Reprinted with permission from St. Louis Metropolitan Medicine.

ST. LOUIS METROPOLITAN MEDICINE

Huge Fines Await Physicians Who Are Non-Compliant With HIPAA

Having strong policies and procedures, and completing a comprehensive risk analysis, are essential in preparing for an OCR or HHS audit

By Kyle J. Haubrich and J. Thaddeus Eckenrode, Eckenrode-Maupin, Attorneys at Law

Last September, a radiation oncology practice with 13 physicians paid $750,000 to settle a claim that they were non-compliant with HIPAA regulations after a laptop was stolen from an employee's car.[1] In another incident, a hospital in Massachusetts agreed to settle HIPAA violation claims for $850,000 because a laptop was stolen from an unlocked treatment room.[2] Likewise, Affinity Health Plan was fined over $1.2 million for returning photocopiers without erasing the internal hard drives.[3]

As shocking as these figures may be, they reflect fines and settlements that are actually within the average range for HIPAA violation claims. Health-care providers need to be aware of the substantial risk they face, in these modern times of computers, social media and information technology, of being assessed fines by the government in the seven-figure range. Unfortunately, that risk—and the challenges posed to practicing physicians—is not going away. In fact, it will only become more difficult. The government anticipates increasing the number of audits they do in the coming months and years, and all physicians and medical practices must be prepared for that.[4] Unfortunately, this is not something that can be addressed with a quick coat of paint.

Background

As all health-care providers likely know, the Health Insurance Portability and Accountability Act of 1996 (HIPAA)[5] establishes certain rules and guidelines for the use, dissemination and communication of protected health information (PHI), and those laws are enforced by the U.S. Department of Health and Human Services (HHS) and Office for Civil Rights (OCR).

In the case referenced above involving the radiation oncology group (Cancer Care Group, P.C.), the OCR found that Cancer Care was in widespread non-compliance with the HIPAA Security Rule.[1] Cancer Care had not conducted an **enterprise-wide risk analysis** when the breach occurred in July 2012; nor did Cancer Care have in place a **written policy** specific to the removal of hardware and electronic media containing ePHI (Electronic Protected Health Information) into and out of its facilities, even though this was common practice within the organization. OCR Director Jocelyn Samuels stated, "Organizations must complete a comprehensive risk analysis and establish strong policies and procedures to protect patients' health information.[1]"

When Lahey Hospital and Medical Center in Massachusetts agreed to settle the alleged HIPAA violations, they not only had to agree to the $850,000 settlement noted above, but also to adopt a robust corrective action plan to address deficiencies in its HIPAA compliance program.[2] The OCR investigation concluded that the hospital had:

1. Failed to conduct a thorough risk analysis of all its ePHI;
2. Failed to physically safeguard a workstation that accessed ePHI;
3. Failed to implement and maintain policies and procedures regarding the safeguarding of ePHI maintained on workstations utilized in connection with diagnostic/laboratory equipment;
4. Lacked ... a unique user name for identifying and tracking user identity with respect to the workstation at issue in this incident;
5. Failed to implement procedures that recorded and examined activity in the workstation at issue in this incident; and
6. Made impermissible disclosure of 599 individuals' PHI.[2]

So, what does all this mean to the average physician who hangs out his own shingle, or to a group practice that doesn't have its own in-house legal team working full-time to keep the practice updated and in compliance with the various nuances of these rapidly changing laws? Unfortunately, it makes such practice

J. Thaddeus Eckenrode

Kyle J. Haubrich

J. Thaddeus Eckenrode is the managing partner of Eckenrode-Maupin, Attorneys-at-Law, a St. Louis based insurance defense firm practicing in Missouri and Illinois. He focuses on defense of complex tort litigation, most notably in the areas of medical malpractice, wrongful death, nursing homes and product liability. Kyle J. Haubrich is an attorney with Eckenrode-Maupin and is experienced in health-care law. They can be reached 314-726-6670, or jte@eckenrode-law.com or kjh@eckenrode-law.com. The firm's website is www.eckenrode-law.com.

groups or individuals prime targets for an audit by HHS, and such an audit is likely to find HIPAA violations, leading to the assessment of fines, often for significant or astronomical amounts, for not being in absolute compliance with HIPAA's Privacy, Security, and Breach Notification rules.

