A White Paper for Health Care Professionals

Preparing for the HIPAA Security Rule Again; now, with Teeth from the HITECH Act!

Introduction

Several years ago we first published "A White Paper for Health Care Professionals: Preparing for the HIPAA Security Rule". This new paper updates that very popular original guide.

The Health Information Technology for Economic and Clinical Health (HITECH) Act, which was enacted as part of the American Recovery and Reinvestment Act of 2009, significantly modified and strengthened many aspects of the HIPAA Security Rule, including the penalties that the HHS could impose for violations of the HIPAA rules.

It's time to get serious! After essentially ignoring the law for five years, Covered Entities and, now, Business Associates need to get serious! As an example, the deadline for Business Associates of Covered Entities to become fully compliant with the Security Rule is February 17, 2010.

Benefit from our expertise – complete a HIPAA Security Rule refresher, learn about the sweeping changes to HIPAA overall and the Security Rule and Contingency Planning, in particular, and jump-start your Security Rule compliance efforts with our specific guidance.

As a reminder, the Health Insurance Portability and Accountability Act (HIPAA) comprises three sets of standards — transactions and code sets, privacy, and security. The goals of these standards are to:

- Simplify the administration of health insurance claims and lower costs.
- Give individuals more control over and access to their medical information.
- Protect individually identifiable medical information from threats of loss or disclosure.

The HIPAA Security Final Rule, the last of the three HIPAA Rules, was published in the February 20, 2003 Federal Register with an effective date of April 21, 2003. Most Covered Entities (CEs) had two full years -- until April 21, 2005 -- to comply with these standards. Most covered entities, especially providers, did not comply by that date and are still non-compliant.

In general, the Security Rule protects electronic patient health information (EPHI) whether it is stored in a computer or printed from a computer.

The Security Rule is comprehensive including 18 standards defining with what safeguards those covered by the Rule must implement and 35 specifications that describe how the standards must be implemented. The documentation requirements for the Security Rule are daunting. In fact, there are two standards in the Rule covering policies and procedures and documentation. In some cases, no guidance is provided for how the standards must be implemented.

Not surprisingly, few covered entities including a miniscule number of medical practices took serious action to comply with the law. Enforcement was equally weak with an approach that was complaint-driven and not proactive.

Most experts originally agreed that the HIPAA Security Rule requirements are much more extensive than the HIPAA Privacy Rule! To make matters worse, most healthcare companies or medical practices covered by the Rule had and still have limited staff resources to implement an initiative to comply with the Security Rule. And available information security consulting expertise in many communities may be limited and expensive. The upshot has been: very poor information security in the healthcare industry.

Enter the HITECH Act which many describe as a "game-changer" and "ground-breaking". Many accurately observe that healthcare industry woefully unprepared for major changes in fifteen (15) key areas. Without a doubt, HITECH is the largest and most consequential expansion and change to the federal privacy and security rules ever. The fifteen (15) change areas comprise new federal privacy and security provisions that will have major financial, operational and legal consequences for all hospitals, medical practices, health plans, and now their "business associates," and some vendors and service providers that were not previously considered "business associates."

This white paper, presented in the form of Frequently Asked Questions, will help you prepare for the original sweeping changes in the way you must do business under the terms of the HIPAA Security Rule and includes specific updates to the Security Rule required by the HITECH Act.

This paper also specifically highlights and addresses the Contingency Plan Standard and its explicit requirements around data backup and recoverability. Data Mountain provides the best online data backup, archiving, recovery and protection services in the world that help Covered Entities and Business Associates meet the stringent data protection requirements of the HIPAA Security Rule and HITECH Act.

Frequently Asked Questions about the HIPAA Security Rule and HITECH

Q1. Why do I need to be HIPAA Security compliant?

The HIPAA law requires all health care Covered Entities (CEs) and their Business Associates (BAs) to safeguard the privacy of patient health information. The HIPAA law also requires CEs and BAs to implement required security measures to protect patient health information.

Q2. What is a "Covered Entity?"

