

Expect Increased Focus on HIPAA Security 2008

TYNAN OLECHNY, MBA, MPH

While initial compliance with the Health Insurance Portability and Accountability Act (HIPAA) "Security Standards for the Protection of Electronic Protected Health Information" (commonly known as the "Security Rule") was required by April 20, 2005, for defined "covered entities," including audiology practices, increased focus on compliance with these standards is expected to take center stage in 2008. In the wake of the first governmental audit conducted since the Security Rule went into effect (conducted at Piedmont Hospital in Atlanta, Georgia, in March 2007 by the Department of Health and Human Services [HHS]), health-care providers governed by HIPAA are taking renewed steps to ensure required standards are in place.

Renewed attention to compliance is also being fueled by the Office of Inspector General's (OIG's) stated focus in the FY2008 *OIG Work Plan*: to "review CMS' oversight, implementation, and enforcement of the regulations implementing security standards" and to "determine whether CMS has implemented controls to reasonably ensure that the HIPAA Security Rule achieves its intended results" (p. 56).

It is therefore expected that the upcoming year will result in the addition of more providers to the list of those who have already been investigated by CMS. According to the October 31, 2007, *CMS Enforcement Statistics Report*, there have been 370 total security cases investigated by CMS. One hundred forty of these remain "open" with outstanding issues while 230 are "closed" requiring no further action. CMS further reported that the top five most common security complaints in descending order include information access management, security awareness and training, access control, workstation use, and device and media controls. Consequently, it is critical that practices continuously evaluate and reevaluate their approach to compliance.

HIPAA SECURITY RULE BACKGROUND

On February 20, 2003, HHS published the final Security Rule. Prior to this, there had been no national or consistent industry standard governing the security of an individual's health information. The Security Rule focuses on requirements for

covered entities (including audiology practices) to protect and safeguard the confidentiality of protected health information (PHI) *created, maintained, and transmitted in electronic form* (e.g., computer discs, including floppy, compact and DVD; magnetic tape; computer hard drives; or information transmitted via the Internet). The purpose of the Security Rule is to adopt

national standards for safeguards to protect the confidentiality, integrity, and availability of electronic protected health information (EPHI). Among other things, the practice's computer network (and other locations where EPHI is stored including personal and handheld computers, document imaging and storage systems, and digital and video cameras) and access to the network, and the method by which the practice stores and handles such data come under close scrutiny by the Security Rule.

While the Security Rule requires covered entities to implement basic safeguards to protect EPHI from unauthorized access, alteration, deletion, and transmission, it is

broadly written. Accordingly, the detail and means of actual application among parties will vary, though all must meet the standards set forth in the Rule. Unlike the Privacy Rule, which was implemented in April 2003, the Security Rule is much more flexible and gives practices much more leeway in how to comply with the Rule. It was written to be scalable among covered entities of various forms, sizes, and technological sophistication. Unfortunately, despite the potentially considerable investment, practices may not use cost of implementation as an excuse not to meet the requirements. However, the Security Rule does allow for implementation in any order that best suits the individual practice and is "technology neutral," meaning it neither refers nor advocates specific technology with respect to which information system, hardware and software an organization uses.

Security Rule Components

The Security Rule is comprised of three primary security safeguards: administrative safeguards, physical safeguards, and technical safeguards. These safeguards are intended to support the protection of the electronic information covered by the Privacy Rule. Within each of these three safeguards,

WHAT IS A "COVERED ENTITY"?

Under HIPAA, this means health plans, health-care clearinghouses and any health-care provider (physicians, hospitals, nursing homes, etc.) who transmits any health information in electronic form in connection with a HIPAA transaction.

Tynan Olechny, MBA, MPH, Gates, Moore and Company

TABLE 1

Safeguard	Standard
Administrative Safeguards	Relates primarily to policies, procedures and organizational practices dealing with the behavioral side of security. Components include: <ul style="list-style-type: none"> • Security Official Designation and Assignment of Responsibilities • Security Management • Workforce Security • Information Access Management
Physical Safeguards	Relates to policies and procedures ensuring the security of the physical practice to authorized access. Components include: <ul style="list-style-type: none"> • Facility Access Controls • Workstation Use and Security • Device and Medical Controls
Technical Safeguards	Relates to policies and procedures that must be implemented in order to protect the integrity, confidentiality and availability of EPHI. Components include: <ul style="list-style-type: none"> • Access Control • Audit Controls • Data Integrity and Authentication • Transmission Security

there are specific security standards that must be satisfied by the practice, and within each standard there are a number of “implementation specifications” describing how each standard should be addressed. Table 1 summarizes the various safeguards and standards that must be considered.

While compliance with each of the elements of the Rule is required, for certain standards the Rule requires a particular means of compliance—referred to as the “necessary” implementation specifications. For other standards, the Rule requires that the practice address whether the implementation specifications are applicable and reasonable before the practice is required to implement the specifications set forth in the Rule or take other specific action—referred to as the “addressable” implementation specifications.

