see Washington Link, page 14

OIG beginning audits of HIPAA security rule compliance

The Department of Health and Human Services (HHS) Office of Inspector General (OIG) has initiated security compliance audits of health care organizations. Compliance revolves around a broad set of security requirements that took effect in 2005, mandated as part of the Health Insurance Portability and Accountability Act (HIPAA). Although hospitals have been the early targets of these audits, medical practices could be next.

In light of a possible OIG audit, and given the potentially disastrous financial consequences of a major security breach, practices should review their security compliance, as well as internal policies and procedures. Remember: Protecting the security and availability of your patients' clinical, administrative and financial data also protects your group's ability to see patients and conduct business.

Moving your practice toward security compliance

The foundation of any security initiative is the risk assessment/analysis. A required element of the security rule, a risk assessment allows a medical practice to identify potential threats and vulnerabilities. CMS has included a matrix at the back of the HIPAA security regulation (www.cms.hhs.gov/SecurityStandard/02_Regulations.asp#TopOfPage) that offers a concise listing of all the requirements and most likely represents the OIG auditor's checklist.

OIG auditors are expected to concentrate on an organization's administrative, physical and technical safeguards — the core requirements under the security regulation. This could include policies and procedures relating to:

- Access to electronically protected health information (e-PHI);
- The risk assessment relative to e-PHI;
- Electronically transmitting e-PHI;
- Preventing, detecting, containing and correcting security violations;
- Monitoring systems;
- Remote access;
- Wireless security;
- Antivirus mechanisms;
- Firewalls; and
- Other e-PHI security requirements.

The security rule provides a number of "implementation specifications" for each provision. There are two kinds of implementation specifications: required and addressable. Required specifications mandate what a practice must do; addressable specifications allow for more flexibility and can be tailored to the requirements of your group.

Documentation is critical for each type of implementation specification. If your practice is audited, a written account of your security risk assessment, as well as your policies and procedures, will assist in a successful resolution. The risk of OIG security compliance audits, combined with an increasing level of electronic patient data, should encourage every practice to complete and fully document its HIPAA security program.

Educational materials available from CMS

Find CMS white papers at: www.cms.hhs.gov/EducationMaterials/04_SecurityMaterials.asp#TopOfPage

Find guidance to reinforce some of the ways a covered entity may protect e-PHI when it is accessed or used outside of the practice at: www.cms.hhs.gov/SecurityStandard/Downloads/SecurityGuidanceforRemoteUseFinal122806.pdf

HIPAA Security Guidance

Introduction

There have been a number of security incidents related to the use of laptops, other portable and/or mobile devices and external hardware that store, contain or are used to access Electronic Protected Health Information (EPHI) under the responsibility of a HIPAA covered entity. All covered entities are required to be in compliance with the HIPAA Security Rule[1], which includes, among its requirements, reviewing and modifying, where necessary, security policies and procedures on a regular basis. This is particularly relevant for organizations that allow remote access to EPHI through portable devices or on external systems or hardware not owned or managed by the covered entity.

This guidance document has been prepared with the main objective of reinforcing some of the ways a covered entity may protect EPHI when it is accessed or used outside of the organization's physical purview. In so doing, this document sets forth strategies that may be reasonable and appropriate for organizations that conduct some of their business activities through (1) the use of portable media/devices (such as USB flash drives) that store EPHI and (2) offsite access or transport of EPHI via laptops, personal digital assistants (PDAs), home computers or other non corporate equipment.

The Centers for Medicare & Medicaid Services (CMS) has delegated authority to enforce the HIPAA Security Standards, and may rely upon this guidance document in determining whether or not the actions of a covered entity are reasonable and appropriate for safeguarding the confidentiality, integrity and availability of EPHI, and it may be given deference in any administrative hearing pursuant to 45 C.F.R. § 160.508(c)(1), the HIPAA Enforcement Rule[2].

The kinds of devices and tools about which there is growing concern because of their vulnerability, include the following examples: laptops; home-based personal computers; PDAs and Smart Phones; hotel, library or other public workstations and Wireless Access Points (WAPs); USB Flash Drives and Memory Cards; floppy disks; CDs; DVDs; backup media; Email; Smart cards; and Remote Access Devices (including security hardware).