Covered Entities (CEs) include all health care providers (doctors, dentists, therapists, psychologists, pharmacists, etc.), health care clearinghouses, and health plans (i.e., health insurance companies) that electronically store, process or transmit electronic protected health information (EPHI).

Previously, any business associate of these CEs who by agreement has access to this EPHI was required to comply with the Security Rule as well by means of a so-called BA Agreement. The HITECH Act now explicitly places the same comprehensive Security Rule requirements on BAs to ensure that the same level of security is consistent throughout whenever health information is accessed or exchanged between organizations.

Q3. What are the objectives of the HIPAA Privacy and Security Rules?

The objectives of these rules are to:

- Ensure confidentiality, integrity, and availability of all EPHI that a CE or CE business associate creates, receives, maintains, or transmits.
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such EPHI.
- Protect against any reasonably anticipated losses or disclosures of EPHI.

Q4. What is the difference between the HIPAA Privacy Rule and the HIPAA Security Rule?

The Security and Privacy Rules are distinct rules but they are inextricably linked. The privacy of information depends in large part upon existence of security measures. The HIPAA Security Rule defines the standards that CEs must implement to provide basic safeguards to protect EPHI. The Privacy Rule sets the standards spelling out how CEs should control EPHI.

In general, the Privacy Rule covers protected health information (PHI) in all forms while the Security Rule only covers PHI in electronic form.

The HITECH Act makes significant changes to all provisions of HIPAA of which the Privacy Rule and Security Rule are a part.

Q5. What does HIPAA mean by "EPHI" and "electronic media?"

In general, patient health information that has been converted to, stored in, or transmitted by electronic media is deemed to be "EPHI" and as such is to be controlled and protected under the HIPAA Privacy and Security Rules.

"Electronic media" is defined as:

- Any electronic storage media including memory in computers (hard drives)
- Any removable or transportable digital memory medium (magnetic tapes or disk, optical disk, or memory card)
- Transmission media used to exchange information electronically (Internet, leased lines, dial-up, intranets, and private networks)

Q6. Does the Security Rule cover all patient health information?

There is an exception. PHI transmitted by FAX or telephone is not covered by the HIPAA Security Rule, although this information is covered by the HIPAA Privacy Rule.

Q7. What is the definition of "common control?"

"Common control" exists if a CE has the power, directly or indirectly, to influence or direct the actions or policies of another entity (e.g., a business associate) in a significant way. This means that CEs as custodians of PHI must secure this information and take appropriate actions to ensure that outside vendors, they contracted with, also take the necessary safeguards to control and protect this PHI. As mentioned, the HITECH Act now makes the compliance, enforcement and penalties for BAs explicitly clear in that they are also completely covered by the law.

Q8. What is a "standard" as defined by the Security Rule?

A standard is a provision of the Security Rule that all CEs must comply with, specifically with respect to EPHI. There are no exceptions. There are 19 standards defined in the Security Rule. With HITECH, the number of Standards has not changed; however, more explicit guidance and clarity is provided in many areas of the Security Rule and the Privacy Rule as well.

Q9. What are "implementation specifications?"

Generally, a standard defines what a CE must do while an "implementation specification" describes how it must be done. There are two types of specifications, those that are "required" and those that are "addressable." Required implementation specifications are critical and CEs and BAs, must implement them.

Addressable implementation specifications may or may not be implemented depending on the outcome of a security risk analysis. For an addressable specification, a CE or BA must:

- **ASSESS** whether the specification is a reasonable and appropriate safeguard,
- **AND** implement the specification if it is reasonable and appropriate,
- **OR** document why it is not reasonable and appropriate,
- **AND** implement an equivalent alternative measure if one can be identified as reasonable and appropriate.

For years, we have been advising both CEs and BAs treat both "required" and "addressable" specifications as "required". First, it simply makes good business and risk management sense. Second, data and information is becoming more and not less vulnerable and privacy and security laws are only going to become more stringent over time.

Q10. What is a "risk analysis?"

