increase for use of electronic medical records (EMRs), providers must maintain compliance with ever-changing regulatory requirements. However, HIPAA and HITECH rules about patient privacy tell healthcare organizations what they need to do, but not how to do it—especially regarding how to implement network security.

Healthcare records aren't the only regulated electronic data that is targeted by network attackers. Information about credit/debit card numbers and transactions for patient billing must also meet Payment Card Industry (PCI) security requirements. In the future, it will become increasingly important to supply proof of compliance with all of these regulatory requirements.

MegaPath™ DATA · VOICE · SECURITY

Network Security

Rapidly Changing Medical and Communications Technology

Digital records in EMR systems create new opportunities for online data theft or manipulation. Expanded use of wireless networks and mobile devices provides new avenues for accidental data exposure or a network breach. And social media applications – such as Facebook and Twitter – can impact patient privacy and HIPAA compliance when data is shared improperly.

Limited Resources for Managing Network Security

Small and midsize healthcare organizations must address IT security needs with a small budget. The Ponemon study found that nearly half of respondents dedicate less than 10 percent of an already small IT budget to network security technology and services.

These organizations also likely have a small IT staffin this role – perhaps one person or a part-time contractor – who must manage all network issues for multiple sites. Typically, no one in this role has strong network security expertise, which means nobody wants to be accountable for compliance.

The MegaPath Solution

Network security challenges are particularly daunting for clinics, medical practices, labs, pharmacies, and other non-hospital healthcare organizations with 100 to 250 employees and one or multiple locations. IT managers in many of these organizations now realize that a “do-it-yourself” approach to network security is no longer working. It is too difficult and expensive to stay ahead of security threats, and take advantage of new security solutions on your own.

- Managed Security Services from MegaPath offer the security expertise and advanced network security technologies that deliver an ideal solution for healthcare organizations.
- Gain security expertise, outsource burdensome security management.
- Instead of trying to manage with constrained resources, you can completely outsource your network security functions. This allows for management by a smaller IT staff, and eliminates the necessity to hire a network security expert or to place IT staff at each location.
- Managed Security Services also eliminates the need for ongoing maintenance tasks for network security systems, which can become a large and time-consuming effort for a small IT staff.

Leverage Advanced Network Security Technology:

MegaPath Compliance

Security governance is the first line of defense for most organizations, but governance policies alone do not ensure compliance with HIPAA/HITECH and other regulations. MegaPath offers a technology foundation that meets the unique needs of healthcare by enforcing security policies, protecting the network, and reporting on security issues and performance for regulatory compliance.

MegaPath Security Policy Enforcement

Policies that govern access and use of data and applications on the network can be enforced automatically and with flexibility to meet diverse business needs. Essential capabilities in the MegaPath platform for enforcing network security policies include:

- **Application Control:** Restricts access to online chat, Web-hosted email, and other online services that are often used as conduits for a network attack or breach. This control can be applied to all network users or specific groups of employees.
- **Content Filtering:** Blocks access to social media, entertainment, shopping, and other non-business sites for specific groups of employees. This capability also protects against sites that host inappropriate or malicious content.
- **Data Loss Prevention:** Detects sensitive data types such as patient ID, social security, and credit card numbers – then blocks this data from being transmitted outside of the network.

MegaPath Provides Network Protection

Networks need direct protection through security technologies and services – such as:

- Cloud-based and premises-based Unified Threat Management (UTM) capabilities provide a defense-in-depth approach to security by protecting healthcare provider data at the network edge and at the site level.
- **Intrusion Prevention:** Detects disruptive threats and reacts instantly to prevent network impact.
- **Anti-Virus/Anti-Malware:** Protects against all types of malware – including "drive-by" malware injection that can occur when employees browse infected websites.

Compliance and Reporting from MegaPath

Information about network access and activity by users and their devices is vital for ensuring appropriate use, to identify trends, and to produce reports on compliance.

- **Managed Logging:** Collects, stores, analyzes, and reports on all security devices, network infrastructures, and host systems.
- **Vulnerability Assessment:** Performs periodic network scans to identify network risks and remediation recommendations that include detailed reports for use in compliance documentation.
- **Vulnerability Assessment:** Performs periodic network scans to identify network risks and remediation recommendations that include detailed reports for use in compliance documentation.
- **File Integrity Monitoring:** Tracks and alerts when critical system files are modified.

MegaPath Managed Security Services for Healthcare

MegaPath Managed Security Services (MSS) provide a comprehensive, multi-layered approach to network security that helps protect systems and patient data while maintaining security compliance. These services run on MegaPath's secure, MPLS-based private network with additional layers of protection provided by MegaPath premises-based MSS. At MegaPath, we are Secure to the Core – the core of your network and ours.