



## 2009 HIMSS Security Survey

Statement to the HIT Standards Committee  
Privacy and Security Workgroup

Lisa Gallagher, BSEE, CISM, CPHIMS  
Senior Director, Privacy and Security  
Healthcare Information and Management Systems Society

November 19, 2009

Secretary Chopra, Dr. Blumenthal, Dr. Baker, and members of the Privacy and Security Workgroup, thank you for the invitation to provide testimony today. I am Lisa Gallagher, Senior Director, Privacy and Security for the Healthcare Information and Management Systems Society (HIMSS). HIMSS is the healthcare industry's membership organization exclusively focused on providing leadership for the optimal use of healthcare information technology and management systems for the betterment of healthcare. HIMSS represents more than 23,000 individual, 380 corporate members, and 46 chapters nationwide. HIMSS seeks to shape healthcare public policy and industry practices through its educational, professional development, and government relations initiatives designed to promote information and management systems' contribution to quality patient care.

In the area of privacy and security, HIMSS has a volunteer member-populated Steering Committee, two Task Forces, and several work groups working on creating and maintaining materials for the HIMSS Privacy and Security Toolkit. The "Toolkit" contains the collective work of the volunteer groups to provide resources, best practices, case studies and other tools and information to help member organizations protect health data. In addition, the Privacy and Security Steering Committee coordinates the submission of public comments from HIMSS members relating to HHS, Federal Trade Commission, Food and Drug Administration, Office of Civil Rights, and other rulemaking activities.

### **Background**

Recently, HIMSS conducted the "2009 HIMSS Security Survey." Now in its second year, this survey reports the opinions of information technology (IT) and security professionals from healthcare provider organizations across the U.S. The study collected information on a multitude of topics including access to patient data, access tracking and audit logs, security in a networked environment, and medical identity theft. This year, we have also probed our respondents with regard to their preparedness and approach for meeting new privacy and security requirements contained in the American Recovery and Reinvestment Act (ARRA).

See Reference Document: 2009 HIMSS Security Survey, attached and available at:  
<http://www.himss.org/content/files/HIMSS2009SecuritySurveyReport.pdf>

### **Survey Methodology**

This year's HIMSS Security Survey was a web-based survey conducted between August 21, 2009 and October 5, 2009. A total of 196 individuals responded to the survey which was sponsored by Symantec. Approximately three-quarters of respondents were senior level IT executives, including CIOs, VP of IT and/or Director of IT. While the survey was web-based, it was also an invitation-only survey, whereby we identified individuals with the titles who had direct involvement and/or responsibility for security, such as CIOs and Chief Security Officers.

Nearly three-quarters of respondents indicated that they are a senior Information Technology (IT) executive at their organization. Specifically, 56 percent of respondents indicated that they are the Chief Information Officer at their organization. Another eight percent are Vice Presidents of IT/IS.



Lisa A. Gallagher, BSEE, CISM, CPHIMS  
Senior Director, Privacy and Security  
Testimony before the HIT Standards  
Committee Privacy and Security Workgroup  
November 19, 2009

A similar percent reported that their title is Director of IS. Approximately 17 percent of respondents reported their title to be Chief Security Officer and two percent indicated their title is Chief Privacy Officer. The remaining ten percent of respondents reported their title as “other”, which includes a wide variety of IT and security titles.

Another seventeen percent of respondents were Chief Security Officers. The other participants were other technology and security professionals. The majority of the respondents represent the hospital environment, although there are some respondents from other types of organizations, such as ambulatory facilities included in the research.

For perspective with regard to year-over-year comparison, the 2008 survey had 155 respondents.

### **Key Survey Results:**

Key results, by question category, are summarized as follows:

**Maturity of Environment:** Respondents characterized their environment at a middle rate of maturity, with an average score of 4.27 on a scale of one to seven, where one is not at all mature and seven is a high level of maturity.

**Security Budget:** Approximately sixty percent of respondents reported that their organization spends three percent or less of their organization’s IT budget on information security. This is consistent to the level of spending identified in the 2008 study, and indicates that little additional resources have been applied to information security.