A fundamental design principle in the Security Rule was that "one size does not fit all". That is, organizations needed to first understand the law, second assess their risks vis-à-vis the law and, third, take appropriate actions for their organization to mitigate their risks in order to comply with the law.

"Risk" is defined as the degree or likelihood that a certain threat or vulnerability will occur, resulting in a breach of safeguards designed to provide control or protection of patient health information. Risk is quantified by taking into account two factors involving (1) the likelihood and (2) the impact (criticality) of loss.

A "risk analysis" is a systematic and comprehensive assessment of all aspects of information including electronic conversion, processing, storage, or transmission that could potentially compromise the integrity of patient health information. Thus, the scope of a risk analysis should address all facets of the CE's and BA's computer hardware, software, and networks and associated electronic equipment and systems.

The initial risk analysis should also assess security policies and procedures and technical safeguards, to determine the extent to which they meet the standards contained in the Security Rule. Then CEs and BAs must perform ongoing risk analyses in response to environmental or operational changes.

Risk analysis findings should identify levels of risk and make recommendations to reduce these risks to a reasonable and appropriate level. These findings and their remedies should be documented and retained as a permanent component of the HIPAA Security Rule compliance program. This documentation should take the form of:

- Security Gap Analysis (depicting the difference between the current and the optimal levels of risk)
- Risk Remediation Plan (outlining the process for achieving the optimal levels of risk)

A CE or BA can choose to have a third party perform the risk analysis and thus provide an independent assessment of the organization's security with respect to the HIPAA Security Standards.

Q11. What kinds of threats to security do CE's face today?

The Security Rule was designed to protect the confidentiality, integrity, and availability of EPHI. Health information that is stored on a computer, processed or transmitted across computer networks, including the Internet, is vulnerable to and must be protected from:

- Hacker and disgruntled employee abuse
- Untrained personnel mishandling
- Exploitation by people not having a "need to know"
- Unplanned system outages
- Burglary and theft
- Fire, flood, and other natural disasters

The Security Rule requires CEs and BAs to assess their exposure to these and other threats.

Q12. What safeguards does the Security Rule mandate for the protection of EPHI?

The Security Rule mandates certain technology-neutral, flexible, and scalable administrative, physical, and technical safeguards that outline which technologies, policies, and procedures should be put in place to ensure adequate ongoing protection of EPHI. These are all based on information security best practices, many of which have been around for decades.

The original HIPAA security provisions did not mandate use of any particular technical system or safeguards. No specific guidance was provided, there was no mandate on any specific technology or approach and solutions implemented to protect EPHI were Self-risk assessment based.

The HITECH Act changes this, to a degree. The Department of Health and Human Services ("HHS") must issue guidance annually on the "most effective and appropriate technical safeguards for use in carrying out" the HIPAA security standards.

Although the statute does not state that the technical safeguards set forth in HHS guidance are the only effective and appropriate technical means of satisfying HIPAA security safeguards, they are the "most effective and appropriate" means of security compliance. Those covered entities and business associates who choose not to comply with the HHS guidance should justify their choice of technical systems that are not the most effective and appropriate means of compliance.

Q13. What are some of the electronic security techniques that CEs may have to consider to be compliant?

The HIPAA Security Standards are largely technology-neutral. Standards are categorized into Administrative, Physical and Technical. The five technical safeguard standards are: access control, audit controls, integrity, person or entity authentication, and transmission security. Each standard has implementation specifications, which can be *required* or *addressable*. Remember, addressable does not mean "optional." The rule lays out the requirements and it is up to each individual organization to determine how to best meet the requirements, including which specific security technologies to implement. Now, however, on an annual basis, HHS is required to issue "…guidance on the most effective and appropriate technical safeguards". HHS is required to assess advances in information technology and security measures that CEs and BAs may use to control and protect their EPHI including:

- Firewalls
- Encryption
- Password authentication
- Digital signatures
- Secure, remote data backup
- Biometric access methods
- Anti-Spyware and Anti-virus software
- Security Auditing and Logging
- Smart cards
- Computer physician order entry (CPOE) systems

Q14. When must CEs and BAs have to comply with the provisions of the Security Rule?