In general, covered entities should be extremely cautious about allowing the offsite use of, or access to, EPHI. There may be situations that warrant such offsite use or access, e.g., when it is clearly determined necessary through the entity's business case(s), and then only where great rigor has been taken to ensure that policies, procedures and workforce training have been effectively deployed, and access is provided consistent with the applicable requirements of the HIPAA Privacy Rule[3]. Some examples of appropriate business cases might include:

---

[1] The HIPAA Security Rule: Health Insurance Reform: Security Standards, February 20, 2003, 68 FR 8334.
[2] The HIPAA Enforcement Rule: Administrative Simplification: Enforcement, February 16, 2006, 45 FR 8390.
[3] The HIPAA Privacy Rule: Standards for Privacy of Individually Identifiable Health Information, December 28, 2000, 65 FR 82462, as amended August 14, 2002, 67 FR 53182

- ❑ A home health nurse collecting and accessing patient data using a PDA or laptop during a home health visit;
- ❑ A physician accessing an e-prescribing application on a PDA, while out of the office, to respond to patient requests for refills;
- ❑ A health plan employee transporting backup enrollee data on a media storage device, to an offsite facility.

We recognize that there may be additional business cases that will require the offsite use of, or access to, EPHI. This guidance is not intended to provide a comprehensive list of applicable business cases nor does it attempt to identify all covered entity compliance scenarios. A covered entity must evaluate its own need for offsite use of, or access to, EPHI, and when deciding which security strategies to use, must consider those factors identified in § 164.306(b)(2):

> *"(i) The size, complexity, and capabilities of the covered entity.*
> *(ii) The covered entity's technical infrastructure, hardware, and software security capabilities.*
> *(iii) The costs of security measures.*
> *(iv) The probability and criticality of potential risks to [EPHI]."*

Specifically, with respect to remote access to or use of EPHI, covered entities should place significant emphasis and attention on their:

- ❑ Risk analysis and risk management strategies;
- ❑ Policies and procedures for safeguarding EPHI;
- ❑ Security awareness and training on the policies & procedures for safeguarding EPHI.

Risk analysis and risk management drive policies

Once the covered entity has completed the analysis of the potential risks and vulnerabilities associated with remote access to, and offsite use of, EPHI, it must develop risk management measures to reduce such risks and vulnerabilities to a reasonable and appropriate level in compliance with § 164.306(a).

We group some of the risks associated with remote access and offsite use of EPHI into three areas: *access, storage and transmission.* Risk management planning takes all three areas into account, based on the unique vulnerabilities they introduce to covered entities that rely on remote operations involving EPHI.

A covered entity's analysis of the risks associated with accessing, storing and transmitting EPHI will form the basis for the policies and procedures designed to protect this sensitive information. Each area presents a unique set of challenges and should be individually addressed. Below is a brief summary of considerations to help guide the development or enhancement of these policies:

Data access policies and procedures focus on ensuring that users only access data for which they are appropriately authorized. Remote access to EPHI should only be granted to authorized users based on their role within the organization and their need for access to EPHI.

Storage policies and procedures address the security requirements for media and devices which contain EPHI and are moved beyond the covered entity's physical control. Such media and devices include laptops, hard drives, backup media, USB flash drives and any other data storage item which could potentially be removed from the organization's facilities.

Transmission policies focus on ensuring the integrity and safety of EPHI sent over networks, and include both the direct exchange of data (for example, in trading partner relationships) and the provisioning of remote access to applications hosted by the organization (such as a provider's home access to ePrescribing systems or "web mail" in organizations where EPHI might be included in internal communications).

Policies require training

No amount of risk analysis and policy development will be effective if the workforce does not have an appropriate security workforce awareness and training program; it is important that a covered entity's workforce awareness and training program specifically address any vulnerabilities associated with remote access to EPHI. Training should provide, at minimum, clear and concise instructions for accessing, storing and transmitting EPHI. If applicable, covered entities should include in their workforce awareness and training programs, password management procedures (for changing and safeguarding passwords); remote device/media protection to reinforce policies that prohibit leaving devices/media in unattended cars or public thoroughfares; as well as training on policies prohibiting the transmission of EPHI over open networks (including email) or downloading EPHI to public or remote computers.

It is imperative to again stress that in situations involving remote use of, and access to, EPHI, covered entities must make reasonable efforts to ensure that any such use or access is authorized and limited as required by the HIPAA Security Rule at §164.308(a)(4) and the HIPAA Privacy Rule.