**Formal Security Position:** Fewer than half of respondents indicated that their organization has either a formally designated CISO (Chief Information Security Officer) or CSO (Chief Security Officer).

**Risk Analysis:** Three-quarters of surveyed organizations conduct a formal risk analysis (only half of these conduct this assessment on a yearly basis or more frequently), which has remained the same in the past year. Three-quarters of organizations that did conduct risk assessments found patient data at risk due to inadequate security controls, policies and processes. Conducting this analysis positions organizations to identify gaps in their security controls and/or policies and procedures.

**Security Controls:** Most respondents reported that they use the information generated in their risk analysis to determine which security controls should be used at their organization. About 85 percent of respondents reported that they *monitor* the success of these controls and two-thirds of these respondents *measure* the success of these reports.

**Patient Data Access:** Surveyed organizations most widely use user-based and role-based controls to secure electronic patient information. Approximately half of respondents reported that their organization allows patients/surrogates to access electronic patient information. Patients/surrogates are most likely to be granted access to high level clinical information, such as diagnosis or lab results.

**Management of Security Environment:** Nearly all respondents reported that their organization actively works to determine the cause/origin of security breaches. However, only half have a plan in place for responding to threats or incidents related to a security breach.

**Security in a Networked Environment:** Nearly all respondents reported that their organizations share patient data in an electronic format. Respondents were most likely to report that they share data with state government entities. Respondents also reported that the area in which they are most likely to share data in the future is with Health Information Exchanges (HIEs)/Regional Health Information Organizations (RHIOs).

Approximately half of these organizations (41 percent) indicated that these sharing arrangements have resulted in the use of additional security controls beyond those that were already in place at their organization. This is similar to the data reported in the 2008 survey.

**Future Use of Security Technologies:** E-mail encryption and single sign on and were most frequently identified by respondents as technologies that were not presently installed at their organization but were planned for future installation.

**Medical Identity Theft:** One-third of respondents reported that their organization has had at least one known case of medical identity theft at their organization. However, only a handful of these organizations experienced direct consequences from the breach.

### **Summary/Conclusions**

Results from the 2009 HIMSS Security Survey suggest that, despite changes to the security and privacy landscape including new legal and regulatory requirements and increasing risk, healthcare organizations have made relatively little change since the assessment of the market that HIMSS conducted in 2008 relating to a number of important areas of the security environment. This is reflected in the responding healthcare organizations' assessment of their own readiness for today's risks and security challenges. Respondents characterized their own maturity level as mid-range, budgets dedicated to security remain low, and many organizations still do not have a formally designated CSO/CISO. Also, organizations often do not have a plan for responding to threats or incidents relating to a security breach.

This year's survey data showed that respondents characterized the maturity of their organization's security program as mid-level (4.27 on a scale of one to seven where one is low and seven is high). Spending on security represents only a small percentage of the overall IT budget and fewer than half of respondents indicated that their organization has a formally designated Chief Information Security Officer or Chief Security Officer. Nearly half of the respondents do not currently have a plan for responding to threats or incidents relating to a security breach.

Furthermore, risk assessments are not universal among the responding organizations – only three-quarters perform such an assessment. These results are somewhat concerning considering that the operating environment is becoming more complex due to an increase in adoption of health IT, the prospect of increasing levels of data exchange, new laws and regulations, and an increasingly complex threat environment. These factors may put health data at a higher risk of exposure in the future, and increase the need for mature security processes and controls, based on ongoing risk analysis.

Importantly, of those organizations that do actively perform risk assessments, half (52 percent) indicated that patient data at their organization was found to be at risk as a result of both a lack of effective security controls and a lack of adequate policies and/or procedures. Another 15 percent indicated that their organization's patient data was at risk as a result of a lack of effective security controls in place at their organization and five percent indicated that their organization's patient



Lisa A. Gallagher, BSEE, CISM, CPHIMS  
Senior Director, Privacy and Security  
Testimony before the HIT Standards  
Committee Privacy and Security Workgroup  
November 19, 2009

data was at risk because their organization did not have adequate policies and procedures in place. The risk assessment activity positions organizations to correct deficiencies and the survey data serves to emphasize the important role and value that ongoing security risk analysis can play in protecting health data.