Most CEs were required to be in compliance with the Security Rule by April 21, 2005. However, a large portion of the Privacy Rule required certain Security Rule components to be in place as of April 14, 2003.

BAs must be fully compliant with the Security Rule by February 17, 2010. Remember, HITECH is a game-changer, especially for BAs.

- All of the HIPAA security administrative safeguards, physical safeguards, technical safeguards, and security policies, procedures, and documentation requirements apply directly to all business associates.
- HHS (and state attorneys general under the new enforcement provisions) may impose fines directly against business associates of HIPAA covered entities who do not comply with these HIPAA security standards.
- New business associate security requirements must be added to all business associate agreements
- All civil and criminal penalties applicable to covered entities for violating the security provisions are also applicable to business associates.

Q15. What are the consequences for non-compliance?

The original *proposed* Security Rule listed penalties ranging from $100 for violations and up to $250,000 and a 10-year jail term in the case of malicious harm. However, the final Security Rule stated that a separate regulation addressing enforcement would be issued at a later date. Therefore, under the final Security Rule:

- A penalty could be no more than $100 for each violation or $25,000 for all identical violations of the same provision
- A CE could bar the secretary's imposition of a civil money penalty by demonstrating that it did not know that it violated the HIPAA rules.
- BAs were not directly subject to liability and penalties

Here again, HITECH raises the ante literally in a very significant way. For example, a New Civil Monetary Penalty (CMP) System makes monetary penalties mandatory for violations involving "willful neglect" as of Feb. 17, 2011. Subsection 13410(c), which requires civil penalties that are collected under the HITECH Act to be funneled back into the Department of Health and Human Services' Office of Civil Rights enforcement budget. Section 13410(d) of the HITECH Act strengthened the enforcement by establishing tiered ranges of increasing minimum penalty amounts, with a maximum penalty of $1.5 million for all violations of an identical provision. A CE and now, a BA, can no longer bar the imposition of a civil money penalty for an unknown violation unless it corrects the violation within 30 days of discovery.

The Tiered CMP System:

- Tier A is for 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, and
  - $25,000, maximum total imposed for the calendar year.
- Tier B is for violations due to reasonable cause, but not "willful neglect."
  - $1,000 fine for each violation, and
  - $100,000, maximum total imposed for the calendar year.
- Tier C is for violations due to willful neglect that the organization ultimately corrected.
  - $10,000 fine for each violation, and
  - $250,000, maximum total imposed for the calendar year.
- Tier D is for violations of willful neglect that the organization did not correct.
  - $50,000 fine for each violation, and
  - $1,500,000, maximum total imposed for the calendar year.

The new level of CMPs applies immediately to all violations. HHS will use the CMP proceeds to further enforce the HIPAA privacy and security standards and within 3 years of enactment, HHS must promulgate a regulation to distribute a portion of CMP proceeds directly to harmed individuals which will provide a direct incentive for individuals to report alleged violations to HHS and state attorneys general. It's going to get exciting!

At the same time, there are other perhaps more serious consequences for CEs than potential penalties. These include the loss of the CE's reputation and expensive lawsuits. Should a security breach occur in which EPHI is accessed by an unauthorized user, a CE could lose the trust of its patients, members, physicians and partners, and so on. HIPAA's high standard could be cited in civil litigation thereby creating the potential for huge settlements.

Q16. In summary, what are the most significant changes brought about by the HITECH Act?

Before, during and after the HIPAA Security Final Rule went in law in April 2005, there was confusion and turmoil from CEs, BAs, security professionals and government officials. It took years for people to figure out their roles and requirements under the then-new rules… and many still have not complied.

Now, with the issuance of changes under the HITECH Act, as part of American Recovery and Reinvestment Act (ARRA) of 2009, it's still surprising to hear some of the mis-statements.

