White Paper

Protecting Patient Health Information in the HITECH Era

Security challenges for adopting Health Information Technology to comply with HIPAA and the HITECH Act

Rapid7 Research Series: Security in Healthcare

Introduction

The American Healthcare system is getting a complete facelift thanks to incentives to adopt Health Information Technology introduced by the Health Information Technology for Economic and Clinical Health (HITECH) Act. Signed into law by President Barack Obama in February 2009, the HITECH Act is part of the American Recovery and Reinvestment Act. It is also part of the broader healthcare reform initiative championed by President Obama. That agenda includes a push for the adoption of interoperable data capture, storage and transmission protocols in healthcare systems. New health information technology is considered to be a vital step in the drive to reduce costs, gain efficiencies, and ultimately to improve patient care. This perspective is also held by the Healthcare Information Management Systems Society (HIMSS). HIMSS believes that "lives can be saved, outcomes of care improved, and costs reduced by transforming the healthcare system through the appropriate use of IT and management systems."[1]

However, reports of healthcare data breaches have historically undermined trust in electronic healthcare systems. For this reason, the HITECH Act was designed to both enforce HIPAA regulations, as well as to provide tools to accelerate the adoption of information systems that keep patient health information secure. This paper examines the HITECH Act, describes how the HITECH Act provides enforcement for HIPAA, and outlines the key challenges faced by the healthcare service industry today in protecting patient information in a fashion that meets HIPAA regulatory requirements.

Understanding the HITECH Act: Improving patient care with Technology interoperability

The HITECH Act has come at a time when healthcare data breaches are on the rise. According to the *2009 ITRC Breach Stats Report*, healthcare breaches account for over 66% of all records breached in 2009, which is a 20% increase from 2008.2 Among the high profile data breaches in 2009 were those at Blue Cross Blue Shield and AIG – Medical Excess LLC.3 Data breaches from such high profile health service providers, in addition to the overall magnitude of the problem, continue to sound alarm bells at all levels. The Federal Government reacted by proposing mechanisms that would give the security standards in the existing Health Insurance Portability and Accountability Act (HIPAA) more "teeth". The Verizon Business 2009 Data Breach Investigations Report warned that organizations storing large quantities of data valued by the criminal community should be prepared to detect and defend against very determined, well-funded, skilled, targeted and sophisticated attacks.4

The American Recovery and Reinvestment Act (ARRA), also known as the Economic Stimulus Package, provided more than $20 billion to aid in the development of a robust and comprehensive Health Information Technology (HIT) infrastructure, and assist providers and other entities in the adoption and daily utilization of healthcare IT, particularly regarding the adoption and "meaningful use" of "certified" Electronic Health Records (EHRs) in conjunction with a secure nationwide electronic Health Information Exchange (HIE) network. Approximately $2 billion was specifically earmarked to jump start both the development of data standards and HIE support, as well as to initiate grants, loans and demonstration programs. The overall goal of the HIT and HIE provisions in the Act is to update and ensure the security and protection of patients' Electronic Private Health Information (ePHI), while improving the quality of care and reducing healthcare costs through efficiencies gained by increased data exchange and information system interoperability. This requires covered entities to update not only existing HIT contracts to require vendors to earn any EHR certification that may be required, but also to update existing HIPAA privacy and security policies and procedures.

1 Executive Summary, *A Call to Action – Enabling Healthcare Reform Using Information Technology,* HIMSS

2 Pollack, Doug. (2009, November 4). *Staying HITECH-Healthy: How Healthcare Can Protect Patient Privacy*. Retrieved from: **http://blog.idexpertscorp.com/**

3 Identity Theft Resource Centre (ITRC). (2009, November 3). *2009 Data Breach Stats*, Retrieved from: **http://www.idtheftcenter.org/ITRC%20Breach%20Stats%20Report%202009.pdf**

4 Verizon Business News Release (2009, April 15). *Verizon Business 2009 Data Breach Study Finds Significant Rise in Targeted Attacks, Organized Crime Involvement*. Retrieved from: **http://newscenter.verizon.com/press-releases/verizon/2009/verizon-business-2009-data.html**

Patient information collected and stored in hospitals and other healthcare facilities is a prime target for criminals, because these records contain valuable data such as names, mailing addresses, Social Security Numbers, insurance policy information, medical history, dates of birth, and sometimes, credit card or other financial information.

