This is a corrected version of the article originally published.

DANIEL F. SHAY, JD, AND ALICE G. GOSFIELD, JD

HIPAA AGAIN:
Confronting the Updated Privacy and Security Rules

New regulations will require practices to revisit and adapt their privacy policies.

A long-awaited update to the patient privacy and security rules that were established 10 years ago under HIPAA (the Health Insurance Portability and Accountability Act) is meaning significant changes for family physicians and their practices. Recently released regulations that enforce the Health Information Technology for Economic and Clinical Health (HITECH) Act expand the scope of the privacy and security provisions of HIPAA. The updated rules, which went into effect March 26, 2013, and which practices must comply with by Sept. 23, 2013, may be confusing to some, but this much is clear: The penalties for violations of the law have increased, and the government will enforce these rules, even for relatively small practices.

This article is intended to provide practical guidance to help physicians and their practices understand and comply with the law. While occasional errors in managing protected health information (PHI) are inevitable, it is increasingly evident that prevention is by far the best tactic.

Business associates: who, what, and when?

The "business associate" (BA) section of HIPAA, which dictates with whom a health care provider or other covered entity may share PHI, frequently confuses practices; namely, how do you define who is a BA? As a general rule, the fundamental question to ask yourself is "Do they perform a service *on our behalf* that has them accessing, using, and/or disclosing our patients' PHI?" If the answer is "yes," then the entity is probably your BA. While relatively straightforward in theory, this question can be harder to answer in practice, because whether an entity is your BA also depends on the nature of the activity the entity performs for you and the degree of control you exercise over it.

Not all disclosures of PHI create a BA relationship. For example, referring a patient to radiology for an imaging study does not make your practice the BA of the radiology practice. Likewise, the radiology practice would not be your BA when it sends back the results. Each entity is using the PHI for its own purposes, and the disclosure is done by one covered entity to another for treatment purposes. But if your practice was purchasing and billing for the diagnostic tests performed by the radiology group, then the radiology group would be your practice's BA.

If you have direct control over the individuals performing the service, they generally are not BAs and are instead considered "workforce." Your own staff members are not your BAs. By contrast, an independent contractor over whom you exercise no control at all (such as your attorney or your call service) is a BA if it has access to your practice's PHI.

However, things become more complicated if you exercise a sufficient degree of control over a separate corporate entity to make it an "agent" of your practice under federal common law. In such cases, you are responsible for its PHI infractions. For example, a staffing company that provides part-time physician assistants to

About the Authors

Daniel Shay is an associate at the law firm of Alice G. Gosfield & Associates in Philadelphia. Alice Gosfield is principal of Alice G. Gosfield & Associates. Author disclosures: no relevant financial affiliations disclosed.

your practice could be a BA. But your practice might also be held responsible for HIPAA violations by the physician assistants as you have a greater degree of control when they are working in your facility. In essence, the physician assistants are your agents even though you do not directly employ them.

To learn more about BA relationships and HIPAA, consult the Office of Civil Rights (OCR) for the Department of Health and Human Services (HHS) list of frequently asked questions, at http://www.hhs.gov/ocr/privacy/hipaa/faq/index.html.

The new regulations expand the number of entities that are considered BAs because of the routine access to PHI that they require. These can include electronic prescribing gateways, health information organizations, and other data-transmission services. Similarly, entities that maintain PHI on behalf of a covered entity, such as your document storage company, are now considered BAs. However, the regulations exempt entities with "random" access to PHI (such as an Internet service provider), considering them to be a "mere conduit" of information. Your electronic health record (EHR) vendor is considered a BA if it provides "personal health records" to patients on your practice's behalf. There is currently no standard definition of a personal health record, but the OCR provides some guidance at http://www.hhs.gov/ocr/privacy/hipaa/understanding/special/healthit/phrs.pdf. In many cases, you may have already established a BA agreement with such entities. If not, you must have these agreements in place.