SECURITY RULE IMPLEMENTATION

To best understand how to address the standards and appropriate specifications, the first required step toward Security Rule compliance is to perform a risk analysis to assess current security measures and identify any potential risks and vulnerabilities to the confidentiality, integrity and availability of EPHI.

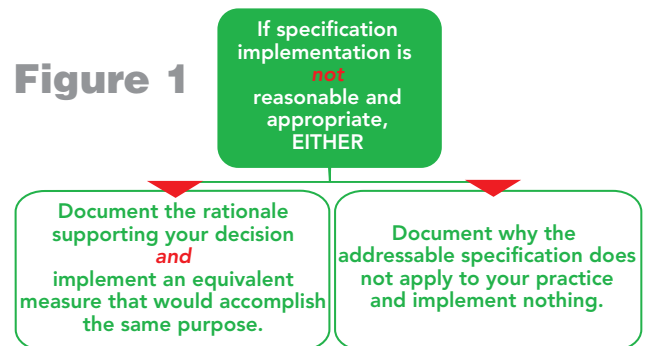
In order to comply with the “addressable” specifications, part of the risk analysis conducted by the practice will include determination as to whether the specification is reasonable for its particular situation. Key considerations to determining reasonableness include the following:

- *Size, complexity and capabilities of the practice.* For example, if you do not utilize e-mail, then it would be considered unreasonable to purchase encryption software.
- *Necessary hardware and software security capabilities.* If your current infrastructure lacks security measures, then it is reasonable to consider purchasing equipment and software to satisfy this need.
- *Cost of implementation.* Note that while you cannot use cost alone as a means to determining implementation, it may be a strong consideration in terms of identifying the solution. For example, rather than purchasing the most expensive, top of the line security product, you may opt to purchase a less expensive solution.
- *Probability of a potential risk to EPHI exposure.* Regardless of whether it actually occurs, practices should plan for potential theft. Also, while not all practices will have the same threat level regarding the potential for natural disasters, each practice needs to determine its vulnerabilities and take the necessary steps should an

event occur. A practice located in a hurricane-prone part of the country, for instance, should be sure its compliance with the Security Rule is appropriate for that situation.

If your practice determines, for whatever reason, that compliance with a specification is not reasonable and appropriate, there are still documentation steps that must be taken to illustrate thoughtful consideration of the Security Rule’s goals (see Figure 1).

Completion of the risk analysis and identification of which



addressable standards to execute provides the basis for developing an implementation plan to ensure compliance with the Security Rule. While not all-inclusive, the following provides a sample list of activities, both required and addressable, that should be reviewed and incorporated as

part of implementation and compliance with the Security Rule:

- Appoint a Security Official and delineate job responsibilities
- Implement policies and procedures regarding staff access to EPHI
- Implement a security awareness and training program
- Develop procedures for detecting and reporting malicious software, monitoring log-on attempts and reporting discrepancies, and creating, changing and safeguarding passwords
- Create policies and procedures to address security incidents
- Establish a contingency plan for responding to emergencies or other events that could compromise EPHI (e.g., fire, vandalism, natural disaster)
- Implement policies and procedures to limit physical access to electronic information systems, specify workstation use and security, and determine receipt and removal of hardware and electronic media that contain EPHI
- Develop hardware, software and/or procedural mechanisms that record and examine activity and information systems that contain or use PHI
- Periodically review and update security measures and documentation in response to practice changes, both environmental and operational, affecting security of EPHI

Most likely, by this time, your practice has already instituted the appropriate measures necessary to obtain compliance; however, given the renewed focus and attention on the Security Rule, it is imperative that you take the opportunity to consistently review and reevaluate the mechanisms you have in place to ensure compliance. 🗣️


For additional information, contact Tynan Olechny at Gates, Moore and Company, Atlanta, GA, at tolechny@gatesmoore.com; 404-266-9876.

REFERENCES

U.S. Department of Health and Human Services, Office of Inspector General. (2007) *Office of Inspector General Work Plan: Fiscal Year 2008*. http://oig.hhs.gov/publications/docs/workplan/2008/Work_Plan_FY_2008.pdf.

U.S. Department of Health and Human Services, Centers for Medicare and Medicaid Services. (2007) *CMS Enforcement Statistics Report*. <http://www.cms.hhs.gov/Enforcement/Downloads/EnforcementStatistics-October2007.pdf>.

For more information on audiology standards, guidelines, and position statements, visit
<http://www.audiology.org/publications/documents/positions/>



Visit us in Booth 1324 at Audiology NOW!



**Best Coverage
Best Service
Best Price**

Protect your clients' Hearing Aids from Loss, Damage or Failure



Discovery
Hearing Aid Warranties

800.525.7936
www.discoverywarranties.com

VOLUME 20, NUMBER 2
AUDIOLOGY TODAY