2009 HIMSS Analytics Report: Evaluating HITECH's Impact on Healthcare Privacy and Security

Commissioned by ID Experts

November 2009

INTRODUCTION

Healthcare breaches are on the rise; according to the *2009 ITRC Breach Stats Report* healthcare breaches account for over 66 percent of all records breached this year (up from 20 percent in 2008). In fact, some of the largest names in healthcare have suffered data breaches. In one incident, an employee at a high-profile medical center allegedly stole the personal information of 1,000 patients with the intent to defraud insurance companies. Another case involved the theft of a laptop from a Chicago hotel that may have contained Personal Health Information (PHI) such as medical record numbers, names, and Social Security numbers. And at a New York City hospital, an admissions employee was suspected of selling 2,000 patients' data as part of an identity theft scheme and illegally accessing nearly 50,000 records.

On September 23, 2009 the Health Information Technology for Economic and Clinical Health (HITECH) Act took effect. The HITECH Act is Title 13, Subtitle D of the American Recovery and Reinvestment Act (ARRA) and it was enacted to reduce healthcare costs through the adoption of electronic medical records. To ensure that privacy and security go hand in hand with the digitization of health records, HITECH also imposes new privacy requirements on healthcare organizations and their business associates.

The new requirements include a broader definition of what PHI must be protected, increased penalties for violations of rules, provisions for more aggressive enforcement and explicit authority for state Attorney Generals to enforce HIPAA rules and pursue criminal cases. Additionally, the HITECH Act creates stringent data breach notification provisions including a 60 day notification requirement, posting of breach information to "prominent media outlets" if 500 or residents of an area are affected and mandatory reporting of all breaches to the Secretary of Health & Human Services (HHS).

HITECH Act has also provided a breach definition; the term breach is defined as "the unauthorized acquisition, access, use or disclosure of protected health information which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information".

HIMSS Analytics joined with ID Experts, to begin to understand awareness of the privacy and security provisions outlined in the HITECH Act and understand the challenges that HITECH is creating at healthcare organizations, as well as gain an understanding of how healthcare organizations are addressing data breaches (and the potential of data breaches at their organization). This report summarizes our findings from a survey of senior executives from healthcare organizations and individuals working for business associates across the United States. Funding for this research was provided by ID Experts.

Contents

1. Executive Summary

The broad objective of this research was to gain an understanding of the status of patient data privacy and security, and the related potential for data breaches at hospitals and their business associates across the United States. We looked at this particularly in the context of the recently enacted HITECH (Health Information Technology for Economic and Clinical Health) Act. Respondents were asked to provide information in the following areas:

- Their awareness of the HITECH Act
- Their challenges associated with meeting the requirements outlined in the data breach provisions of the HITECH Act
- How the HITECH Act has changed their organizations' expectations of future data breaches
- How the HITECH Act impacts the relationship that healthcare organizations have with their business associates
- How organizations are addressing data breach incidents and the future potential for data breach events

Following are the key findings in the report:

Risk assessments are common practice but alone do not mitigate breach risks. One-third (31 percent) of hospitals reported having a data breach at their organization in the last 12 months despite almost all (91 percent) having conducted a risk assessment and taken actions to address identified risks and gaps. Additionally, nearly all (97 percent) respondents indicated performing employee training and a significant percentage (81 percent) indicated they used data encryption technology.

Large hospitals experience the most data breaches and are at the greatest risk for future incidents. Fully half (52 percent) of large hospitals experienced a data breach in the past year compared to 33 percent of medium hospitals and 25 percent of small hospitals in our study.

Business associates are generally unprepared to meet the new data breach related obligations brought on by the HITECH Act. Business associates lag behind in all areas that were tested in this survey to measure awareness of the privacy requirements of the HITECH Act. Over 30 percent of business associates surveyed did not know the HIPAA privacy and security requirements have been extended to cover their organizations.