Before passage of the HITECH Act, BAs would be liable for breach of contract only if they failed to meet an obligation of a BA agreement. However, the HITECH Act made BAs directly liable under HIPAA, meaning that a BA now has the same legal exposure as a covered entity and the government can enforce directly against the BA. The regulations also now require BAs to bind any subcontractor to a BA agreement. Moreover, those subcontractors are themselves directly liable under the law. In other words, each link in the chain is directly liable under the law, and each must bind any immediate subcontractor to a BA agreement. Make sure that you have the required agreements in place to comply with the law and that those agreements obligate your BAs to bind their subcontractors to a BA agreement. In addition, where possible avoid exercising too much control over the BA to avoid the law treating the BA as your agent.

On the bright side, you have until Sept. 23, 2014, to renegotiate your existing BA agreements to the new rules if they haven't been revised or renewed before then. The deadline will be here sooner than you think, so you should begin renegotiating your existing agreements now.

Patient access to information

HIPAA established that patients have the right to access their PHI as well as control how information in their medical record can be changed.[1] The new rules explicitly say that if you are using an EHR you must give the patient copies of electronic records if they ask for them. The regulations allow for a wide range of formats, such as PDF, HTML, MS Word, Excel, and text-based files. Unfortunately, not all EHRs make it easy to provide copies or excerpts. The law imposes this burden on all covered entities, which most family physicians are today.

Patients can also direct a physician in writing to transmit PHI to a third party. This is a long-standing policy in most practices when it comes to sharing information with other physicians or hospitals, although some practices mistakenly believe that HIPAA prevents such sharing without a written consent or authorization. Remember that no authorization or consent is required to share PHI with another party for purposes of treatment, payment, or operations of the practice. Your "Notice of Privacy Practices" should make that clear. The patient must provide prior authorization or consent in writing only if the information contains psychotherapeutic notes or is used for marketing or sale. The new standard pertains to disclosures made to

GREG CLARKE

THE PENALTIES HAVE INCREASED, AND THE GOVERNMENT WILL ENFORCE THESE RULES, EVEN FOR RELATIVELY SMALL PRACTICES.

other types of third parties, such as employers.

Under the new rules, it is entirely legitimate for a physician practice to charge the patient for the labor and materials (e.g., CDs, paper, or thumb drives) to produce the information requested. In addition, you can charge for postage if you have to send the information through the mail. Most state laws allow physicians to make a reasonable charge for copies of medical records, but you should consult your state society to determine the parameters of these laws in your state. It is also wise to train staff on dealing with these requests, especially on steps to take to ensure that the right person receives the right records.

Practices can charge reasonable fees for the materials and labor to handle patient requests for copies of their health information.

Others' access to information

For physicians who have wondered about their responsibilities to safeguard the privacy of a deceased patient's PHI, the new rules establish that the privacy rule applies for 50 years after death. As to what the family is allowed to see after the patient dies, the rules establish that the practice must respect the patient's wishes, regardless of whether the family member requesting information was paying for or was otherwise involved in the care. If the patient expressly told the practice not to show the information to a paying family member or says to show the information to someone otherwise uninvolved with the care or payment, then the practice must abide by the patient's request. If the patient dies without providing directions of this sort, the default position is that family members involved in the care or payment for the patient can see the information while uninvolved family members cannot.

If a patient doesn't specify who has access to their records after death, access is limited to family involved in care or payment.

A new rule explicitly allows a physician to disclose proof of immunization to a school if the law requires it as part of a student's admission. Written authorization is not required, but you still must obtain a verbal agreement from a parent, guardian, or the student if he or she is an adult or emancipated minor. As always, when the authorization is obtained verbally, the date, time, and name of the person to whom the authorization was provided should be entered in the record, to create an audit trail showing that you have followed the rules.