What Is Required to Be HIPAA-Compliant?

Most physicians simply want to practice medicine, and that's what they trained to do. Very few have the time to learn the details of what the law requires under HIPAA, and as a result, most doctors' offices fail to do the basic things required by the HIPAA law. They are not purposefully non-compliant, but they just don't grasp the significance of the law's requirements, and tend to hand off the responsibility to an office manager or staff member who is already swamped with work themselves. Most of the time the office manager or staff member who is given this responsibility is not an attorney and, when faced with a set of voluminous laws that read like Egyptian hieroglyphics, the staff struggle to fully understand the law and to comprehend the minutia and details that are actually required to keep the practice in compliance. Therefore, it begs the question, "What does HIPAA require in order to be compliant with the law?" In short, a covered entity must:

- Have **written** policies and procedures in place to protect a patient's protected health information (PHI) or his/her ePHI.
- Conduct training for all staff on these policies and procedures and the law itself, **at least twice a year** (although doing so quarterly will be viewed more favorably by HHS).
- Conduct risk analysis walkthroughs to ensure compliance with the privacy and security rules of HIPAA and to see where the office might be lacking in compliance with these rules.
- Assure that all documents, forms, letters and other information-gathering documents be in HIPAA-approved format and are easy enough for the patient to understand the manner in which their PHI is used, and to what they are agreeing, etc.[6]

1) Written Policies

HIPAA requires that all covered entities, such as hospitals, physician practices, pharmacies and clinics, must have policies and procedures in place to protect PHI from being unlawfully used or disclosed.[7] Basically, every covered entity should work with their office manager, officers and physicians to draft a **practice-specific** HIPAA manual that includes policies and procedures on everything from disaster recovery of medical files to how to respond if a patient's personal representative requests a copy of the patient's medical record. Some medical offices think they're in compliance because they have pulled a generic sample of "policies" off the Internet but never took the time to formulate and revise those policies to meet their specific practice needs. As noted below, all medical staff personnel must be trained on the practice's specific HIPAA policies and procedures, and must strictly adhere to those requirements.[7] An entity cannot comply with that requirement and effectively train its staff on their policies and procedures for HIPAA if they don't have a policy manual or if it is generic or outdated. The fines, as noted above, can be hefty if a practice simply fails to have such written policies and procedures in place.

2) Training

HIPAA **requires** that all covered entities train their staff on the specific expectations for each staff member when it comes to complying with HIPAA, and the detailed policies and procedures in the office for HIPAA compliance.[8] This is where most medical practices tend to drop the ball and expose themselves to sanctions. They either do no training at all, or the training they do is inadequate for the staff to fully understand how to comply. For example, if all an office did concerning training on HIPAA was to have its staff read a brief pamphlet every few months and then take a quiz right after reading the pamphlet, chances are good that the practice would not be in compliance with this part of the law. Because the law is so complex, training should consist of a presentation of the material the law requires the medical staff to know and understand concerning HIPAA, followed by several practice scenarios to help reinforce what was taught. Inadequate staff training may lead to a practice being heavily fined, sometimes to the tune of $50,000 or more for this deficiency alone.[8]

3) Risk Analysis

Most medical offices have never done a "walkthrough" of the office to see where they may be out of compliance with HIPAA or identify vulnerabilities that may lead to a breach of PHI. Such walkthroughs should be done at least twice a year to identify these vulnerabilities and to ensure that progress is being made to correct any identified deficiencies. Failure to conduct these risk analysis walkthroughs can also expose a practice to fines of hundreds of thousands of dollars.[1, 2] Your walkthrough should be performed as though **you** are the HHS auditor. Be very detailed and tough on yourself and your practice, and ask yourself the questions an auditor might raise: "Can I see patients' names on the computer at the front desk if I were a different patient and making an appointment?" "How easy is it for one patient to look at another patient's medical record?" Conducting your walkthrough with someone who knows what to look for as possible vulnerabilities may save headaches and expense in the future.