Healthcare organizations are prepared to sanction business associates that don't comply with the regulations outlined in the HITECH Act. 85 percent of hospitals indicated they will take action to protect their patient data that is held by a business associate, while a full 39 percent of business associates admitted they did not know what actions hospitals are taking. In addition, business associates were unaware that 47 percent of hospitals would terminate their contracts for violations.

Inter-departmental disconnects between IT and Compliance on data breach policies and procedures leave hospitals at risk. Our research found that non-IT respondents were more aware of data breach risks and notification regulations than IT respondents. Non-IT respondents reported that their organization had experienced twice as many data breaches as IT respondents (41 percent vs. 22 percent).

The report draws the following conclusions:

The HITECH Act treats business associates as a covered entity and as such, they need to be prepared to address the implications of a breach violation. The business associates in this survey lag behind the provider respondents in terms of awareness of the information in the HITECH Act. As of 2010, business associates will be bound by the same privacy and security requirements as are other covered entities. Our research demonstrated a difference in awareness of not only this requirement, but other requirements outlined in the HITECH Act, suggesting that additional education is needed in the business associate community. This is critical, as nearly half of covered entities said they were prepared to terminate a contract with a business associate for a data breach violation.

All information that is relevant to the security environment should be included in the risk assessment in order to quantify and mitigate data breach risk. Risk assessments are clearly part of the strategy that healthcare organizations are using to identify gaps in their organizations' security environments. However, only half of the organizations that conduct these assessments are doing them at least yearly. In addition, organizations are not including all aspects of the security environment that they can in the assessment. Specifically, while nearly all are conducting a policy and procedure review as part of this assessment, 25 percent are not tracking external threats or looking at data on employee compliance.

While hospitals are widely providing training for their employees, they are not always monitoring that employees are complying with the organization's policies and procedures on which they were trained. Nearly all respondents reported that they perform employee privacy and security training to protect against data breach risk. Respondents also found this training to be valuable – a 6.29 on a one to seven scale where one is not at all effective and seven is highly effective. However, less than three-quarters of respondents at hospitals that conducted a risk assessment indicated that information on employee compliance is part of the risk assessment.

Respondents working for large hospitals have a higher level of awareness of the potential for a security breach than do respondents working for small organizations. While large hospitals (300 or more beds) were more likely to have had a security breach at their organization than were smaller organizations, respondents at these organizations were also more likely to indicate that the passage of ARRA and HITECH have resulted in a greater level of awareness of data breaches and breach risk at their organization. Larger organizations also appear to be more prepared for the eventuality of a breach – 86 percent of respondents working for a large hospital reported that they believed that the HITECH Act's expanded requirements will result in discovery and reporting of additional breaches. All healthcare organizations, regardless of size, need to be aware of the provisions of HITECH to mitigate breach risk.

There are different levels of awareness between IT and non-IT executives in some key areas of the security environment at healthcare organizations. Non-IT executives are more likely than IT executives to indicate that a breach has occurred at their organization. Furthermore, non-IT executives are somewhat more aware of some key HITECH Act requirements, such as the requirement that notification of breach victims in ANY breach is required within 60 days. Finally, these individuals were somewhat more likely to indicate that their organization had made changes to their security environment as a result of a breach. This suggests that all departments within a healthcare organization need to work closely together to ensure a secure environment.

2. Methodology

HIMSS Analytics extended invitations to participate in this telephone-based survey to senior information technology (IT) executives, Chief Security Officers, Chief Medical Information Officers (CMIOs), Chief Information Security Officers and Chief Privacy Officers at hospitals throughout the United States. In addition, HIMSS Analytics contacted individuals at vendor organizations that have Business Associate relationships with healthcare organizations. This information was collected via Web-based survey. For the purposes of this research, organizations were asked to classify themselves as a business associate if they do business for or on behalf of a HIPAA-covered entity

All individuals who participated in this research were either a member of their organization's executive team or reported to a member of the organization's executive team. In order to ensure that respondents were qualified to speak about the security environment at their organization, respondents had to confirm they were involved in the security of data at their organization.