Finally, patients who choose to pay out of pocket for a health service rather than having a claim submitted to their health plan may dictate that their insurer not have access to information about the service. This is most common among patients with employer-sponsored health plans who do not want their employers to know about a medical condition. Patients may want to restrict health plans from having access to other data as well. Your practice should develop procedures to ensure that the appropriate staff are made aware of

Patients can request that care paid out of pocket not be disclosed to their insurer.

NEW HIPAA PENALTIES

Knowledge level	One-time violation, per violation	Repeated violations (of the same requirement), per year
Did not know of the violation (and could not have known)	$100 per violation, up to $50,000	$1.5 million
Violation due to reasonable cause, not willful neglect	$1,000 per violation, up to $50,000	$1.5 million
Violation due to willful neglect, later corrected	$10,000 per violation, up to $50,000	$1.5 million
Violation due to willful neglect, never corrected	$50,000	$1.5 million

such requests, that restricted information is documented appropriately and flagged, and that payments are processed appropriately.

Notice of privacy practices

Because of all the changes, your Notice of Privacy Practices will have to be updated and redistributed. In addition to the information already provided, the notice must address the following new issues:

- Patients' rights to restrict their health plans' access to certain information,
- The new right to electronic PHI.

Also, practices that send patients automated appointment reminders or information regarding treatment alternatives or health-related benefits – and receive remuneration from the patient for doing that – must get authorization from the patient and have the option to disclose that intent in their notice.

The good news about these additions is that you do not have to have established patients re-sign the notice, nor must you distribute a copy to every patient. You may simply post the notice publicly – such as in your waiting room and exam rooms – and have copies on hand to distribute to any patient who requests one. New patients must sign a statement that they have received and reviewed the notice. Remember to actually read your notice if it was copied from another source. We have seen many notices that contain errors or statements that are not applicable to the practice using them.

Security

The HIPAA security rules, which HHS implemented in 2003 after officials recognized that PHI was increasingly being stored electronically and would not remain private without implementing access restrictions, remain largely unchanged under the new regulations. Still, it's good to remember that securing PHI is about not only physically protecting it but also anticipating inappropriate disclosures and avoiding them. Physician practices must establish policies to safeguard PHI and must impose these rules on their workforce in a meaningful way. Policies must specify who has access to PHI, how much, and for what purposes.

Besides using passwords and other forms of authentication to restrict access, practices should also consider antivirus software and when and how to encrypt computer data.[2] Security policies must also address the enormous vulnerability created by storing and carrying PHI on mobile devices. The government has now identified this as a primary target of enforcement efforts. Policies must determine who, if anyone, can access PHI from offsite locations, as well as the use of email, text, and social media that might contain PHI. Since business associates are now directly subject to these rules, it is important to use your

HITECH ACT COMPLIANCE: A TO-DO LIST

- Conduct periodic risk assessments to determine the level of security risk and the steps you must take to ensure HIPAA compliance – and then follow through.
- Create a spreadsheet of all your practice's business associates, adding new ones as required under the new rules. Send an updated business associate agreement to all of them for signature. Ensure that they are returned and complete.
- Update your Notice of Privacy Practices and post it in a visible location. Have copies available to give to patients who ask for one. Make sure new patients sign that they've received a copy.
- Ensure your electronic health record (EHR) allows your staff to comply with patient requests for copies of their information, whether in paper or in most common computer formats (PDF, MS Word, Excel, etc.). Also, provide a written policy for patients to sign authorizing the transfer of electronic health information to third parties.
- Develop policies and train staff for dealing with patients who wish to pay for health services out of pocket and restrict their health plans' access to information about those services.
- Do an inventory of all the mobile devices your office and providers use. Develop and enforce policies about what protected health information (PHI) can be accessed on those devices. Install password protection on laptops and all other mobile devices in case they are lost or stolen.
- If you absolutely must send PHI via unsecured email, make sure it is encrypted. Engage a technology vendor for assistance, if necessary.
- Use a Virtual Private Network to access your EHR remotely. Make sure firewalls and effective antivirus software are in place, once again getting technology assistance if needed.
- Make sure your fax cover page has an appropriate HIPAA disclaimer, and don't fax PHI without a cover page.
- Ensure that EHR users change their passwords at least every six months and never share them with anyone.

agreements to obtain assurance that your BAs have appropriate security policies in place.

