Medical Economics®
SMARTER BUSINESS. BETTER PATIENT CARE.

Published on *Medical Economics* (http://medicaleconomics.modernmedicine.com)

New HIPAA rules: Make sure you are in compliance because your liability has increased

Jeffrey Bendix, MA
Publish Date: MAY 10,2013

Healthcare providers have until September 23 to put into place internal policies and procedures needed to comply with sweeping changes coming to the Health Insurance Portability and Accountability Act (HIPAA).

In January, the U.S. Department of Health and Human Services (HHS) released a set of rules, known collectively as the omnibus rule, designed to supplement and modify the privacy, security, breach notification, and enforcement rules governing patient health information in HIPAA. HHS has made it clear that the September 23 compliance deadline is final. Penalties can range from $100 to $1.5 million depending on the violation.

For primary care and other 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 protected health information (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 (see "Encrypting your patients' health information");
- modifying the practice's electronic health record (EHR) system so that you can flag information a patient does not want shared with an insurance company;
- 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.

Other provisions

Other provisions of the omnibus rule include restrictions on selling PHI or using it for marketing and fundraising purposes without obtaining the patient's permission and loosening some of the restrictions on sharing PHI with family members or other caregivers of deceased patients. Disclosure is only permitted, however, to the extent that the PHI is relevant to the role the family member or caregiver played in the decedent's treatment. Moreover, release is not permitted in cases in which the individual expressly stated before death that he or she did not want the PHI released.

The omnibus rule also permits doctors in states with compulsory vaccination laws to disclose a child's immunization records to schools without obtaining formal authorization from parents. Physicians now can do so with only a verbal agreement, provided they document that they obtained the permission. Lastly, the rule prohibits health plans from using or disclosing genetic information for the purpose of insurance underwriting.

The rule also sets and describes the four categories of penalties for violating the rules and the dollar amounts for each.

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 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.