Only one respondent per organization was invited to participate in this survey. A total of 150 respondents from a provider organization and 26 individuals from an organization that has a business associate relationship with provider organizations participated in this research, which was conducted in August and September of 2009.

3. Profile of Survey Respondents

This survey focused on the responses of individuals who were familiar with the security of patient data at their organization and currently members of their organization's executive committee or reported to the executive committee.

Among the respondents working for provider organizations, nearly half of the sample is comprised of senior IT executives, including Chief Information Officers (CIOs) and Vice Presidents of Information Technology (IT)/Directors of IT. Another 15 percent of the sample reported their title to be Chief Privacy Officer; 12 percent indicated that they are either the Chief Compliance Officer or General Counsel and 11 percent identified their title as Chief Medical Information Officer (CMIO). Other titles represented in this research include Chief Security Officer, Chief Medical Officer, medical records professionals or Chief Operating Officer.

Additional analysis was done in this paper by the job title provider respondents reported. For the purposes of this research, provider respondents will be divided into two groups – IT executives and non-IT executives. Each group contains about half of the survey respondents.

Approximately half of survey respondents (55 percent) work for organizations with fewer than 100 beds. Another third (31 percent) work for organizations with between 100 and 299 beds. The final 14 percent of respondents work for a hospital with 300 or more beds. The average number of licensed beds per hospital is 135 and the median is 75 beds.

More than half of survey respondents (57 percent) reported that they work for a general med/surg hospital. Another third work for a critical access hospital and three percent work for an academic organization. The remaining eight percent of respondents work for organizations that can be categorized as pediatric or long term acute.

4. HITECH AND THE ARRA: Awareness, impact and challenges of complying with the new rules

Overall, awareness of the new provisions required by HITECH is high among provider respondents. Only two percent were not aware of these requirements. Awareness among the respondents working for a business associate was lower than among providers—twelve percent of respondents reported that they were not aware of any of these requirements. Respondents also identified several challenges to addressing the HITECH Act, including ensuring that employees are fully trained, getting the proper funding to implement the systems needed and simply understanding the full scope of the rules and regulations outlined by the HITECH Act.

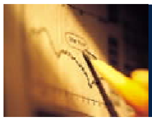
Awareness of data breach risks and regulations

Respondents were asked if the passage of ARRA and the HITECH Act had resulted in a changed level of awareness of data breaches and the risk of a breach. Slightly more than half (57 percent) of provider respondents reported that they now have a greater level of awareness of data breaches and breach risk. More than one-third (37 percent) indicated that there was no change in their level of awareness and two percent said that they were now less aware. Among provider respondents, those working for a larger healthcare organization were more likely to indicate that they now have a greater level of awareness of data breach and breach risk. Below is the number of respondents in each bed-size category that indicated they had a greater level of awareness:

- Under 100 beds – 53 percent
- 100 to 299 beds – 52 percent
- 300 or more beds – 86 percent

The passage of ARRA and HITECH has had more of an impact on the business associate respondents to this survey. Approximately three-quarters (73 percent) indicated that their organization now has a greater level of awareness that their organization might be vulnerable to a data breach. One-quarter indicated that there was no level of change in their awareness level.

HITECH imposes new privacy and data breach notification requirements on healthcare organizations and business associates. This research tests awareness of these provisions in three areas – accountability, breach notification and consumer access. Table One below outlines the percent of respondents who indicated they were aware of these provisions.



