NEW HIPAA RULES: WHAT YOU NEED TO KNOW

"Modifications" to the HIPAA Privacy, Security, Enforcement and Breach Notification Rules, posted earlier this year, have significant implications for practices.

BY MICHAEL J. SACOPULOS, JD

Michael J. Sacopulos is the CEO of Medical Risk Institute (MRI). Medical Risk Institute is a firm formed exclusively to provide proactive counsel to the healthcare community to help providers understand where liability risks originate, and reduce or remove these risks. He also serves as Legal Analyst for Dental Products Report, Plastic Surgery Practice and is National Counsel for Medical Justice Services, Inc. He may be reached at msacopulos@medriskinstitute.com.

Although HIPAA has been around since 1996, it was recently supplemented by approximately 570 pages of new rules. I assume that you would prefer me to give you some highlights instead of reading all of those pages yourself. Here are seven new rules found in the "modifications" to the HIPAA Privacy, Security, Enforcement and Breach Notification Rules posted January 17, 2013 by the Department of Health and Human Services.

BUSINESS ASSOCIATES

Business Associates are those entities to which you provide access to your patients' protected health information (PHI). Business Associates are not employees, but are third parties. Examples include an outside billing firm, a transcription firm, a collection agency, or your data backup firm. These business entities are now fully subjected to the privacy requirements that Covered Entities have been under for some time. They will be subjected to random audits by the Office of Civil Rights. They will also be subjected to monetary penalties that can reach as high as $1.5 million. They will need to have staff trained on privacy issues, have breach notification policies, and have security policies in place. This is a comprehensive new world of compliance for your Business Associates.

So what do you need to do about this? You will need to modify your Business Associate Agreements to reflect the new rules. Any new Business Associate Agreement executed from now on will need to comply with these new rules. For those existing Business Associate Agreements that your practice has, they will need to be revised by the end of September 2013. Because the law is clear that your practice is liable for actions of your Business Associates, you may wish to add indemnity clauses into your Business Associate Agreements going forward.

MARKETING

The new rules substantially change the definition of marketing when it comes to your practice. Marketing is now defined as communication issued by your practice or one of your Business Associates regarding a treatment or service offered by a third party and that third party has compensated your practice or Business Associate for this communication. If this is the situation, your patient will need to authorize such communications with several notable exceptions. When you are marketing a third party's service to your patients and you're being compensated for that marketing, the patients will need to authorize that marketing effort before you begin.

SELLING PHI

Thinking about selling PHI to a third party that might

DO THIS NOW

Modify your Business Associate Agreements to reflect the new rules. Any new Business Associate Agreement executed from now on will need to comply with these new rules.

be able to benefit your patients? Think again. Disclosing PHI for remuneration must be authorized by your patients in advance. Additionally, that authorization must disclose that you are being compensated for providing PHI. Remember, compensation does not have to be strictly monetary; compensation can be in the form of goods and services your practice receives. This is a dangerous area; if you want to journey down this path, consult counsel.

PATIENT PRIVACY NOTICES

The new rules tell us it is time to update privacy notices provided to your patients. There are a number of modifications that need to be made into privacy notices that have been handed out to your patients in the past. Some of these modifications include the listing of uses and disclosures of PHI. Patients need to be told that they may opt out of fundraising efforts conducted by your practice or a business associate on behalf of a non-profit entity. Patients now are able to receive a copy of their PHI in an electronic form within 30 days (although you can add another 30-day extension, if need be). Note the time for this used to be 90 days. Finally, patients must be informed of their rights to prohibit disclosure of certain PHI to their health plans/third-party payers under certain circumstances, which will be discussed below.

TIME CHECK

Patients now are able to receive PHI in electronic form within 30 days (possibly 60), rather than 90.

PATIENT-DIRECTED PHI RESTRICTIONS

Patients may now restrict certain disclosures of their PHI to their health plans or insurance carrier where that patient has paid out of pocket in full for health care for the specific health care item or service. This means that if a patient wants to restrict his or her insurance company from learning about a type of medical service they have received, they may pay out of pocket and prohibit the disclosure of that information to their insurer. Note the problem this presents for your electronic health record system. While much information will be accessible to third-party payers, it is conceivable that some information will not be available to them. This shadow charting will obviously cause difficulties for all involved in the future.

BOTTOM LINE

Your practice will need to revise its Business Associate Agreement and its Breach Notification Policy. New patient privacy disclosures should replace the current ones you use.

MONETARY PENALTIES

Monetary penalties for violations of HIPAA were substantially increased under the new rules. The Office of Civil Rights will now use a scaled approach. This approach will use four categories at varying levels of culpability for the HIPAA violation. A single violation can range anywhere from a penalty of $100 to a penalty of $50,000 depending upon the perceived level of culpability. But the penalties don't end there. Violations can be added together and grow until they reach a cap of $1.5 million per calendar year. The Office of Civil Rights is deadly serious about these penalties. You are far better off to comply than to test your luck.

DEFINITION OF BREACH

The definition of a breach of PHI was substantially changed by the new rules. Previously, a breach has been defined as the inappropriate use or disclosure of PHI involving a "significant risk" of harm. The new rules define a breach as an impermissible use or disclosure of PHI unless it can be demonstrated that there is low probability that PHI has been compromised. The new rules go on to give a four-part risk assessment test to get at the term of "low probability." All this means is that the presumption has totally shifted. Before, the presumption was no breach unless significant risk of harm. Now, the presumption is a breach unless you can show a low probability of PHI being compromised.

LEGALLY SPEAKING

A breach is now defined as an impermissible use or disclosure of PHI unless there is low probability that PHI has been compromised.

This means that your practice will need to modify its Breach Notification Policy to comply with these new rules. It also may mean that more incidents will need to be reported to the Office of Civil Rights based on what appears to be an expanded definition of the word "breach."

CONCLUSION

The above seven points are some of the most significant highlights of the rules released earlier this year by the Department of Health and Human Services. Your practice will need to revise its Business Associate Agreement and its Breach Notification Policy. New patient privacy disclosures should replace the current ones you use. Unfortunately, given the significant penalties associated with non-compliance, your practice will have no option but to fully comply with these new rules. ■