According to one report, "there is more data in one (patient) record than in those of any other source such as banks, schools, or HR departments."5 The rise of breaches in hospitals, despite more stringent privacy regulations, is due to more hospitals integrating their electronic records. Pam Dixon, the Executive Director of the World Privacy Forum, states: "until recently, we were in an era of privacy through obscurity,"6 meaning that it was possible to get information on a patient from paper records, but that it was not easy to share that information. Now that medical information is often shared electronically, there is a far greater need for increased data control.

The ARRA designated $20.2 billion in funding earmarked for healthcare IT through the HITECH Act for facilities that adopt "meaningful use" of "certified" electronic medical records. In the words of Robinsue Frohboese, Acting Director and Principal Deputy Director of Office of Civil Rights at the HHS, "these protections will be a cornerstone of maintaining consumer trust as we move forward with meaningful use of electronic health records and electronic exchange of health information."7

Enforcing HIPAA's Security Rule with HITECH

The role of HIPAA

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is enforced by the Department of Health and Human Services (HHS). HIPAA began as a "portability act" to help individuals keep their health insurance coverage as they moved from one job to another, but it has evolved to include much more.

Title I deals with HIPAA's original intent in that it protects health insurance coverage for workers and their families when they change or lose their jobs.

Title II extends that original intent by protecting the privacy, confidentiality, integrity, and availability of an individual's personal healthcare information. Its Administrative Simplification (AS) provisions, the most significant part of Title II, address the security and privacy of healthcare data.

These rules apply to "covered entities," as defined by HIPAA and HHS, including all healthcare organizations that create, receive, maintain, or transmit patient healthcare information. These include:

- Healthcare providers
- Health plans
- Healthcare clearinghouses such as billing services and community health information systems
- Medicare prescription drug card sponsors

Security provisions for HIPAA compliance are designed to help healthcare service providers and their business associates mitigate the risk of becoming a victim of data loss. Theft of valuable patient information leads to the loss of trust in the usage of electronic health records (EHRs) that are used by healthcare providers to share information. This loss of trust reduces the adoption of EHRs, which erodes patient care. To protect patient information, the HITECH Act has tied the utilization of EHRs back to adoption of the HIPAA Security Rule. The Security Rule is addressed in Title II of HIPAA as part of the Administrative Simplification (AS) provisions which address both the security and privacy of electronic health data as part of the three rules: the Electronic Data Interchange Rule, the Privacy Rule, and the Security Rule.

---

5 Health Information and Management Systems Society (2008, April). *2008 HIMSS Analytics Report: Security of Patient Data*, Retrieved from: http://www.mmc.com/views/Kroll_HIMSS_Study_April2008.pdf

6 Poremba, Sue Marquette (2008, May 14) "Medical data breaches on the rise", *SC Magazine*, Retrieved from: http://www.scmagazineus.com/Medical-data-breaches-on-the-rise/article/110114/

7 Health and Human Services Press Release (2009, August 19). *HHS Issues Rule Requiring Individuals Be Notified of Breaches of Their Health Information*, Retrieved from: **http://www.hhs.gov/news/press/2009pres/08/20090819f.html**

To achieve HIPAA compliance, covered entities must demonstrate adherence to the Security Rule. The Security Rule mandates protection of all electronic Personal Health Information (ePHI) created, received, maintained, or transmitted by any covered entity. This is primarily achieved through the application of requirements in three main categories of safeguards: Administrative, Physical, and Technical.