Privacy Requirements of HITECH Act

Privacy Requirement	Provider	Business Associate
Accountability		
Beginning in 2010, business associates are bound by the same security and privacy requirements as covered entities.	86.7%	69.2%
Increased penalties for privacy and security breaches, ranging from $25,000 to $1.5 million. Penalties will be mandatory in the event of willful neglect	84.0%	80.8%
State Attorney Generals have explicit authority to file a civil action in federal court relating to HIPAA and HITECH violations in their state.	68.7%	53.8%
Breach Notification		
Beginning in September 2009, mandatory notification to breach victims within 60 days after ANY breach incident.[1]	84.7%	76.9%
Beginning in September 2009, obligation to notify of breach extends to business associates of covered entities.	78.0%	73.1%
Beginning in 2010, mandatory notification of HHS and prominent media outlets if breach is more than 500 records.	63.3%	61.5%
"Temporary" breach notification provision for PHR vendors.	39.2%	23.1%
Consumer Access		
Beginning in 2010, individuals are guaranteed prompt access to their own health records in the form of an electronic copy of data retained in an EHR.	68.0%	42.3%
Beginning in 2010, individuals can restrict disclosure of their records when they pay for their own medical services.	67.3%	50.0%

It is clear from the table above that awareness across all areas is higher among provider respondents. This is particularly notable in the area of consumer access.

[1] This language is what was asked in the original survey. However we do realize that when HHS promulgated the interim final rules, the language was changed to include a breach for which there is significant risk of harm to the individual.

There are also some differences in awareness by organization size. In general, respondents working for larger organizations are more likely to be aware of certain provisions than are those respondents working for smaller organizations. These areas are:

- Beginning in 2010, business associates are bound by the same security and privacy requirements as covered entities
- Beginning in 2010, mandatory notification of HHS and prominent media outlets if there is a breach of more than 500 records
- Beginning in September 2009, obligation to notify of breach extends to business associates of covered entities

In addition, 96 percent of those provider respondents that reported that their organization had had a data breach were aware of the provision that beginning in 2010, business associates are bound by the same security and privacy requirements as covered entities. This can be compared to 82 percent of those respondents that did not report a breach at their organization.

Finally, 90 percent of non-IT respondents at healthcare organizations were aware that beginning in September 2009, it is mandatory to notify breach victims of ANY breach incident within 60 days of the breach. Only 80 percent of IT executives at provider organizations were aware of this provision.

Impact of HITECH on data breach discovery

For the purposes of this research, business associates were defined as an organization doing business for or on behalf of a HIPAA covered entity. Respondents working at a provider organization were asked to indicate whether or not the HITECH Act's expanded requirements about Breach Notification obligations for both business associates and covered entities will result in discovery and reporting more incidents. About two-thirds of respondents (68 percent) indicated that they believe this to be the case. Among provider respondents, there is a mixed level of response to this question. While nearly three-quarters of respondents that work for a small hospital (72 percent) and 86 percent of respondents working for a large hospital (300 or more beds) indicated that they believed that the HITECH Act's expanded requirements will result in discovery and reporting of more breaches, only half (52 percent) of respondents working for a hospital with 100 to 299 beds reported this to be the case.

A slightly higher percent of the business associate respondents (73 percent) also believe this to be the case.

Measures taken to prevent data breaches and comply with new regulations

As a result of the passage of ARRA and HITECH, more than 90 percent of respondents who work for a provider organization indicated that their organization has either changed or planned to change policies and procedures to prevent and detect data breaches. Among respondents at provider organizations, more than three-quarters reported their organization has (or would) provide additional training for their staff. Nearly the same percent reported that their organization would revise their organization's security policies and procedures. "Making additional investments in security tools and/or technologies" was selected by 57 percent of respondents. When these options are looked at categorically, nearly half of respondents (46 percent) reported that their organization would take all of these steps.

While a similar percent of business associate respondents indicated that their organization has (or intends to) take additional steps to prevent and detect data breaches (92 percent), respondents were less likely to take multiple steps to prevent and detect data breaches. In fact, about 70 percent are taking only one or two steps in this direction. More specifically, 62 percent of respondents indicated that their organization is (or intends to) revise the security policies at their organization. Slightly more than half (54 percent) will provide additional training for their staff and one-third will make an investment in additional security tools or technologies.