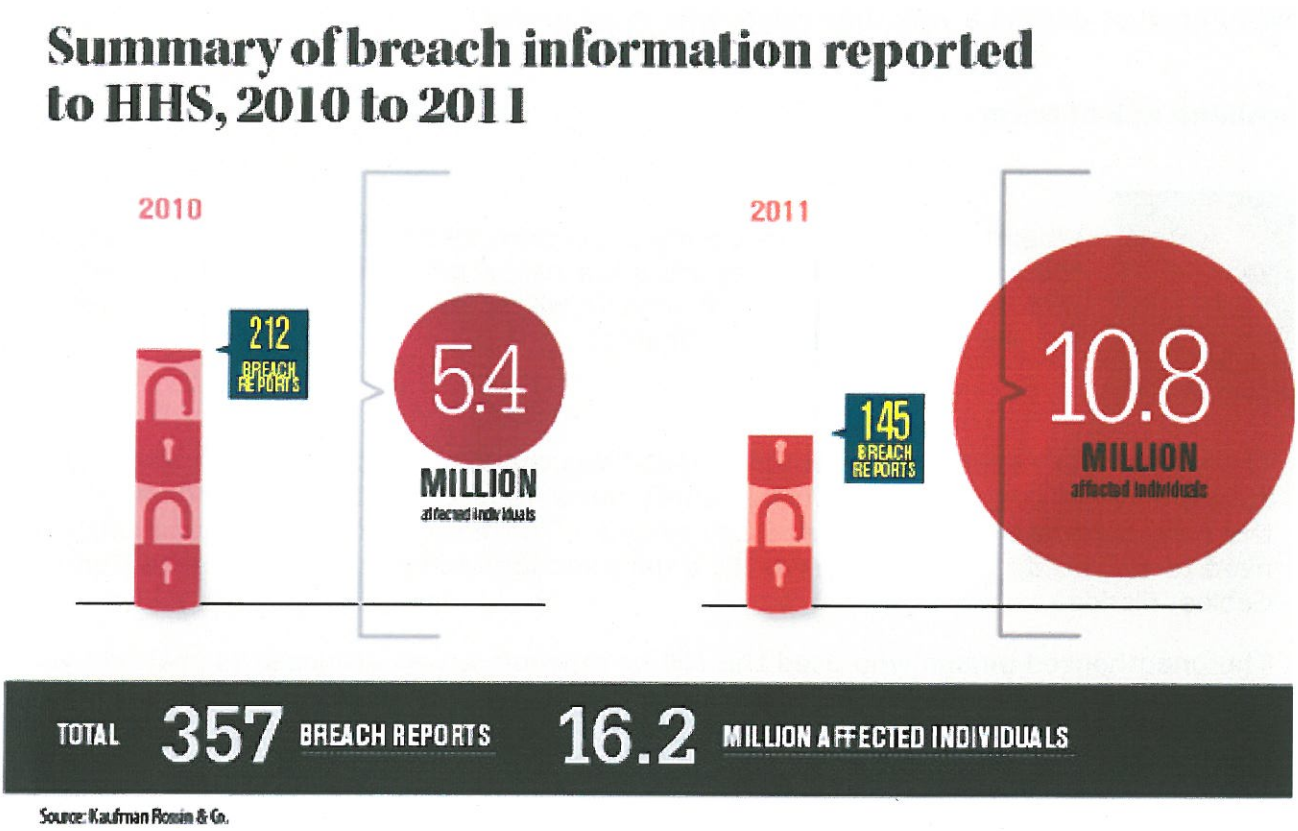
Growth in EHRs drive changes

Driving many of the changes in the omnibus rule is the proliferation of EHRs and the accompanying digitization of patient information, says Jeffrey J. Cain, MD, FAAFP, president of the American Academy of Family Physicians (AAFP).

"The [original] HIPAA legislation is 15 years old now and was enacted at a time when EHRs were nothing more than a gleam in Microsoft's eye, but now everyone's using them, and the rules were seen to be in need of tightening up," he says.

Angela Dinh Rose, director of health information management excellence for the American Health Information Management Association, says, "HITECH was a huge factor in pushing the adoption of health information technology, 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."

According to a study of breaches reported on the HHS Web site by Kaufman Rossin & Co., an accounting and consulting firm based in Miami, Florida, the number of individuals affected by data breaches doubled from 2010 to 2011, even though the number of entities involved in a breach declined (see "Summary of health breach information reported to HHS, 2010 to 2011," below). The largest cause of breaches was theft (53%), followed by unauthorized access (20%) and loss (14%).



New rules for data breaches

The changes 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. Why? Whereas before the omnibus rule, breaches only had to be reported if they involved a "significant risk of harm," now the presumption is that virtually any unauthorized disclosure of PHI may be a breach, unless the practice can demonstrate a low probability that the information has been compromised, explains Kenneth Rashbaum, JD, a health law attorney with Rashbaum Associates in New York, New York.

"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 breah by the entity that made the disclosures," Rashbaum says.

Given the new standard, the most important action practices can take to protect themselves against penalties, experts emphasize, 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. Why? "In the [omnibus] rule now, they're defining a breach as the loss of unsecured PHI," explains Juli A. Ochs, CPA, healthcare engagement director for the consulting and accounting firm CliftonLarsonAllen LLP. "So anything that renders the data 'unusable, unreadable, or undecipherable' is now not

considered a breach." (See "Encrypting your patient's health information" below for suggestions on how to encrypt data in a way that meets HHS requirements.)

Determining risk of harm

Whenever a breach does occur, it is presumed to be reportable to HHS unless the practice can demonstrate a low risk of probability that the PHI will be compromised, meaning that anyone will be harmed as a result. Demonstrating the risk contains four components:

- The nature and extent of the data involved. "Was the information just a list of patients? Did it include identifying data like Social Security numbers or other financial information? Were there intimate medical or psychotherapy records? Those are the types of questions that need to be asked," says Aldo Leiva, JD, a data security and privacy attorney in Coral Gables, Florida.
- The unauthorized person who used the PHI or to whom it was disclosed (something you can't know if the breach resulted from a device being lost or stolen).
- Whether the PHI was actually acquired or viewed.
- The extent to which the risk has been mitigated after the fact. An example, Leiva says, might be having a contractor to whom the PHI accidentally was sent sign a non-disclosure agreement.