- *"Our XYZ product is HIPAA compliant"*
- *"The HITECH Act doesn't change HIPAA, it just pushes electronic records."*
- *"It doesn't apply to my small medical practice."*
- *"Business Associates have to comply just as they did before."*
- *"Installing the EMR doesn't change the what we do in our office."*
- *"Enforcement is only for Covered Entities; BAs just follow the contract."*

NOT!

As stated above, HITECH is the largest and most consequential expansion and change to the federal privacy and security rules ever. The fifteen (15) change areas comprise new federal privacy and security provisions that will have major financial, operational and legal consequences for all hospitals, medical practices, health plans, and now their BAs and some vendors and service providers that were not previously considered BAs.

Following is a listing of key change areas brought about by the HITECH Act:

Enforcement is strengthened significantly

1. Penalties are increased in the new Civil Monetary Penalty (CMP) System
2. Enforcement is more proactive, more punitive and by more parties
3. Additional audit authority is now provided to HHS audit CEs and BAs

Business Associates and others are fully and completely "in scope"

4. BAs are now statutorily obligated to comply with the relevant regulations.
5. Adds temporary breach notification requirements to vendors of personal health records

Security Provisions are strengthened and clarified

6. Data protected is expanded beyond EPHI to include other personal information
7. More specific guidance on technical safeguards is provided by HHS annually
8. New data breach notification requirement is first-time Federal legislation on same

Privacy Provisions are strengthened and clarified

9. Individual right to request restrictions on use and disclosure of PHI is now mandatory
10. The definition of "minimum necessary" PHI to use/disclose is clarified
11. Disclosure accounting is strengthened - eliminates any exceptions from the disclosure accounting rules
12. Tightens restrictions on use of protected health information for marketing purposes
13. Requires clear and conspicuous opt-out opportunity for fund-raising communications
14. Consumers now have the right to receive an *electronic* copy of their PHI
15. Prohibits a CE or BA from receiving payment in exchange for any PHI

Q17. What is the Contingency Plan Standard and what must I do to comply?

The Contingency Plan Standard is one of nine (9) standards in the Administrative Safeguards category of the HIPAA Security Final Rule. As a reminder, there are a total of eighteen (18) standards in three safeguards categories: Technical, Physical, and Administrative.

It is important to note that the Contingency Plan Standard is not a Technical safeguard; this underscores the importance of contingency planning as an important business risk management problem and not an "IT problem".

This Standard is very explicit about, among risk management actions, backing up EPHI and ensuring its recoverability in the event of a data loss event. Like all others, this standard has implementation specifications, which can be *required* or *addressable*. Remember, addressable does not mean "optional."

The exact wording in the law follows below:

§ 164.308 Administrative safeguards.

(7) *Standard:*

(i) *Contingency plan.* Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

(ii) *Implementation specifications:*

(A) *Data backup plan (Required).* Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.

(B) *Disaster recovery plan (Required).* Establish (and implement as needed) procedures to restore any loss of data.

(C) *Emergency mode operation plan (Required).* Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.

(D) *Testing and revision procedures (Addressable).* Implement procedures for periodic testing and revision of contingency plans.

(E) *Applications and data criticality analysis (Addressable).* Assess the relative criticality of specific applications and data in support of other contingency plan components.

In plain English, CEs and BAs must securely backup and, most importantly, be able to fully restore or recover EPHI in the event of a data loss event. Furthermore, as part of recovery and during any emergency mode operations, the same set of security requirements that apply under normal business operations must also apply during emergency mode – CEs and BAs cannot let their guard down. For example, many practices fail in this regard because their data backup solution does not encrypt the data in storage or during recovery.

Q18. Where can I find the complete language in the final Security Rule and HITECH Act?

The following link will take you directly to the final Security Rule in the Federal Register:

http://abouthipaa.com/wp-content/uploads/HIPAA_Security_Final_Rule.pdf

The following link will take you directly to the final ARRA Law, including the HITECH Act which is Title XIII and begins on page 112:

http://abouthipaa.com/wp-content/uploads/Full_ARRA_Law_incl_HITECH_Act.pdf

Q19. In practical terms, what should I do first?