Perception of HHS enforcement

Finally, the HITECH Act contains provisions that Congress intended to increase enforcement by HHS and HIPAA privacy and security provisions. Compared to the present level of enforcement, nearly 60 percent of provider respondents indicated that the future level of enforcement will be greater. Another 38 percent of respondents indicated that they don't perceive a change in the level of enforcement. Those working for a business associate organization had a different perception in this area. Only 39 percent indicated a perception that the level of enforcement will increase in the future. Another half believed that the level of enforcement will not change. The remaining respondents were not sure if the level of enforcement would change.

Challenges to complying with HITECH Act

Respondents were also asked to identify the biggest challenges to addressing the HITECH Act at their organization. Among the provider respondents, the two biggest challenges identified by respondents were ensuring that employees are properly trained and the costs associated with meeting the requirements put forth in the HITECH Act. Each of these was selected by approximately one-third of respondents.

> "I think the biggest challenge to performing the changes to meet the policy requirements of the HITECH Act is education of the employees and provider education. It is also the cost of the new technology needed and of education".

> "Financing would be the biggest challenge to addressing the changes needed to comply with the HITECH Act. Financing for IT solutions, upgrades in software and cost of staff education would be a challenge".

> "Money would be the biggest challenge, specifically the cost of getting things put into place and of the training. That would be my main concern".

In addition to employee training and the finances needed to meet the requirements, organizations also reported concern about the having to obtain new software and/or having the necessary resources to install the software.

> "The biggest challenge to addressing the HITECH Act at our organization will be converting to total EHR. We are a hybrid right now, meaning partial paper and partial electronic. It may take awhile to actually convert".

> "The biggest challenge is funding for the security systems. The second challenge is the timing of implementation of the upgrades to the system".

> "I think the biggest challenge to addressing the HITECH Act will be the need of more staff members in our department. The medical records department in our organization is made up of only a few members".

Another issue identified by respondents is simply a lack of understanding what the requirements of the HITECH are.

> "The biggest challenge will be understanding the rules. We need to understand what is required of us".

A number of respondents also noted that they were concerned about their business associate relationships.

> “I think the biggest challenge to addressing the HITECH Act at our organization will be to ensure BA compliance and making sure each is aware of the responsibilities that come with these new requirements”.
>
> “The biggest challenge to addressing the HITECH Act at our organization will be monitoring the external activities, including the performance and handling of information by our business associates and covered entities”.

5. Business Associates (BA): How are organizations managing the expanded requirements?

Respondents indicated that the HITECH Act’s expanded requirements for business associates whereby business associates are now directly covered by the HIPAA security rule and some parts of the HIPAA privacy rule, will cause them to take additional steps to protect patient data. Most provider organizations are being proactive in terms of ensuring that the data held by a business associate is not being breached.

About 85 percent of respondents working at a provider organization indicated that they will take some action to ensure that the data held by a business associate is not being breached. Slightly more than half of respondents (57 percent) indicated that their organization will renegotiate their business associate agreements. Another half (49 percent) indicated that they will monitor their business associate’s performance/security posture, while 47 percent indicated that they will terminate business contracts for violations.

Renegotiation of the business associate contract will be more likely among large hospitals than among small hospitals. See below for the percent of each hospital group reporting a “yes” answer to this question.

- Under 100 beds – 48 percent
- 100 to 299 beds – 61 percent
- 300 or more beds – 81 percent

Business associates were asked to identify the steps that the healthcare organizations they work with were taking to ensure that data held by a business associate is not at risk of a breach. While only four percent said that they didn’t believe that healthcare organizations were taking any steps, a full 39 percent indicated that they did not know what steps these organizations were taking. These respondents were most likely (35 percent) to believe that the healthcare organizations they work with will monitor the performance and security posture of their business associates. Another quarter indicated that their provider clients will renegotiate their business associate agreement. Only eight percent indicated that they believe their provider clients will terminate their business associate agreement.