Addressing security incidents and non-compliance

Should a covered entity experience loss of EPHI via portable media, the entity's security incident procedures must specify the actions workforce members must take to manage harmful effects of the loss. Procedures may include securing and preserving evidence; managing the harmful effects of improper use or disclosure; and notification to affected parties. Needless to say, such incidents should be evaluated as part of the entity's ongoing risk management initiatives.

A sanction policy must be in place and effectively communicated so that workforce members understand the consequences of failing to comply with the security policies and procedures of the covered entity related to offsite use of, or access to EPHI. When addressing the development and implementation of sanction policies, a covered entity should consider at least requiring employees to sign a statement of adherence to security policies and procedures as a prerequisite to employment.

Possible Risk Management Strategies

The tables in this section list risks applicable to each category identified earlier (access, storage, transmission), paired with risk management strategies. The "Risk" column includes general problems that could occur with the use of remote devices, or work done off-site, and lists risks in order of those that may be likely to occur followed by those that may be less likely to occur but are still pertinent to the overall risk analysis. Where applicable, the "Possible Risk Management Strategies" column

suggests basic solutions first, followed by solutions that may be more complex and therefore, possibly more appropriate for organizations with advanced technical capabilities.

Covered entities that allow or require offsite use of, or access to EPHI, and are capable of implementing all of the strategies described below, are strongly urged to do so. Furthermore, since the lists are not comprehensive, entities should strive to incorporate any other appropriate strategies to ensure the protection of EPHI. In the Strategies column, we do not repeat the same strategy multiple times even though a strategy may be appropriate to address more than one of the listed risks. For example, in the category of storing EPHI, there are risks related to the loss of a laptop or risks associated with inadvertently saving a file containing sensitive information as a temporary file or cache on a foreign computer. Assuming the files on the laptop, and those launched from an email onto an offsite system are protected by passwords, the use of a strong password to protect access to the device or file would be an appropriate and expected risk management strategy. However, "use of strong passwords" may only appear once in the entire table for that section. The tables should be read so that a number of different strategies can be considered appropriate for any or all of the risks listed, and for others that may be identified by the covered entity.

Accessing EPHI

Covered entities must develop and implement policies and procedures for authorizing EPHI access in accordance with the HIPAA Security Rule at §164.308(a)(4) and the HIPAA Privacy Rule at §164.508. It is important that only those workforce members who have been trained and have proper authorization are granted access to EPHI.

Risks	Possible Risk Management Strategies
➢ Log-on/password information is lost or stolen resulting in potential unauthorized or improper access to or inappropriate viewing or modification of EPHI.	➢ Implement two-factor authentication for granting remote access to systems that contain EPHI. This process requires factors beyond general usernames and passwords to gain access to systems (e.g., requiring users to answer a security question such as "Favorite Pet's Name"); ➢ Implement a technical process for creating unique user names and performing authentication when granting remote access to a workforce member. This may be done using Remote Authentication Dial-In User Service (RADIUS) or other similar tools.
➢ Employees access EPHI when not authorized to do so while working offsite.	➢ Develop and employ proper clearance procedures and verify training of workforce members prior to granting remote access; ➢ Establish remote access roles specific to applications and business requirements. Different remote users may require different levels of access based on job function. ➢ Ensure that the issue of unauthorized access of EPHI is appropriately addressed in the required sanction policy.
➢ Home or other offsite workstations left unattended risking improper access to EPHI.	➢ Establish appropriate procedures for session termination (time-out) on inactive portable or remote devices. Covered entities can work with vendors to deliver systems or applications with appropriate defaults.
➢ Contamination of systems by a virus introduced from an	➢ Install personal firewall software on all laptops that store or access EPHI or connect to networks on which EPHI is

Risks	Possible Risk Management Strategies
infected external device used to gain remote access to systems that contain EPHI.	accessible; ➢ Install, use and regularly update virus-protection software on all portable or remote devices that access EPHI.

Storing EPHI

Covered entities must develop and implement policies and procedures to protect EPHI that is stored on remote or portable devices, or on potentially transportable media (particularly backups).