The survey also assessed some aspects of healthcare organizations' readiness to comply with the new privacy statutes in American Recovery and Reinvestment Act of 2009 (ARRA) and related upcoming regulation from Health and Human Services (HHS). For example, under ARRA, healthcare organizations are required to provide notification of data breaches to the patient (as well as HHS and the public in some circumstances) and provide accounting of all disclosures of protected health information upon patient request (for the three years prior to the request). This survey specifically addresses some of the tools that organization's use to gather the data necessary to provide this information.

Results showed that audit logs are widely used among the healthcare organizations represented in this survey. Data from firewalls, application logs and server logs are common sources of information retained in the audit logs. However, at this time, only one-quarter of respondents reported that analysis of log data is done entirely electronically. Many respondents reported that they analyze most, if not all, of the information in these logs through manual means (survey data shows that 38 percent of the organizations conduct only manual log review and an additional 36 percent use some combination of automation and manual review). More clinical data is being created/stored/exchanged in electronic form, the volume of data in logs and audit trails continues to grow. Thus, the need to correlate data from various log sources increases, the need for near real-time, automated reviews based on business rules will only become greater. Without the assistance of some automated/electronic means to analyze log data, organizations may not be well positioned to provide patients with a breach notification. Also, they may have difficulty producing a clear and accurate accounting of disclosures.

In addition, many organizations are not using available technologies to secure data, such as encryption, which is used by just 67 percent of responding organizations to secure data in transmission, while fewer than half encrypt stored data. The use of encryption represents a common security tool to protect data and, with respect to ARRA, can provide a safe harbor for healthcare organizations with respect to breach notification. That is, if organizations use appropriate means to secure data, they may be exempt from the breach notification requirement for breaches of that data. Another notable security control area with a low adoption rate is data loss prevention (which helps protect data confidentiality), and which is implemented in only one quarter of the responding organizations.

Nearly all respondents reported that they currently share data with other organizations and the number of respondents that plan to share information externally in the future is increasing. For instance, the number of respondents participating in health information exchanges (HIEs) is projected to triple in the future among organizations participating in this survey. This increased data sharing will provide added pressure for organizations to be "good business partners" – that is, to be good stewards of what they store and exchange. Finally, state and federal laws and regulations for data exchange, and HIE enterprise data sharing agreements also will apply.

Healthcare organizations today face increasing challenges as they are being urged to adopt electronic health records in the midst of a complex legal, regulatory and risk environment. To effectively secure patient data, it is important that organizations appropriately resource and manage their security initiatives. Trends as reflected in the survey results indicate that organizations are currently required to be extremely efficient in terms of how they are using their



Lisa A. Gallagher, BSEE, CISM, CPHIMS  
Senior Director, Privacy and Security  
Testimony before the HIT Standards  
Committee Privacy and Security Workgroup  
November 19, 2009

resources. These factors will become even more critical in the future, as organizations will have to continue to deal with an increasingly complex operating environment.

In closing, HIMSS looks forward to engaging with the Privacy and Security Workgroup to bring practical solutions to the discussion. At the present time, we are still in an “awareness and education” phase. Healthcare organizations and their business associates need to be educated on the statutory changes in ARRA and have sufficient information so as to actively engage in the public comment periods of the ongoing rulemaking activities.

Through our collective work, HIMSS is confident the healthcare community can address the privacy and security challenges associated with the electronic transfer of healthcare data. HIMSS is prepared to leverage our membership and other resources to ensure data security remains a high priority for the healthcare community.



Lisa A. Gallagher, BSEE, CISM, CPHIMS  
Senior Director, Privacy and Security  
Testimony before the HIT Standards  
Committee Privacy and Security Workgroup  
November 19, 2009