6. Data Breaches: Managing breach exposure and response

While one-third of respondents reported that their organization had experienced a data breach in the past 12 months, nearly three-quarters of these respondents reported that their organization had multiple security breaches. Despite this, respondents were not overly concerned that their organization would be exposed to a future data breach under the new HITECH privacy requirements.

Respondents experience with data breaches

Approximately one-third of respondents (31 percent) indicated that their organization had experienced at least one data breach in the past 12 months. A higher percent of non-IT executives (41 percent) than IT executives (22 percent) reported that they had had a security breach at their organization. By bed size, half of those working for a hospital with 300 or more beds reported a breach, compared to one-third of respondents working for a hospital with 100 to 299 beds and one-quarter of those working for a hospital with under 100 beds.

Seventy (70) percent of these respondents reported that their organization has had more than one breach during this time. Only one respondent who works for a business associate reported that they had a security breach in the past year—the number of breaches was undisclosed.

Among the respondents that indicated that they had a security breach at their organization, approximately 90 percent reported that their organization has taken some action in response to the breach. Respondents were most likely to report that they provided additional training to their staff (83 percent). Approximately two-thirds (63 percent) reported that they revised the security policies/procedures at their organization. Slightly fewer than half (45 percent), reported that they made additional investments in security tools and/or technologies. Approximately 37 percent of respondents indicated that their organization has taken all of these steps. Among the handful of respondents that reported that their organization had not made any changes in response to a breach, a higher percent of IT respondents (18 percent) than non-IT respondents (three percent) reported that their organization had not made any changes.

Measuring breach exposure

Respondents were also asked to identify their organization's risk of exposure to a future data breach at their organization under the new HITECH privacy requirements. Based on a one to seven scale, where one represents "we are at no risk of a breach in the next year" and seven is "a breach will take place at our organization within the next year", respondents working for a provider organization reported an average score of 3.15, indicating that they do not perceive a great risk of a breach in the next year. Those who had already experienced a breach were not much more likely to perceive the risk of a breach in the future – 3.87. Among survey respondents, the likelihood that an organization will be at risk for a data breach in the future by bed size is mixed – large hospitals and small hospitals are more likely than mid-sized hospitals to report that they will be at risk of a breach in the next year. See below:

- Under 100 beds – 3.16
- 100 to 299 beds – 3.09
- 300 or more beds – 3.25

The respondents working for a business associate organization were even less likely to perceive that there would be a security breach at their organization in the next year; they reported an average score of 2.25.
According to survey respondents, most provider organizations use at least one measure to identify exposure to future security breaches; only three percent reported that they do not measure their future risk. The most frequently used measure for identifying exposure is to conduct an internal security risk assessment (87 percent). Fewer than half of respondents (43 percent) reported that their organization conducts a third party provided risk assessment.

More than half of respondents (55 percent) also say they use intrusion detection services. Provider respondents that work for hospitals with between 100 and 299 beds were most likely to report that they used intrusion detection services at their organization. A high percent of respondents who work at hospitals with fewer than 100 beds also used this technology (58 percent). Least likely to use intrusion detection tools were those working for a hospital with 300 or more beds. By title, a higher percent of IT executives reported using intrusion detection than did non-IT executives (64 percent compared to 47 percent).

In comparison, nearly 15 percent of the business associate respondents reported that they do not measure exposure to future security breaches at their organization. The measures used by these respondents to assess exposure are similar to the provider respondents – internal security risk assessment (73 percent); intrusion detection service (58 percent) and third party risk assessment (35 percent).

Managing data breach response

In the event that a data breach occurred at their organization, most respondents (93 percent) reported that their organization would use internal resources to address this issue. However, nearly all those who reported using internal resources supplement these resources with an outside resource such as a third party vendor/consulting firm, legal counsel and/or association. Overall, three-quarters of respondents indicated that their organization did/would turn to a law firm in the event of a data breach. This is particularly the case for larger hospitals. Over 90 percent of respondents working for a hospital with 300 or more beds and 89 percent of respondents working for a hospital with 100 to 299 beds would turn to a law firm in the event of a data breach. In comparison, only 66 percent of respondents working for hospitals with fewer than 100 beds reported they did/would turn to a law firm in the event of a data breach.

