

## **A White Paper for Health Care Professionals**

# **Preparing for the HIPAA Security Rule**

### **Introduction**

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) will have had two full years -- until April 21, 2005 -- to comply with these standards.

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 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.

Most experts agree 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 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.

This white paper, presented in the form of Frequently Asked Questions, will help you prepare for the sweeping changes in the way you must do business under the terms of the HIPAA Security Rule.

## Frequently Asked Questions about the HIPAA Security Rule

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

The HIPAA law requires all health care Covered Entities (CEs) and their business associates to safeguard the privacy of patient health information. The HIPAA law also requires CEs and associates 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 that electronically store or transmit electronic patient health information (EPHI).

In addition, any business associate of these CEs who by agreement has access to this EPHI will be required to comply with the Security Rule as well. This comprehensive requirement will help 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 HIPPA 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.

#### **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. Is all patient health information covered by the Security Rule?**

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.

**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.

**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 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 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.

**Q10. What is a “risk analysis?”**

“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, 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 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 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 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 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 disasters

The Security Rule requires CEs 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.

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

The HIPAA Security Standards are technology-neutral. 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. In recent years, advances in information technology have resulted in the introduction of a number of security measures and devices that CEs may determine to be reasonable and appropriate means 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 will CE's have to comply with the provisions of the Security Rule?**

Most covered entities will have to be in compliance with the Security Rule by April 21, 2005. However, a large portion of the Privacy Rule requires certain Security Rule components to be in place as of April 14, 2003.

**Q15. What are the consequences for non-compliance?**

The 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 does not specify penalties but states that a separate regulation addressing enforcement will be issued at a later date.

HIPAA sets a high standard of care that CEs should strive to uphold. As stated in the final rule, Congress intended for HIPAA to "set an exceptionally high goal for the security of electronic protected health information."

But 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. Where can I find the documented final Security Rule?**

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

[http://www.DataMountain.com/files/1202/File/HIPAA\\_Security\\_Final\\_Rule.pdf](http://www.DataMountain.com/files/1202/File/HIPAA_Security_Final_Rule.pdf)

### **Q17. In practical terms, what should I do first?**

Here is the short list of critically important actions you should take as soon as possible:

- Read the Rule to make sure you understand how it applies to you.
- Charter a formal HIPAA Security team of dedicated internal staff members and/or outside experts
- 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.
- Perform a thorough Risk Analysis as a basis for preparing a Security Gap Analysis and a Final Risk Remediation Plan
- Document all decisions made and risks that are deemed accepted
- Ensure that all employees (including doctors and upper management) are trained on their roles and responsibilities with respect to the Security Rule
- Develop your Confidential HIPAA Security Compliance Manual
- Maintain an ongoing program for monitoring your environment and operational processes for HIPAA Security Rule compliance.

### **Q18. How can Data Mountain help?**

Data Mountain assists health care companies and medical practices throughout Middle Tennessee with all matters related to data protection, data backup and recovery, disaster recovery, and data security -- and in bringing our clients into compliance with HIPAA Security Rule standards.

In anticipation of the burdensome impact of the HIPAA Security Rule on our clients, we have developed a complete set of tools and techniques to streamline the Security Rule compliance process. If you feel that retaining outside expertise in this area is the right approach for you, we offer a quick and cost-effective solution beginning with our HIPAA Security Assessment (HSA).

For more information or to schedule an informative HSA presentation at your offices, please contact us on **(800) 704-3394**.

Thank you.

# Are you still betting the Practice on a tape backup system that fails 50% of the time?



In fact, 77% of the respondents to a recent *Storage Magazine* survey found their tapes failed while testing their backup. Don't bet your practice's future on those odds.

## Get a Jump On HIPAA Security Rule Compliance.

Many sections of the Final Rule cite data protection. Section 106.308(a)(7), Contingency Plan, specifically calls for data protection. *"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."* Two key REQUIRED standards call for a "Data Backup Plan" and a "Disaster Recovery Plan". LiveVault, the premier provider of remote backup solutions, can provide secure, online backup solutions that provide exact, readily retrievable copies of EPHI that will help you meet these required standards.



## Eliminate Tapes. Eliminate Risk.

With the **LiveVault Online Backup Service** you can eliminate business risk and the daily hassle of tape backup.

The LiveVault Service will continuously backup your critical server data, archive it securely at an off-site data center, and make it immediately available for recovery 24 hours a day.

Best of all, it's completely automated and online, so you never touch tape again!

## Explore Tape-Less Backup.

Learn more about our tape-less backup service by calling us today at **(800) 704-3394**. Or visit, [www.DataMountain.com](http://www.DataMountain.com)