In addition, the rule requires practices to notify patients whose PHI has been breached within 60 days of discovery of the breach. If the breach affects more than 500 patients, then HHS and the local news media must be notified within the same 60-day timeframe. Practices must keep a log of all breaches regardless of the number of patients affected, and they must submit the log annually to HHS.

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—through theft of a laptop computer on which data are stored, for example—and putting in place policies and procedures to reduce those vulnerabilities.

"People get overwhelmed by this, because they think it needs to be a formal process," Ochs says, "but it can be just everyone in the practice sitting down to talk about where are we vulnerable, assessing the risk of each vulnerability, deciding how to address it, and then documenting that they've gone through the process."

In addition, practices should 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. Practices can—and often do—assign the responsibilities to a current employee rather than hire someone new, Ochs says. "The main thing is just that it's assigned," she adds.

Violators of the privacy and security rules will be fined in amounts ranging from $100 to $50,000 per violation (see "HIPAA rule violation categories and penalty amounts"). The maximum a practice or other covered entity can be fined in a year is $1.5 million.

HIPAA rule violation categories and penalty amounts

The Health Insurance Portability and Accountability Act omnibus rule establishes four "tiers" of violations, based on what it terms "increasing levels of culpability," with a range of fines for each tier.

Violations of the same requirement or prohibition for any of the categories are limited to **$1.5 million** per calendar year.

The language of the rule states that actual dollar amounts will be based on "the nature and extent of the violation, the nature and extent of the resulting harm, and other factors...includ[ing] both the financial condition and size of the covered entity or business associate."

Category	Fine range
Did not know of breach	$100 to $50,000
Had reasonable cause to know	$1,000 to $50,000
Willful neglect, corrected	$10,000 to $50,000
Willful neglect, not corrected	$50,000

Relations with business associates

After changes to the PHI security and breach notification rules, the omnibus rule changes of greatest interest to practices are those affecting their relationships with "business associates," vendors that have access to a practice's PHI. Such vendors are now directly responsible to HHS for securing and guarding the privacy of PHI in the same way that practices are, and they are subject to the same penalties.

"Before [the omnibus rule], physicians and medical organizations might be protecting patient data the way they were supposed to, but their third-party providers were not obligated except under the terms of their contract with the providers," notes Jorge Rey, CISA, CISM, director of security and compliance for Kaufman, Rossin & Co. "Now the rules say that if you have access to patient healthcare-related information, you need to comply with all the privacy requirements." The rule also puts subcontractors to practice vendors under HHS jurisdiction.

The increased responsibility of business associates does not let doctors off the hook entirely. That's because even if the business associate loses PHI or has it stolen, the medical practice ultimately is responsible for notifying affected patients and reporting the breach to HHS.

Leiva notes that many health information technology (HIT) vendors and consultants include

boilerplate language in their contracts absolving them from liability for data loss. Consequently, he advises reviewing all contracts with HIT vendors to ensure that their wording conforms with the omnibus rules governing relations between covered entities and their business associates. (A sample business associate agreement is available from the government at http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contr...)

Greater patient control

The third part of the omnibus rule affecting doctors' practices concerns patients' rights related to their own health information.

The rules gives patients the right to:

- obtain copies of their health information in an electronic format within 30 days of requesting it, with one 30-day extension permitted, and
- instruct his or her doctor not to share information about a test or treatment for which the patient has paid out-of-pocket with his or her insurance company.

In addition, the rule requires practices to update their notice-of-privacy practices (NPPs) to reflect the changes to patients' rights included in the omnibus rule and requires sending the updated NPP to all patients and posting it prominently in the practice and on the practice's Web site.

Complying with the changes likely will be challenging for doctors due to the limitations of EHR systems. "EHRs were designed so that you could share information easily between healthcare providers and insurance providers," notes the AAFP's Cain. "Now we have this law saying that if a patient pays cash, the condition won't be revealed to insurance providers, which is problematic for the way most EHRs are built."