Slightly more than one-third (38 percent) would turn to an association such as their state's hospital association, while one-third would turn to a third-party vendor.

Internal resources were also most frequently identified by those working for a business associate organization (69 percent). Half turned to legal counsel; 39 percent turned to a third party vendor/consulting firm and 12 percent turned to an association.

7. Risk Assessment: Components of assessment and tools for breach prevention

The majority of healthcare organizations conduct risk assessments. Reviewing policies and procedures and considering systems vulnerabilities are two key parts of this assessment. Employee privacy and security training is a critical element in protecting organizations from a future data breach. This is the case for respondents from both provider and business associate respondents.

Use of risk assessments

Ninety-one percent of provider respondents indicated that their organization conducted either an internal or third-party risk assessment. Among these respondents, more than half indicated that this risk assessment was conducted within the past year. Only six percent of respondents indicated that it has been at least three years since their organization conducted a formal risk assessment.

Below is a list of the percent of respondents indicating specific areas that were included in their risk assessment; all were selected by at least three quarters of respondents.

- Policy and procedure review – 91 percent
- Considering systems vulnerabilities – 87 percent
- Inventory of personally identifiable information (PII)/protected health information (PHI) – 78 percent
- Regulatory review – 77 percent
- Data on employee compliance – 72 percent
- Tracking external threats – 72 percent

In comparison, only 74 percent of respondents working for an organization classified as a business associate reported that they have conducted a risk assessment. The percent of respondents reporting each of the measures taken is as follows:

- Policy and procedure review – 79 percent
- Considering systems vulnerabilities – 68 percent
- Inventory of personally identifiable information/protected health information – 63 percent
- Tracking external threats – 63 percent
- Regulatory review – 58 percent
- Data on employee compliance – 47 percent

Measures used to prevent data breaches

More specifically, the provider respondents were asked to identify the measures that their organization has in place to protect itself from data breach risk. They were also asked to identify how important these mechanisms are in protecting the organization from a data breach. This data was collected on a one to seven scale, where one is "not at all important" and seven is "highly important". This value is shown in ( ) below.

- Performed employee privacy and security training – 97 percent (6.29)
- Use data encryption – 81 percent (6.25)
- Performed PII/PHI inventory – 65 percent (5.91)
- Use data loss prevention (DLP) software – 43 percent (5.89)
- Own cyber liability insurance – 26 percent (5.31)

It is also of interest to note that there is an association between hospital size and use of data encryption. All of the respondents working for a hospital with 300 or more beds reported that they use this tool. This can be compared to 85 percent of respondents working for a hospital with 100 to 299 beds and 75 percent of respondents working for hospitals with fewer than 100 beds.

Respondents working for a business associate organization were asked to identify the measures that their organization has in place to protect itself from data breach risk and measure their importance.

- Performed employee privacy and security training – 85 percent (6.55)
- Use data encryption – 69 percent (6.33)
- Performed PII/PHI inventory – 42 percent (5.45)
- Use data loss prevention (DLP) software – 19 percent (4.71)
- Own cyber liability insurance – 4 percent (5.00)

8. Conclusions and recommendations

The report draws the following conclusions:

The HITECH Act treats business associates as a covered entity and as such, they need to be prepared to address the implications of a breach violation. The business associates in this survey lag behind the provider respondents in terms of awareness of the information in the HITECH Act. As of 2010, business associates will be bound by the same privacy and security requirements as are other covered entities. Our research demonstrated a difference in awareness of not only this requirement, but other requirements outlined in the HITECH Act, suggesting that additional education is needed in the business associate community. This is critical, as nearly half of covered entities said they were prepared to terminate a contract with a business associate for a data breach violation.