Whether you are a CE or a BA, following is a short checklist of critically important actions you should take as soon as possible:

- Read the original Final Rule to make sure you understand how it applies to you.
- Read the provisions in the HITECH Act related to Privacy and Security.
- Immediately increase privacy and security as a compliance priority in your practice or business.
- Remember that the HITECH Act significantly alters the entire HIPAA enforcement environment, by increasing the penalties and eliminating in many situations enforcement discretion not to impose penalties. Charter a formal HIPAA Security team of dedicated internal staff members and/or outside experts.
- As a BA, anticipate significant amendments to their business associate agreements - consider how they will comply with the host of new privacy and security rules the now apply you.
- As a CE, make sure all business associate contracts are modified by February 17, 2010—All of the added HIPAA privacy requirements applicable to covered entities will also be applicable to business associates. As a result, all covered entities must incorporate these new requirements into their contracts with business associates by February 17, 2010 at the latest.
- Conduct a complete risk assessment—Your assessment should first and foremost identify all personal health information (PHI) records (both paper and electronic) that you work with in your company. Determine the risks to PHI security that exist in your company and spell out all the controls you have in place for safeguarding PHI.
- Conduct a comprehensive HIPAA Security Assessment to ascertain your current security state of affairs.
- Prepare a Preliminary Risk Remediation Plan outlining those actions requiring your immediate attention.
- Create a plan to mitigate your major risks—Once you've done your risk assessment and identified your top risks, you'll need to then create a written plan with the appropriate controls to address these risks. You'll also need to implement the controls from your plan into your organization's business practices.
- Update policies and procedures—Take a good look at your policies and procedures and determine what needs to be updated or enhanced for compliance with HITECH. Also, BAs of

are now subject to HHS audits and will need to be able to produce documentation (such as policies and procedures) proving that they have formal steps in place to safeguard PHI.

- Consider whether all of their uses, disclosures, and requests for protected health information are in compliance with the "minimum necessary" standard, now that a "limited data set" has been defined as compliance with that standard.
- Consider whether and how changes to the marketing, fundraising, and restriction request rules affect your operations; and how the new disclosure accounting and breach notification rules factor into your choices regarding health information systems and infrastructure.
- Document all decisions made and risks that are deemed accepted
- Ensure that all employees (including all clinicians and upper management) are trained on their roles and responsibilities with respect to the Security Rule and HITECH Act
- Maintain an ongoing program for monitoring your environment and operational processes for HIPAA Security Rule compliance.

Q20. How can Clearwater Compliance help?

Clearwater Compliance LLC (http://ClearwaterCompliance.com) assists health care companies and medical practices throughout the U.S. with all matters related to compliance with the HIPAA Privacy and Security Rule standards and the new HITECH provisions.

To assist our customers with the burdensome impact of the HIPAA Security Rule and the HITECH Act security and privacy provisions, we have developed and offer:

1. Compliance tools and software;
2. Professional services and consulting; and,
3. Remediation solutions

One of our flagship remediation solutions is the world's most reliable and secure online data backup and recovery services, offered under our Data Mountain brand.

Q21. Why Data Mountain for HIPAA-HITECH online data backup and recovery solutions?

(1) We know the HIPAA Security Law and HITECH provisions inside and out!
(2) We are experts and business continuity and disaster recovery planning!
(3) We offer the very best online data backup and recovery services in the world, bar none!
(4) We know the nuances, subtleties and ins and outs of healthcare data protection cold!
(5) We backup your entire server to ensure protection and enable the fastest possible recovery!
(6) And, our plans start as low as $134/month for up to 100GBs of data under protection.

If you feel that retaining outside expertise in this area is the right approach for you, we offer a quick and cost-effective solutions and free access to our tools, beginning with our HIPAA Security Assessment (visit http://HIPAASecurityAssessment.com).

For more information or to schedule a HIPAA-HITECH Security compliance presentation at your offices, please contact us on **(800) 704-3394**.