HIPAA Investigation Risks Are Increasing

Make sure you avoid the “Wall of Shame”.

BY DEBRA CASCARDO, MA

The new HIPAA Omnibus Update rules are now enforceable, and every covered entity and business associate (BA) needs to make changes to stay in compliance. The HIPAA rules for Privacy and Security of Protected Health Information have finalized requirements, significant changes to patient rights, modifications of marketing rules, and a major change to how breaches of protected health information (PHI) are determined. Although the original HIPAA legislation passed in 1996 affects many aspects of medical practices, the primary focus of the Omnibus Rule is on strengthening HIPAA’s privacy and security protections for patients’ PHI.

The Omnibus Rule is the latest step in a process that began when Congress enacted the Health Information Technology for Economic and Clinical Health (HITECH) Act in 2009. Among other provisions, the HITECH Act required the Department of Health and Human Services (HHS) to strengthen HIPAA’s privacy and security protections for health information. HHS adopted interim rules for doing so in 2010 and finalized the rules with adoption of the Omnibus Rule. By the way, the HITECH Act was the same legislation that included the billions of dollars of incentives to providers to adopt electronic health records (EHRs). The new regulations on the release of electronic records are creating new burdens that your EHR system and medical records department must deal with. Most significantly, new rights to request restrictions on disclosures may be difficult to meet.

You will have to update your HIPAA Notice of Privacy Practices to show how you support the new patient rights under HIPAA, as amended by the HIPAA Omnibus Update and the HITECH Act. There has been a significant modification to the Breach Notification Rule. The “harm standard” that was used to determine if a breach were reportable is now replaced with a risk assessment process to determine if there is a “low probability of compromise” of the information. Moreover, violations that are not promptly corrected carry mandatory minimum fines starting at $50,000, which can reach up to $1.5 million for any particular violation.

The Office for Civil Rights (OCR) is responsible for enforcing the HIPAA privacy and security rules, which it does by investigating complaints and conducting compliance audits of businesses and organizations covered by the rules. The OCR has posted case examples and resolution agreements on its Web site, including cases involving breaches of unsecured PHI affecting 500 or more individuals—OCR’s “wall of shame.”

Have You Adopted HIPAA Security and Privacy Rules at Your Practice?

Providers may be at significant risk because they never adopted HIPAA security policies to implement the HIPAA “security” rules. The HIPAA “privacy” rules are what most people think of when you mention HIPAA—they govern the general confidentiality of PHI by regulating how providers use and disclose PHI and by establishing patients’ rights concerning PHI. They require “notices of privacy practices,” “business associate agreements,” and “minimum necessary” uses and disclosures (among other things).

The privacy rules were effective on April 14, 2001, and most providers had two years to comply. Compliance included adopting numerous HIPAA privacy policies. In response, throughout the nation, pro-

Continued on page 86
More than 60 very specific security requirements, including requirements that providers conduct a documented “risk analysis,” appoint a security officer, document physical repairs and modifications to the facility (such as doors and locks), have disaster recovery plans, have automatic computer logoffs after a period of inactivity, have procedures for periodically changing user passwords, and have procedures to monitor login attempts.

Moreover, providers must have written policies that implement the numerous security requirements and must retain a copy of the policies and analysis for at least six years. For physicians in private practice, compliance will mean:

- Conducting and documenting a risk analysis, which HHS defines as “an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability” of electronic PHI in your practice;
- Reviewing the practice’s policies and procedures for when PHI is lost or stolen or otherwise improperly disclosed, and making sure your staff members are trained in them;
- Ensuring that the electronic PHI your practice holds is encrypted so that it cannot be accessed if it is lost or stolen;
- Modifying the practice’s EHR system so that you can flag information a patient does not want shared with an insurance company; and

- Having the ability to send patients their health information in an electronic format, reviewing your contracts with any vendors that have access to your practice’s PHI, and updating your practice’s notice of privacy practices.

**New Rules for Data Breaches**

The changes that are likely to have the greatest effect on medical practices are those concerning how PHI should be secured and kept private and what practices must do in case of a breach—meaning the PHI is lost, stolen, or otherwise made available to someone who should not have it.

The rule also requires the practice to notify patients whose PHI has been breached within 60 days of the discovery of the breach. For breaches affecting more than 500 patients, the HHS and local news media must also be notified within that 60-day period.

Practices must keep a log of all breaches, regardless of the number of patients involved and submit the log to the HHS annually. These changes are a big deal because the standard of what constitutes a reportable breach is much lower; and as a result, there’s now a presumption of harm to the patient by virtue of the breach by the entity that made the disclosures.