The design of EHRs also makes it difficult to share information with individuals who don't have EHRs, Cain notes. "That's going to be a problem and something the vendors will have to help us with," he says.

In the meantime, possible alternatives include joining a private health information exchange network or a one of the regional or statewide networks many states are establishing. Regional extension centers and state and local medical societies are good sources of information about health information exchange networks.

Doctors should ask their EHR vendors about a timetable for implementing a function that allows them to meet the requirement by the September 23 deadline, advises Lisa Gallagher, CISM, vice president of technology solutions for the Healthcare Information and Management Systems Society. If a vendor won't be ready to provide such a feature, then the practice will have to still find a way to meet the requirement, maybe through a different way of recording the patient's data until the function is available, Gallagher says.

"Sometimes regulatory requirements are misaligned," she adds. "What's happened here is the requirement for the provider to do something, and the requirement hasn't made its way down to the vendor. But the important thing for everyone to realize is that HHS has said this requirement is going into effect and you have to meet it."

Cain says that most AAFP members understand the need to provide patients with greater control over who can see their information and the need to guard confidentiality generally. Nevertheless,

"it does add another layer of administrative complexity to managing an office practice," he says.

"All the rules are well-intentioned, but they may interact in ways that aren't understood when they are developed," Cain adds. "The law of unintended consequences is challenging for office-based physicians."

What would you like to know about HIPAA? Post your questions to our Facebook page at www.facebook.com/MedicalEconomics or email us at medec@advanstar.com. We'll present answers in future articles.

Encrypting your patients' health information

Although encryption has long been part of an effective data security strategy, the Health Insurance Portability and Accountability Act omnibus rule makes it more important than ever. That's because the requirements for reporting lost or stolen data that are unusable by anyone else are far less onerous than those for unencrypted data.

Mark Eich, a partner and director of information security for the accounting and consulting firm CliftonLarsonAllen LLP in Minneapolis, Minnesota, notes that numerous encryption tools are available through a Web search. He advises thinking about protected health information (PHI) in two forms: when it is "at rest" (stored) and when it is transmitted.

Start by cataloging where your PHI is at rest in the organization. "It could be servers, work stations, mobile devices, or all of them. That will tell you where you need to apply encryption, tools," he says.

On his own laptop, Eich uses Windows Bitlocker Drive Encryption software, which encrypts everything on his main drive and requires entry of a user ID and password to access.

"If someone steals my computer, they'd need the encryption key to actually interact with the data," he says. Most encryption devices automatically encrypt data when they are transferred to another device, such as a flash drive or smartphone.

Encrypting data for transmission generally requires use of a secure file server and transfer tool so that the data can only be accessed by a password or other key provided to the recipient. Eich says his firm uses a server called LeapFile to transmit PHI. After files are uploaded to the server, he sends the client credentials and a link that applies only to those data.

Although PHI also can be transmitted via standard e-mail, it is a far less secure method, and few security experts recommend it. In fact, many health systems and others dealing with PHI have blanket policies forbidding the use of e-mail to transfer it. "That's a decision you need to make right from the start," Eich advises.

HIPAA rule violation categories and penalty amounts

The Health Insurance Portability and Accountability Act omnibus rule establishes four "tiers" of violations, based on what it terms "increasing levels of culpability," with a rage of fines for each

tier.

Violations of the same requirement or prohibition for any of the categories are limited to $1.5 million per calendar year.

The language of the rule states that actual dollar amounts will be based on "the nature and extent of the violation, the nature and extent of the resulting harm, and other factors...includ[ing] both the financial condition and size of the covered entity or business associate."

Source URL: http://medicaleconomics.modernmedicine.com/medical-economics/news/new-hipaa-rules-make-sure-you-are-compliance-because-your-liability-has-incre

Links:
[1] http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html
[2] http://www.facebook.com/MedicalEconomics
[3] mailto:medec@advanstar.com?subject=HIPAA question