



Search ChiroEco

Go!

[Advanced Search](#)

The Magazine

Current Issue

[Click Here to Read](#)

Subscribe Today

[Current Issue](#)[Coming Soon](#)[Past Issues](#)[Datebook](#)[Editorial Submissions](#)[Calendar](#)[Editorial Submissions](#)[Guidelines](#)

Marketplace

[Buyers' Guide 2005](#)[Card Pack Online - NEW -](#)[Products -NEW -](#)[Insurance](#)[Nutrition](#)[Orthotics](#)[Electrotherapy](#)[Supplies](#)[Rehab](#)[Diagnostics](#)[Software](#)[Tables](#)[Practice Management](#)[Patient Education & Marketing](#)[Financial Services](#)[Colleges & Continuing](#)[Education](#)[Associations](#)

>>>CLASSIFIEDS

Electronic security Get ready for more HIPAA

By Tonio Cutrera

Just when you thought you had "licked" HIPAA and its privacy rules, another HIPAA deadline lurks — the deadline for implementing the HIPAA Security Rule.

Unlike previous HIPAA regulations, the Security Rule has received relatively little publicity. Not only are many healthcare providers not yet compliant with the requirements of the rule, but many doctors are not even aware of the very existence of the legislation — not to mention the rapidly approaching April 20, 2005, deadline.

According to a January 2005 survey by Phoenix Health Systems and the Healthcare Information and Management Systems Society, only 18 percent of provider organizations are currently compliant with the HIPAA Security Rule. The study also indicates that no apparent progress has been made since the summer 2004 survey, when compliance for providers was also at 18 percent.

As with any regulation, ignorance is not bliss. So, what is the HIPAA Security Rule and what are the compliancy requirements for healthcare providers?

Congress passed the Health Insurance Portability and Accountability Act (HIPAA) of 1996 to protect the privacy and security of health information and to promote efficiency in the healthcare industry through standardized electronic transactions. The Department of Health and Human Services (HHS) has published several rules establishing provisions for compliance with HIPAA — the Privacy Rule; the Electronic Transactions and Code Sets Rule; national identifier requirements for employers, providers, and health plans; and the Security Rule.

The HIPAA Security Rule is intended to ensure the integrity, confidentiality and availability of electronic patient health information. It is important to note that the rule focuses specifically on electronic protected health information (EPHI) and is distinct from the Privacy Rule, which makes provisions for the disclosure of patient health information.

In contrast, the Security Rule requires covered entities to implement safeguards to prevent improper access to patient health information that is stored in electronic form, including information contained in e-mails or other electronic transmissions.

WHO MUST COMPLY

Applicability for the Security Rule is the same as for the Privacy Rule. Covered entities include health plans, healthcare

Wednesday



Give Your Practice an Adjustment

CHIROPRACTIC
WWW.ACOME

DouglasLa



SearchMaster

Media Kit

[Editorial Advertising Calendar](#)

[Card Packs Info](#)

[Complete Media Kit](#)

[Rates](#)

[Contact Us](#)

[Subscribe Today](#)

[Feedback](#)

[Customer Service](#)

XML

clearinghouses and any healthcare provider who transmits health information for any of the HIPAA electronic transactions such as claims, claims status, eligibility and referrals.

The rule does not apply to a practice that does not submit any information electronically.

Although nearly all healthcare providers are required to comply with the HIPAA Security Rule, the legislation provides flexibility for covered entities so that they may institute measures that are appropriate and reasonable for their practices. A small practice is not required to take the same security measures as a large practice, hospital or insurance company.

When devising a plan for compliance, the size and complexity of the covered entity, its technical infrastructure, the cost of various security measures and the likelihood of security breaches and the resulting level of potential harm are all factors to be considered.

SPECIFICATIONS

While it is true that the Security Rule is scalable in the approach taken by different covered entities, that does not mean that some portions of the rule are optional. Each specification is identified either as "required" or as "addressable." If an implementation specification is listed as "required," then action must be taken to implement it.

If it is addressable, then the covered entity is not *necessarily* required to implement the specification. But if it does not, it must either implement an equivalent alternative security measure or determine that the specification is not reasonable and appropriate for the practice.