Risks	Possible Risk Management Strategies
➢ Laptop or other portable device is lost or stolen resulting in potential unauthorized/improper access to or modification of EPHI housed or accessible through the device.	➢ Identify the types of hardware and electronic media that must be tracked, such as hard drives, magnetic tapes or disks, optical disks or digital memory cards, and security equipment and develop inventory control systems; ➢ Implement process for maintaining a record of the movements of, and person(s) responsible for, or permitted to use hardware and electronic media containing EPHI; ➢ Require use of lock-down or other locking mechanisms for unattended laptops; ➢ Password protect files; ➢ Password protect all portable or remote devices that store EPHI; ➢ Require that all portable or remote devices that store EPHI employ encryption technologies of the appropriate strength; ➢ Develop processes to ensure appropriate security updates are deployed to portable devices such as Smart Phones and PDAs; ➢ Consider the use of biometrics, such as fingerprint readers, on portable devices.
➢ Use of external device to access corporate data resulting in the loss of operationally critical EPHI on the remote device.	➢ Develop processes to ensure backup of all EPHI entered into remote systems; ➢ Deploy policy to encrypt backup and archival media; ensure that policies direct the use of encryption technologies of the appropriate strength.
➢ Loss or theft of EPHI left on devices after inappropriate disposal by the organization.	➢ Establish EPHI deletion policies and media disposal procedures. At a minimum this involves complete deletion, via specialized deletion tools, of all disks and backup media prior to disposal. For systems at the end of their operational lifecycle, physical destruction may be appropriate.
➢ Data is left on an external device (accidentally or intentionally), such as in a library or hotel business center.	➢ Prohibit or prevent download of EPHI onto remote systems or devices without an operational justification; ➢ Ensure workforce is appropriately trained on policies that require users to search for and delete any files intentionally or unintentionally saved to an external device; ➢ Minimize use of browser-cached data in web based applications which manage EPHI, particularly those accessed remotely.
➢ Contamination of systems by a	➢ Install virus-protection software on all portable or remote

Risks	Possible Risk Management Strategies
virus introduced from a portable storage device.	devices that store EPHI.

Transmitting EPHI

Covered entities must establish and implement appropriate policies and procedures to secure EPHI that is being transmitted over an electronic communications network.

Risks	Possible Risk Management Strategies
➢ Data intercepted or modified during transmission.	➢ Prohibit transmission of EPHI via open networks, such as the Internet, where appropriate; ➢ Prohibit the use of offsite devices or wireless access points (e.g. hotel workstations) for non-secure access to email. ➢ Use more secure connections for email via SSL and the use of message-level standards such as S/MIME, SET, PEM, PGP etc.; ➢ Implement and mandate appropriately strong encryption solutions for transmission of EPHI (e.g. SSL, HTTPS etc.). SSL should be a minimum requirement for all Internet-facing systems which manage EPHI in any form, including corporate web-mail systems.
➢ Contamination of systems by a virus introduced from an external device used to transmit EPHI.	➢ Install virus-protection software on portable devices that can be used to transmit EPHI.

Summary

The HIPAA Security and Privacy Rules require all covered entities to protect the EPHI that they use or disclose to business associates, trading partners or other entities. New standards and technologies have significantly simplified the way in which data is transmitted throughout the healthcare industry and created tremendous opportunities for improvements in the healthcare system. However, these technologies have also created complications and increased the risk of loss and unauthorized use and disclosure of this sensitive information.

This document provides a review of some strategies that may be reasonable and appropriate under the HIPAA Security Rule, for certain covered entities to follow (based upon their individual technological capabilities and operational needs), for offsite use of, or access to, EPHI. For a more detailed review of the HIPAA Security Rule, please visit www.cms.hhs.gov and follow the link under "Regulations and Guidance" for HIPAA Educational Materials. There you will find the "Security Series of Papers" which provide an overview of the regulatory requirements of the HIPAA Security Rule (www.cms.hhs.gov/EducationMaterials/). Please note that the HIPAA Privacy Rule also requires covered entities to implement appropriate administrative, technical, and physical safeguards for protected health information (PHI) in any form, including non-electronic. These provisions are enforced by the Office for Civil Rights (OCR). For more information on the Privacy requirements

please visit www.hhs.gov/ocr/hipaa or call the HIPAA Privacy Hotline at 1-866-627-7748 (TDD: 1-800-537-7697).

To provide feedback regarding this guidance document, you may write to Michael Phillips in the Office of eHealth Standards and Services at RemoteAccessGuidance@cms.hhs.gov.