Given the new standard, the most important action practices can take to protect themselves against penalties is to encrypt patient data, both within the practice itself and when they are taken outside the practice in a laptop computer, smartphone, or other portable device. In the Omnibus Rule, a breach is defined as the loss of unsecured PHI. So loss of data that are “unreadable, unreadable, or undecipherable” is not now considered a breach.

**Determining Risk of Harm**

Whereas before the Omnibus Rule, breaches only had to be reported to HHS if they involved a “significant risk of harm,” now the presumption is that virtually any unauthorized disclosure of PHI may be a breach, unless your practice can demonstrate a low probability that the information that has been compromised will be harmful.

There are four components to determining risk:

1. The nature and extent of the data involved:
   - Just a list of patients;
   - Social Security numbers;

   **There’s now a presumption of harm to the patient by virtue of the breach.**

2. The unauthorized person to whom the PHI was disclosed (unknown if the device was lost or stolen);

3. Whether the PHI was actually acquired or viewed; and

4. The extent to which the risk has been mitigated after the fact (e.g., obtaining a nondisclosure agreement from a vendor who inadvertently received PHI).

**Risk Analysis**

Another requirement of the rule is that practices and other covered entities conduct a risk analysis. The purpose of the exercise is to discover where the practice might be vulnerable to having its patient information lost or stolen and putting in place policies and procedures to reduce those vulnerabilities. Practices should also appoint a privacy and security officer with the responsibility for making sure the practice has policies and procedures for complying with the rules and that staff members are trained in them.

Continued on page 88
HIPAA (from page 86)

Growth in Electronic Health Records Drives Changes

Driving many of the changes in the Omnibus Rule is the proliferation of EHRs and the accompanying digitization of patient information.

The original HIPAA legislation is more than 15 years old now and was enacted at a time when EHRs were hardly known and rarely used; but now everyone’s using them, and the rules were seen to be in need of strengthening. HITECH was a huge factor in pushing the adoption of health IT, so along with that, Congress saw the need for improved privacy and security practices to protect patient information now that so much of it is becoming electronic.

The argument was that if we are going to be storing and transmitting patients’ data electronically, we need to ensure to a greater extent the privacy and security of those data. Electronic health data are fundamentally different from paper data because there is more of it and it is easier to lose or alter inadvertently. The biggest vulnerability for most practices comes from mobile devices such as smartphones, laptops, and tablets that can store electronic information and be picked up and carried away. A readily available solution is encryption software that is relatively inexpensive and a very reasonable step for a practice to take.

In addition to encryption software and electronic protection such as firewalls and passwords, practices need to establish written policies and procedures describing how PHI is safeguarded and what remedial steps are to be taken if a breach occurs. Auditors will look for HIPAA security assessment reports and steps such as the appointment of an information security officer. You also have to prove that staff members have been trained in the policies and that the policies have been implemented. Sign-in sheets and a quiz placed in each employee’s file can document that HIPAA training has been completed.

Staff training can also defuse patient concern over a privacy issue by encouraging the front office staff member to treat any complaint seriously and refer the patient to the office manager or privacy officer. Patients who believe they have not had their grievance addressed are the ones most likely to lodge a complaint with the government. It’s better to deal with the issue internally, issue an apology if appropriate, and of course identify and correct the problem.

Informing Patients

HIPAA has been updated to keep pace with changes in technology, especially the use of e-mail and other forms of electronic communication, and the widespread adoption of EHRs. Inform the patient that using electronic records, e-mail, etc. is normal practice under the privacy laws. The patient doesn’t have to agree to it, he or she just has to see it, and the doctor can make a note that the patient was presented with it, and proceed as usual.

Informing patients of their privacy rights, however, does not relieve doctors of the obligation to use HIPAA-compliant methods to exchange information. This has been a significant concern, because even though they’ve been advised to the contrary, many physicians only use commercial e-mail, and that’s not a secure way to exchange patient information.

Much PHI exchange now takes place via private applications such as a cloud site or virtual private network. I recommend that doctors get patient consent to having his or her information sent over a secure third-party site to share with other caregivers participating in the patient’s treatment. The transparency is helpful.

Another consideration is how much of the patient’s medical history the receiving provider should get. The HIPAA Privacy Rule says providers must make “reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.”

The law allows providers some discretion in deciding what constitutes the “minimum necessary.” The sending provider should at least ask, “Do I need to send the patient’s entire medical history? Or is there a portion I can send that will be sufficient for this purpose?”

Business Associate Agreements

When the HIPAA Omnibus Rule went into effect in March 2013, one of the most significant changes to the HIPAA privacy and security rules involved agreements, and the rules that govern the relationship that practices have with BAs are considered covered entities (CEs), meaning they are responsible for securing and guarding PHI in the same way that practices are, and are subject to the same penalties for violations.