According to HHS, if a covered entity determines that a specification of the Security Rule does not apply to the practice and that the standard can be met without implementing the addressable implementation specification or an equivalent alternative, it must document the decision and the rationale behind it.

Some considerations could include:

- An evaluation of the risk of unauthorized access and disclosure of EPHI,
- Security measures already in place to protect the health information and
- Cost estimates for implementing the specifications and the size and complexity of the covered entity.

PARTS OF THE SECURITY RULE

The Security Rule is comprised of safeguards in three categories — administrative safeguards, physical safeguards and technical safeguards. Each of the three categories consists of a number of standards and the required or addressable implementation specifications for meeting the standards.

- **Administrative safeguards.** The administrative safeguards are those that pertain to administrative functions within a



practice that must be undertaken to implement the Security Rule. Some of the standards in this section have to do with the assignment of security responsibilities and the security awareness and training of the staff. Other administrative safeguards include policies and procedures related to maintaining the security of EPHI.

- **Physical safeguards.** The physical safeguards address the measures that are to be undertaken to control physical access to EPHI and other standards that relate to the use and physical security of computer hardware, software and removable media.

The standards in this section are provided to ensure that only authorized individuals have physical access to patient health information and to protect against security threats, environmental hazards and unauthorized intrusion.

- **Technical safeguards.** The technical safeguards relate to the technical measures that must be implemented to protect data and access to data. These are software and hardware mechanisms, processes and procedures for electronic information systems that ensure that only appropriate individuals obtain electronic confidential information.

The standards include unique user identification and authentication, audit controls to monitor activity, integrity tools to protect EPHI from improper alteration or destruction and transmission security to guard against unauthorized access to EPHI that is transmitted over an electronic communications network.

Because technology advances rapidly, the rule does not dictate the use of specific technologies in the Security Rule, so that covered entities are not bound by specific technologies that may become obsolete. Instead, the security standards were designed to be "technology-neutral" to allow covered entities to adapt and change with the emergence of new and improved technologies in the healthcare industry.

STEPS TO COMPLIANCE

If you fall under the category of a "covered entity," here are steps to guide you into compliance of the Security Rule:

- 1. Assign a security officer.** A first step toward meeting the April 20, 2005, deadline for compliance is to assign security responsibility. The Security Rule requires that each covered entity designate one individual as the "security officer." That person will be responsible for coordinating policies, procedures and actions for attaining compliance. Also identify other staff members to assist with security activities.

- 2. Perform a risk analysis.** Next, study how the practice collects, uses and stores EPHI. Perform a risk analysis to determine what vulnerabilities may exist and what security "gaps" need to be addressed so that risk can be reduced to an acceptable level. Review each standard and implementation specification of the Security Rule to determine if you need to take action to come into compliance with the rule.

- 3. Develop and document policies and procedures.** As you write policies and procedures, keep in mind that the rule is

intended to be flexible and scalable to meet the needs of practices of all sizes. But remember that all implementation specifications must be considered and documented, even if you decide not to implement particular addressable specifications.

4. Implement a security training program. It is important for your workforce to understand the security policies for protecting electronic protected health information and to develop security awareness.

Implementing new policies and procedures for yet another HIPAA regulation seems like a daunting task, given the burdens of operating a busy practice. But, with the April 20 deadline only weeks away, a high priority must be given to this task to avoid getting caught in a last-minute scramble to become compliant.

For additional information and resources or to read the Security Rule online, visit the CMS at:
www.cms.hhs.gov/hipaa/hipaa2.

Tonio Cutrera holds an MBA (specialty in e-business) and is the marketing director and sales manager for E-Z BIS, Inc., a developer of practice management software for the healthcare industry. He can be reached by phone at 800-445-7816 or by e-mail at tcutrera@ezbis.com.

© 2005 Chiropractic Economics - All Rights Reserved
5150 Palm Valley Road, Suite 103 | Ponte Vedra Beach, FL 32082
Tel: (904) 285-6020 | Fax: (904) 285-9944