Breach notification

The Breach Notification Rule has also been revised under the new regulations, with one of the largest changes involving the definition of the term "breach." The rule requires covered entities to notify the patient and potentially the media and the HHS Secretary in the event of an unplanned release of "unsecured PHI." This includes paper, oral, and unencrypted electronic PHI.

A "breach" is now assumed whenever there is an unplanned release of unsecured patient information – unless the practice can prove patient privacy wasn't compromised.

The previous definition of "breach" required a determination of whether there was a likelihood of "harm to the individual." The revised definition now presumes a breach has occurred unless you can demonstrate a low probability that the patient's privacy or security of the PHI in question was compromised, based on a risk analysis considering four factors:

- The nature and extent of the PHI involved, including the ability to reidentify the information, and the types of identifiers included, such as names, Social Security numbers, etc.,
- The unauthorized person to whom disclosure was made or who used the PHI,
- Whether the PHI was actually acquired or viewed,
- The steps taken to reduce the risk to the privacy or security of the PHI.

For example, if you accidentally fax PHI to the wrong physician's office, and the recipient office destroys the fax upon realizing the error, a breach has not occurred.

Encrypting all patient information goes a long way toward avoiding breaches.

The easiest way to avoid the imposition of the Breach Notification Rule is to encrypt your PHI. Remember that the rule *only* applies to *unsecured* PHI; PHI that has been secured through encryption is not subject to the rule. Some physicians are already encrypting electronic PHI to ensure tighter security of the PHI they maintain and to minimize the risk of losing a mobile device that would provide access to PHI. HHS discusses examples of encryption processes that meet the rules at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html.

Penalties for HIPAA violations have gone up, and the size of practices penalized is shrinking.

Because the standard presumes a breach has occurred, and the four factors described above can be difficult to prove, it may be simpler to report the suspected breach. The act of reporting a breach does not carry a penalty (although the breach itself, as a violation of the Privacy Rule, does). Rather than spend time and effort trying to disprove the existence of the breach, it may be easier to spend the time developing a corrective action plan to avoid or at least mitigate any penalties.

Remember also that there is no private right of action under these laws. In other words, a patient can't sue you for failure to follow the HIPAA rules, but the patient can complain to the government, which can investigate and levy penalties.

Enforcement

Headlines about HIPAA enforcement usually involve large-scale violations by larger institutions. The changes to the HIPAA regulations make it clear that HHS will enforce against smaller entities as well, including BAs. Moreover, the penalties for violations have increased with respect to breaches of unsecured PHI (see the table on page 20).

Smaller practices have already been targeted, such as a five-physician cardiac surgery practice in Arizona, which paid a $100,000 fine in April 2012 for multiple HIPAA violations. The practice had done little since 2004 to comply with HIPAA rules and was alleged to have posted appointment schedules on a publicly accessible, Internet-based calendar program. With the new ability to directly enforce BAs' and subcontractors' compliance, it is clear that no entity is too small or too far down the food chain to avoid HIPAA enforcement.

The HITECH Act requires changes that all family medicine practices will have to adopt (see the to-do list on page 21). They represent a significant increase in practices' responsibilities, and the sooner you get yourself into compliance, the better. FPM

Send comments to **fpmedit@aafp.org**, or add your comments to the article at **http://www.aafp.org/fpm/2013/0500/p18.html**.

1. Standards for privacy of individually identifiable health information (final rule). *Fed Reg.* 2000;65(250):82462-82829. Codified at 45 CFR §164.522[a].

2. Kibbe DC. Ten steps to HIPAA security compliance. *Fam Pract Manag.* 2005;12(4):43-49.