Review contracts with vendors that have PHI access to ensure they have all the elements HIPAA requires. Vendors that service multiple phy-
HIPAA (from page 88)

Physician practices may have standard agreements that they ask their customers to sign. An attorney should review any agreement to ensure HIPAA compliance before signing it or have your own attorney prepare an agreement for the vendor to sign. Failure to properly follow these new rules governing agreements with BAs can lead to substantial penalties that have the potential to ruin a medical practice’s reputation and cripple it financially.

The Definition of “Business Associate” Has Changed

Under the revised rules, a BA now includes any vendor that creates, receives, maintains, or transmits PHI on behalf of a covered entity (CE), even those that do not access PHI. BAs can now include organizations involved in patient safety activities, health information organizations, and PHI data storage companies.

With this expanded definition, practices should review all existing contracts to determine if they should be replaced with BA agreements. Practices should also review existing BA agreements to ensure they DO NOT include a clause that removes them and their subcontractors from liability under HIPAA because BAs are now liable under the new rules.

The Definition of “Business Associate” Has Expanded to Include Subcontractors

Subcontractors are now considered BAs of a practice if they have access to the practice’s PHI. A practice should require its BAs to ensure that any subcontractors they may engage on its behalf will have access to the practice’s PHI and agree to the same restrictions, conditions, and requirements that apply to the BA with respect to such information. Practices would be wise to request information on these subcontractors and research them as if the practice were contracting directly with the subcontractors.

Practices should also include in their BA agreements a stipulation that requires BAs to receive approval from the practice before engaging any new subcontractors that will have access to PHI.

Practices Must Take Steps to Confirm That Their Business Associates Follow HIPAA

If a practice delegates duties to a BA, the practice now has a responsibility to confirm—to the best of its ability—that the BA is handling those duties in conformity with HIPAA rules. Practices should request and review copies of a BA’s risk assessment and the policies and procedures developed to ensure that the BA maintains HIPAA compliance. This should include the policy and procedures that states the practice will be notified if a breach occurs.

Practices should request information about a BA’s HIPAA training program. Practices should also request a copy of a BA’s cybersecurity insurance, which is designed to mitigate losses from a variety of cyber incidents, including data breaches.

While it is critical to take these steps to confirm that a BA’s services are HIPAA-compliant, it is perhaps even more important for practices to perform due diligence on the companies they are considering as partners.

Under the revised rules, a BA can now be held directly liable and subject to civil and criminal penalties for committing HIPAA violations. Individuals or companies considered BAs should be taking a number of steps to become compliant with the HIPAA Omnibus Rule. These steps include:

- Conducting a risk assessment of the methods used to protect PHI;
- Developing and/or revising policies;
- Rescinding contracts with BAs that do not fully comply with HIPAA.

Resources and Additional Information

Following are links to HIPAA resources and additional information that doctors and practice managers can use to ensure they are in compliance with HIPAA rules:

- The complete text of the HIPAA Omnibus Rule is available at www.gpo.gov.
- The Office for Civil Rights (OCR) sample provisions for a HIPAA-compliant Business Associate agreement can be viewed at www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html.
- The OCR’s guide to conducting a risk analysis is available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/riskassessment.pdf.
- The definition of what is considered a “covered entity” under HIPAA can be found at www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html.
- The OCR’s list of breaches affecting 500 or more individuals can be viewed at www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidance.html.
- A detailed description of the OCR’s HIPAA enforcement policy, along with enforcement-related data, enforcement highlights, and case examples and resolution agreements, can be found at www.hhs.gov/ocr/privacy/hipaa/enforcement/index.html.
HIPAA (from page 89)

• Business interruption in the event your practice is required to cease operations;
• Breach remediation such as notifying patients and/or the media;
• Fines or other monetary penalties; and
• Legal expenses.

Conclusion

Your staff is your frontline defense and must be kept informed on all current compliance issues. To avoid problems, train every staff member and document the training with sign-in sheets and quizzes. Keep the results in your office with the mandatory logs in case of an audit. Keep your compliance plan updated and available for all to use as a resource.

Debra Cascardo is Principal of The Cascardo Consulting Group, and a Fellow of the New York Academy of Medicine; phone: 914-358-9553; fax: 914-358-9554; e-mail: dcascardo@aol.com.

Debra Cascardo is Principal of The Cascardo Consulting Group, and a Fellow of the New York Academy of Medicine; phone: 914-358-9553; fax: 914-358-9554; e-mail: dcascardo@aol.com.