All information that is relevant to the security environment should be included in the risk assessment in order to quantify and mitigate data breach risk. Risk assessments are clearly part of the strategy that healthcare organizations are using to identify gaps in their organizations' security environments. However, only half of the organizations that conduct these assessments are doing them at least yearly. In addition, organizations are not including all aspects of the security environment that they can in the assessment. Specifically, while nearly all are conducting a policy and procedure review as part of this assessment, 25 percent are not tracking external threats or looking at data on employee compliance.

While hospitals are widely providing training for their employees, they are not always monitoring that employees are complying with the organization's policies and procedures on which they were trained. Nearly all respondents reported that they perform employee privacy and security training to protect against data breach risk. Respondents also found this training to be valuable – a 6.29 on a one to seven scale where one is not at all effective and seven is highly effective. However, less than three-quarters of respondents at hospitals that conducted a risk assessment indicated that information on employee compliance is part of the risk assessment.

Respondents working for large hospitals have a higher level of awareness of the potential for a security breach than do respondents working for small organizations. While large hospitals (300 or more beds) were more likely to have had a security breach at their organization than were smaller organizations, respondents at these organizations were also more likely to indicate that the passage of ARRA and HITECH have resulted in a greater level of awareness of data breaches and breach risk at their organization. Larger organizations also appear to be more prepared for the eventuality of a breach – 86 percent of respondents working for a large hospital reported that they believed that the HITECH Act's expanded requirements will result in discovery and reporting of additional breaches. All healthcare organizations, regardless of size, need to be aware of the provisions of HITECH to mitigate breach risk.

There are different levels of awareness between IT and non-IT executives in some key areas of the security environment at healthcare organizations. Non-IT executives are more likely than IT executives to indicate that a breach has occurred at their organization. Furthermore, non-IT executives are somewhat more aware of some key HITECH Act requirements, such as the requirement that notification of breach victims in ANY breach is required within 60 days. Finally, these individuals were somewhat more likely to indicate that their organization had made changes to their security environment as a result of a breach. This suggests that all departments within a healthcare organization need to work closely together to ensure a secure environment.

9. Survey Sponsors

About HIMSS Analytics

A Trusted, Experienced Resource for Healthcare Provider Organizations

HIMSS Analytics supports improved decision-making for healthcare delivery organizations, as well as healthcare IT companies, state governments, financial companies, pharmaceutical companies and consulting firms, by delivering high quality data and analytical expertise. The company collects and analyzes healthcare data related to IT processes and environments, products, IT department composition and costs, IT department management metrics, healthcare trends and purchasing related decisions. It is a wholly-owned not-for-profit subsidiary of the Healthcare Information and Management Systems Society (HIMSS).

About ID Experts

ID Experts provides data breach solutions, risk assessment, forensic investigation and fully managed victim identity restoration to corporations, financial institutions, healthcare organizations and government agencies. As a leader in data breach prevention and remediation, the company has managed hundreds of data breach events, protects millions of individuals from identity theft and authored the Identity Crime Victim's Bill of Rights. ID Experts is actively involved with industry organizations including ANSI/Identity Theft Prevention and Identity Management Standards Panel, International Association of Privacy Professionals, Internet Security Alliance, and the Santa Fe Group. For more information, visit http://www.idexpertscorp.com/.

9. How to Cite This Study

Individuals are encouraged to cite this report and any accompanying graphics in printed matter, publications, or any other medium, as long as the information is attributed to the 2009 HIMSS Analytics Report: Evaluating HITECH’s Impact on Healthcare Privacy and Security sponsored by ID Experts.

10. For more information, contact:

HIMSS Analytics

Joyce Lofstrom
Sr. Manager, Corporate Communications
312-915-9237
jlofstrom@himss.org

ID Experts

Kelly Stremel
MacKenzie Marketing Group
503-225-0725
kellys@mackenzie-marketing.com