New HIPAA Requirements

Joseph Eastern, MD

Practice Points

- Ignoring the recently proposed Health Insurance Portability and Accountability Act changes could be very costly. Physicians should conduct a thorough risk assessment for their practices as soon as possible.
- It is important for all office staff to be well trained in the new privacy regulations.
- Physicians should reach out to their business associates to make the required modifications to written confidentiality agreements.

Recently proposed changes to the Health Insurance Portability and Accountability Act (HIPAA)[1] have triggered widespread concern among health care professionals that largely is due to an outpouring of purple prose from the US Department of Health & Human Services (HHS), which has presented the modifications to the HIPAA rules as "the most sweeping changes. . . since they were first implemented."[2] After careful perusal of the new rules—all 136 three-column pages of them[1]—it is my humble opinion that, for most physicians, compliance will not be as challenging as some have warned such as those trying to sell compliance-related materials. However, we cannot simply ignore the new regulations, as definitions are more complex, security breaches are more liberally defined, and potential penalties are stiffer. The changes strengthen rules on privacy issues related to business associates (BAs), marketing materials, patient rights to electronic copies of their health information, and breach notification.[1] If your practice is among the many that have not yet addressed the new HIPAA requirements, now would be an excellent time to do so.

The Office for Civil Rights, which is responsible for the enforcement of HIPAA, recently fined a Massachusetts dermatology group $150,000 after it lost a USB flash drive containing unencrypted patient information.[3,4] Although this kind of judgment is not likely to be common, it is an unmistakable sign that the new regulations should be taken seriously.[5] This article will discuss the most important and relevant aspects of the regulations that require immediate attention from dermatologists.

Staff Training

Your staff will need to be trained on the new HIPAA rules. It is suggested to hold formal, classroom-type training sessions. Some consultants advise giving written tests at the conclusion of training sessions and placing the results in the employee's file as proof of training. Appoint a staff privacy officer to make sure the training is put into practice. Training materials are available from the HHS and various consulting organizations.[6]

Training your staff members on the new HIPAA privacy modifications not only enables compliance with the law but also adds an additional layer of security to your office. In my experience, trained staffers are less likely to breach patient confidentiality and are more likely to diffuse a patient's concern over a privacy issue before it is reported to an outside agency.

Risk Assessment

Conducting a comprehensive risk assessment for your practice is as important as staff training. Go through every procedure in your office that involves the processing of personal health information (PHI) and look

From private practice, Belleville, New Jersey.
The author reports no conflict of interest.
Correspondence: Joseph Eastern, MD (joseph.eastern@verizon.net).

for potential HIPAA violations, such as computer screens that are visible to prying eyes, unattended laptops or tablets, and casual texts or e-mails between staff members regarding patient care. Risk analysis guides and tool kits are available from a variety of sources.[7,8]

The biggest privacy vulnerability in most medical practices is probably the use of electronic devices carrying unencrypted PHI. Encryption software is inexpensive and readily available, and every device you own that contains PHI (or might in the future) needs to be encrypted. The Office for Civil Rights has stated that a lost or stolen device will probably not be treated as a breach as long as the PHI it contains is encrypted.[4,5]

Business Associates

Current written agreements between medical practices and their BAs are no longer valid under the new HIPAA privacy modifications and must be rewritten and resigned.[1] Business associates are still defined as nonemployees performing functions or activities on behalf of the covered entity (ie, your practice) that involve creating, receiving, maintaining, or transmitting PHI. Typical BAs include answering and billing services, independent transcriptionists, hardware and software companies, and other vendors involved in creating or maintaining your medical records. Practice management consultants, attorneys, companies that store or create microfilms of medical records, and record-shredding services are considered BAs under the HIPAA privacy modifications if they must have direct access to PHI to perform their services.[1]

Mail carriers, package deliverers, members of the cleaning staff, repair people, bank employees, and other service people who may enter your office are not considered BAs, though they might conceivably come in contact with PHI on occasion.[1] In these cases, you are required to use reasonable diligence in limiting the PHI that these individuals may encounter, but you do not need to enter into written BA agreements with them. Independent contractors who work within your practice, such as aestheticians and physical therapists, also are not considered BAs and do not need to sign a BA agreement; however, they should be provided with the same privacy training as your regular employees.[1]

The new HIPAA privacy modifications place an additional onus on medical practices for confidentiality breaches committed by their BAs.[1] It is not enough to simply have a contract for each BA; "reasonable diligence" must be used in monitoring the work of BAs. Business associates and their subcontractors are directly responsible for their own actions, but the primary responsibility rests with the medical practice. For example, if you hire a contractor to shred old medical records and they are not shredded or if a staffer loses an electronic device containing unencrypted PHI, such as the case in Massachusetts, under the new rules you must assume the worst-case scenario: that someone has the information and plans to use it in nefarious ways. Previously, you would only have to notify the affected patients and the government if there was a "significant risk of financial or reputational harm,"[7] but now any incident involving patient records is assumed to be a breach and must be reported. Failure to report breaches could subject your practice as well as the BA to fines as much as $1.5 million in egregious cases.[1]