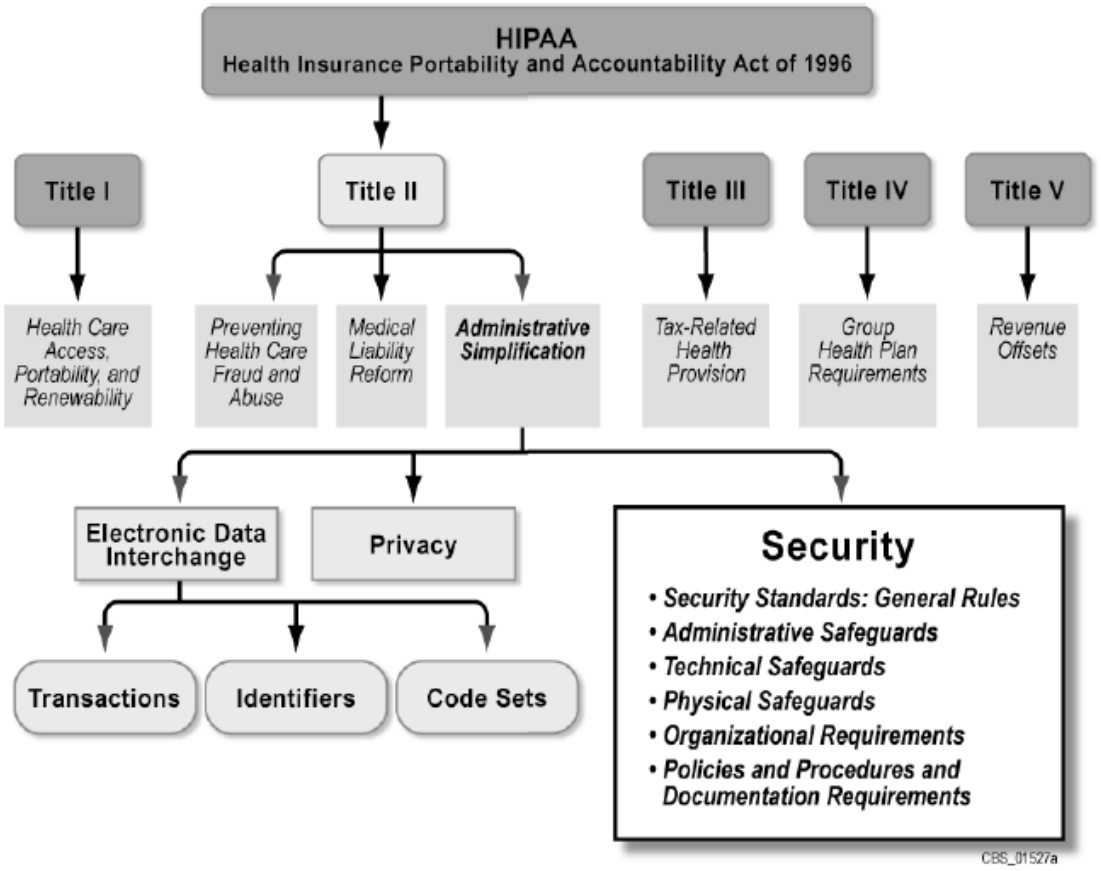

Figure 1 - HIPAA components[8]

The most relevant Administrative Safeguards are:

A contingency plan should be in place for responding to emergencies. Covered entities are responsible for backing up their data and having disaster recovery procedures in place. The plan should document data priority and failure analysis, testing activities, and change control procedures.

Internal audits play a key role in HIPAA compliance by reviewing operations with the goal of identifying potential security violations. Policies and procedures should specifically document the scope, frequency, and procedures of audits. Audits should be both routine and event-based.

The category of Technical Safeguards is also important. The most relevant of those are:

- Information systems housing electronic Patient Health Information (ePHI) must be protected from intrusion. When information flows over open networks, encryption must be utilized.
- Covered entities must make documentation of their HIPAA practices available to the government to determine compliance.

8 National Institute of Standards and Technology (2008, October). *NIST Special Publication 800-66, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule* (Revision 1), 2. Retrieved from: **http://csrc.nist.gov/publications/nistpubs/800-66-Rev1/SP-800-66-Revision1.pdf**

In addition to policies, procedures and access logs, IT documentation should also include a written record of all configuration settings on the components of the network, because these components are complex, configurable, and always changing.

Documented risk analysis and risk management programs are required. Covered entities must carefully consider the risks of their operations as they implement systems to comply with the act.

All of these HIPAA regulations designed to protect the privacy of patient information have meant that many health-care organizations routinely conduct internal audits of their IT environment and produce reports that demonstrate their HIPAA compliance. HIPAA auditors perform HIPAA Risk Assessment Audits using a comprehensive checklist based on Health and Human Services (HHS) regulations and guidance in NIST Special Publication (SP) 800-66. This audit checklist is used to gather evidence that specific administrative, physical, and technical safeguards are in place, and available for inspection by the HHS Office of Civil Rights (OCR).

In terms of security, the audit must provide evidence that the organization meets the electronic Personal Health Information (ePHI) protection regulations required to achieve HIPAA compliance in accordance with relevant sections of §164.308 to §164.316 of the HIPAA Security Rule. HIPAA does not restrict the risk assessment to a single methodology. Instead, HIPAA requires covered entities to periodically review and update its security measures and documentation in response to environmental and operational changes that affect security of its ePHI, and to refer to the comprehensive risk assessment program described in NIST SP 800-30.