Your rewritten BA agreements must reflect these policy changes. Many BAs will draw up their own agreements and offer them for your use; if you use them, be sure to run them by your lawyer to ensure that they protect your practice as well as the BA. Rather than scrutinizing each BA agreement, a better plan is to write a single contract tailored to your own practice and let the various BAs determine if it meets their needs. Your lawyer can help with the agreements or you can modify one of the many templates available online from the American Academy of Dermatology (AAD) Web site (http://www.aad.org) and the HHS Web site (http://www.hhs.gov).

Notice of Privacy Practices

Practitioners also will need to revise their notice of privacy practices to explain how their relationships with BAs have changed under the new rules; you also will need to explain the breach notification process and the new patient rights. You must post the revised notice and make copies available to patients in your office; however, you do not need to mail a copy to every patient.

New Patient Rights

Patients will now be able to restrict the PHI shared with third-party insurers and health plans if they pay for the services themselves. They also have the right to request copies of their electronic health records, and the physician can bill the actual costs of responding to such a request. If you have electronic health records, now might be a good time to work out a system for accommodating these requests, as the response time has been decreased from 90 to 30 days or shorter in some states.[9]

Marketing Limitations

The new HIPAA privacy modifications prohibit third party–funded marketing to patients for products and services without their prior written authorization. You do not need prior authorization to market your own

products and services, even when the communication is funded by a third party, but if there is any such funding, you will need to disclose it.

Time Is of the Essence

The new rules took effect on September 23, 2013; if you have not yet implemented the mandated changes or retrained your staff, now would be the time. The deadline to revise existing BA agreements is September 22, 2014, but the sooner you have it done the better.

The AAD has developed several resources to help dermatologists comply with the new HIPAA regulations. *A Guide to HIPAA and HITECH for Dermatology* outlines all compliance obligations and provides model policies and procedures.[10] Additionally, the AAD's new *HIPAA and Omnibus Final Rule On-Demand Webinar Series* is a 3-part series explaining the history of HIPAA and identifying the various steps dermatology practices should take to comply with the new laws.[11] These products can be purchased online through the AAD (http://www.aad.org/store).

Conclusion

The revised HIPAA regulations cannot be ignored or treated lightly. See to it that your office is in full compliance as soon as possible.

REFERENCES

1. Modifications to the HIPAA privacy, security, enforcement, and breach notification rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; other modifications to the HIPAA rules. *Fed Regist*. 2013;78(17):5566-5702. To be codified at 45 CFR §160 and §164.
2. New rule protects patient privacy, secures health information [press release]. Washington, DC: US Department of Health & Human Services; January 17, 2013. http://www.hhs.gov/news/press/2013pres/01/20130117b.html. Accessed February 12, 2014.
3. Roman J. Clinic hit with $150,000 HIPAA penalty. *Data Breach Today*. December 27, 2013. http://www.databreachtoday.com/clinic-hit-150000-hipaa-penalty-a-6321. Accessed February 12, 2014.
4. Goedert J. Feds fine dermatology practice for HIPAA security violations. *Health Data Management*. January 2, 2014. http://www.healthdatamanagement.com/news/feds-fine-dermatology-practice-for-hipaa-security-violations-47043-1.html. Accessed February 12, 2014.
5. Office for Civil Rights. HIPAA enforcement. US Department of Health & Human Services Web site. http://www.hhs.gov/ocr/privacy/hipaa/enforcement/index.html. Accessed February 12, 2014.
6. Office for Civil Rights. Training materials. US Department of Health & Human Services Web site. http://www.hhs.gov/ocr/privacy/hipaa/understanding/training. Accessed February 12, 2014.
7. Office for Civil Rights. Guidance on risk analysis requirements under the HIPAA security rule. US Department of Health & Human Services Web site. http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf. Published July 14, 2010. Accessed February 12, 2014.
8. HIPAA security rule toolkit user guide. National Institute of Standards and Technology Web site. http://scap.nist.gov/hipaa/NIST_HSR_Toolkit_User_Guide.pdf. Published October 31, 2011. Accessed February 12, 2014.
9. Michon K. Getting your medical records: information on rights, procedures, and denials. Nolo Web site. http://www.nolo.com/legal-encyclopedia/getting-medical-records-information-rights-32220.html. Accessed February 27, 2014.
10. *A Guide to HIPAA and HITECH for Dermatology*. Schaumburg, IL: American Academy of Dermatology; 2013.
11. HIPAA and Omnibus Final Rule Bundle [webinar]. American Academy of Dermatology Web site. https://www.aad.org/store/product/default.aspx?id=8658. Accessed February 6, 2014.