Despite HIPAA's extensive and detailed sets of rules and regulations, healthcare organizations tended to ignore HIPAA provisions since the regulation had not been rigidly enforced. But that has all begun to change, thanks to the passage of the HITECH Act as part of the ARRA. The $20B in ARRA funding earmarked for healthcare IT provides the funding to begin serious audit enforcement measures to support HIPAA.

The role of HITECH

The HITECH Act greatly expands the strength and scope of HIPAA in that it includes "new and far-reaching provisions concerning the privacy and security of health information that will materially and directly affect more entities, businesses and individuals in more diverse ways than ever before."[9]

HIPAA officials are now required to conduct far tougher audits and to issue far more severe penalties. The HITECH Act:

- Immediately increases the amounts of monetary penalties for HIPAA violations
- Obligates the HHS Secretary to establish, within three years, regulations that will allow individuals harmed by privacy and security violations to receive a portion of those monetary penalties
- Authorizes each state attorney general to pursue civil action against those who have violated HIPAA privacy and security mandates and to obtain statutory damages on behalf of those parties affected
- Obligates business associates to comply with HIPAA by developing and implementing *comprehensive* written security policies and procedures with respect to the healthcare information they handle
- Strengthens many of HIPAA's privacy and security requirements by detailing specific violations, penalties, and deadlines for compliance

Penalties for non-compliance

Legal costs, individual lawsuits from patients, class-action lawsuits from parties seeking damages, and fines from state and federal regulatory bodies can cost millions of dollars. One insurer estimated that the August 2009 loss of just 38,000 patient records from the Naval Hospital Pensacola will cost the hospital approximately $6 million. Stricter enforcement requirements and higher penalties for HIPAA violations were signed into law in February under the ARRA HITECH Act using the following tiered approach to HIPAA privacy violation penalties:

---

9 *HITECH Act Greatly Expands Scope of HIPAA's Applicability and Enforcement and Increases Civil Monetary Penalties for Violations*, by Helen Oscislawski and Michael J. Kline, February 20, 2009

Tier	Description of violation	Penalty
A	Violations in which the offender didn't realize he or she violated the Act and would have handled the matter differently if he or she had	$100 fine for each violation Total imposed for such violations cannot exceed $25,000 for the calendar year
B	Violations due to reasonable cause, but not "willful neglect"	$1,000 fine for each violation Fines cannot exceed $100,000 for the calendar year
C	Violations due to willful neglect that the organization ultimately corrected	$10,000 fine for each violation Fines cannot exceed $250,000 for the calendar year
D	Violations of willful neglect that the organization did not correct	$50,000 fine for each violation Fines cannot exceed $1,500,000 for the calendar year

Figure 2 - HITECH Act fines[10]

These increased fines reflect the importance the Federal Government has placed on safeguarding the patient information. Faced with the threat of steep fines from failing a HIPAA audit, healthcare services are working with an increased sense of urgency to become HIPAA compliant.

The HITECH Act extends civil and criminal liability under HIPAA to business associates of other HIPAA covered entities, includes provisions for imprisonment of violators, and clarifies that criminal penalties may apply to an individual or employee of a covered entity that obtains PHI without authorization.

HIPAA regulations originally did not provide for a private right of action, meaning that patients cannot file suit in court based upon alleged HIPAA violations. The HITECH Act heightens HIPAA enforcement by authorizing state attorneys general to file suit on behalf of their residents, levy fines and seek attorneys' fees from covered entities on behalf of victims of HIPAA violations. Courts now have the ability to award costs. One prominent example is that of New York State's attorney general Andrew Cuomo, who has already pursued legal action against six facilities and issued a letter to over 600 other healthcare services. The Cuomo Letter, as it is now called, put healthcare service providers on notice that the NY State Attorney General's office would vigorously prosecute facilities found to be violating HIPAA by either selling or being otherwise negligent in their duty to keep patient information confidential and adequately secured.

With the Department of Health and Human Services (HHS) enforcing HIPAA breach notification rules starting in February 2010, healthcare service providers are now scrambling to find ways to ensure they are HIPAA compliant in order to beat the 2010 deadlines.

10 HIPAA Weekly Advisor (2009, March 16) "HIPAA and the HITECH Act: Know the level of penalties", *HCPRO online*, Retrieved from: http://www.hcpro.com/HIM-229707-866/HIPAA-and-the-HITECH-Act-Know-the-level-of-penalties.html

RAPID7

Using HITECH/HIPAA for real-world threat management: Top three challenges for protecting patient health information

There are three real-world challenges that organizations need to meet if they want to stand a chance defending themselves in the rapidly evolving threat landscape:

1. **Defending systems against attacks from external sources.**
   Preventing sophisticated external resources requires tools and techniques that mimic cyber attacks from external intruders.

2. **Protecting Web applications and Web servers from being compromised.**
   Most automated vulnerability scanning solutions are unable to detect SQL injection and cross-site scripting vulnerabilities, so finding one that does is critical for thwarting real-world cyber attacks.

3. **Deciding what criteria to use when contracting security services out to a third-party.**
   Whether it is due to the lack of security programs, tools used, or lack of training, the fact is that few victims discover their own breaches.

RAPID7

Top three challenges for protecting patient health information

	Challenge	Why[1]	Solutions
1	Defending systems against attacks originating from external sources.	Most data breaches investigated were caused by external sources. 74% of breaches resulted from external sources, while 32% were linked to business partners and only 20% were caused by insiders.	HIPAA risk assessment audits must include testing physical infrastructures, technical system controls, and interfaces with personnel. A vulnerability scanning solution with the ability to perform both internal and external vulnerability scanning is required at a minimum. Security best practices also include following-up with additional external penetration testing.
2	Protecting Web applications and Web servers from being compromised.	Nearly 99% of all breached records were compromised from Web servers and Web applications. Of those breaches, 64% were attributed to hackers using a combination of attack methods. For example, hackers using Web browser vulnerabilities would exploit the trust of a victim, and then leverage that trust to gain access into other systems on the network, followed by further exploits that lead to malware being installed inside the network that could then continue harvesting and transmitting more personal information to the hacker.	HIPAA risk assessment audits must use solutions that test Web servers and Web applications from SQL injection and cross-site scripting vulnerabilities. A vulnerability scanning solution with the ability to detect SQL injection and cross-site scripting (XSS) attacks is required at a minimum. Security best practices would include following-up with additional external penetration testing.
3	Deciding what criteria to use when contracting security services out to a third-party.	In 2009, 69% of breach cases were discovered by third-parties and not by the organization themselves. During the last five years, relatively few victims have discovered their own breaches whether due to process or technology deficiencies.	HIPAA risk assessment audits are more effective if ongoing security management programs use vulnerability scanning to establish and measure against a baseline. Security best practices would include following-up with additional external penetration testing.

Conclusion

The HITECH Act signifies a significant win for citizens and security advocates alike, thanks to the significant provisions it added for enforcement privacy, security, and breach notification measures for HIPAA. The American healthcare system is on the path towards "meaningful use" of EHRs, thanks to the much needed funding for adoption of HIT provided by the HITECH Act. The challenge faced by HIPAA-covered healthcare service entities is to achieve HIPAA/HITECH compliance by selecting an appropriate mix of technology, process and security expertise to secure their ePHI from data breaches by confronting real-world threats head on. How quickly they meet this challenge will determine how effective they are at protecting ePHI from falling into the hands of criminals intent on stealing identities and committing frauds for financial gain. The success of the healthcare providers will also rely upon whether they can avoid the newly instituted penalties introduced by the HITECH Act, and avoid the further loss of public trust from continued data breaches. The February 1, 2010 breach notification enforcement deadline sends healthcare providers a firm message; either secure patient data or pay a hefty price, both financially and in the court of public opinion.

About Rapid7

Rapid7 is a leading provider of IT security risk management software. Its integrated **vulnerability management** and **penetration testing** products, Nexpose and Metasploit, and **mobile risk management** solution, Mobilisafe, enable defenders to gain contextual visibility and manage the risk associated with the IT environment, users and threats relevant to their organization. Rapid7's simple and innovative solutions are used by more than 2,000 enterprises and government agencies in more than 65 countries, while the Company's free products are downloaded more than one million times per year and enhanced by more than 175,000 members of its open source security community. Rapid7 has been recognized as one of the fastest growing security companies by Inc. Magazine and as a "Top Place to Work" by the Boston Globe. Its products are top rated by Gartner®, Forrester® and SC Magazine. The Company is backed by Bain Capital and Technology Crossover Ventures. For more information about Rapid7, please visit **http://www.rapid7.com**.

(Footnotes)

1 Based on investigation results found by Verizon Business as published in the Verizon Business 2009 Data Breach Study