4) Documentation

Professional documents and forms need to be in HIPAA-compliant format as well.[9] These include all business associate contracts, documents for the release of medical records, letters denying or approving changes to medical records, and the list goes on and on. Most practices have a lot of these forms already. Unfortunately, many of these forms, especially those found on Internet websites or other such "examples" that one might obtain, can be outdated or inaccurately worded. Properly drafted and up-to-date forms and documentation help your staff comply with the policies and procedures required by HIPAA and reduce the risk of huge fines for findings of non-compliance.

What all physicians and practice managers should understand is that when the government comes in to audit your practice, they are looking for a **paper trail** showing that you have done everything required of you to comply with HIPAA. The more detailed your paper trail the less likely you are to be found out of compliance.

Will I Be Audited? If So, How Soon Could I Expect an Audit?

According to recent reports, the director of HHS has announced that more audits, which are required under the HITECH Act, will begin in early 2016.[4] They have found with the audits conducted in 2014 that almost 95 percent of all covered entities, when audited, **failed** the audits.[10] "After conducting a study to assess OCR's oversight of covered entities' compliance with the HIPAA Privacy Rule, the Office of Inspector General issued a report finding that OCR should strengthen its oversight of covered entities and made several recommendations. Specifically, OIG recommended that OCR:

1. Fully implement a **permanent** audit program;
2. Maintain complete documentation of corrective action;
3. Develop an efficient method in its case-tracking system to search for and track covered entities;
4. Develop a policy requiring OCR staff to check whether covered entities have been previously investigated; and
5. Continue to expand outreach and education efforts to covered entities."[4]

The OCR responded to this report by stating that "it is ***moving forward with a permanent audit program*** and will launch Phase 2 of that program in early 2016." This "Phase 2" will "target common areas of noncompliance ..." It will also "… test the efficacy of the combination of desk reviews of policies as well as onsite reviews." Therefore, private practice physicians, hospitals, clinics and even pharmacies, should be "reviewing their HIPAA policies and practices and developing a plan for working with OCR in onsite reviews."[4]

It is clear from this report that every covered entity should **expect** an audit of its practice within the very near future. Be prepared for OCR to review everything you and your practice have ever done toward HIPAA compliance. Unfortunately, if you do not have good documentation of all of the actions and steps you've taken—even if you have been faithful in doing all of the work necessary to comply—you may not be able to prove it, and the fines assessed could be massive.

In light of these developments, each physician and/or practice manager should ask themselves these questions:

1. Do we conduct training on HIPAA at least twice a year?
2. Do we have documentation showing that we have conducted training, who attended that training, what topics the training covered, and other required documented items?
3. Have we done our risk analysis/walkthroughs? Are they documented? Can we show that we have made progress in correcting any identified lapses in our security of PHI?
4. Do we have a HIPAA manual? Is our HIPAA manual up to date? Have our employees been trained on our policies and procedures from that manual?
5. Are all of our documents, forms, letters and other required information for patients and/or their respected personal representatives up to date and in HIPAA-compliant format?

If you can't confidently answer these questions in the affirmative, then your risk of a bad outcome from an OCR audit of your practice is substantial. The fines that may be levied against your practice will likely depend on the extent of the issues found in the audit, but even for the most nominal findings of non-compliance, fines of hundreds of thousands of dollars are possible.

Conclusion

To summarize, the Department of Health and Human Services and the Office for Civil Rights are ramping up audits of covered entities to ensure that they are complying with HIPAA's Privacy, Security and Breach Notification Rules. Every covered entity must be able to show that it has policies and procedures in place to protect a patient's protected health information (PHI) or the electronic version of the patient's information. The covered entity must show that it has conducted trainings on its policies and procedures concerning HIPAA. Training must be documented and the covered entity must have that documentation handy and ready to show an auditor. All of the covered entity's documents must be current and in HIPAA-required format.

Failure to have any of these things as required by HIPAA, or simply having them in an inadequate form, will likely result in fines being imposed by HHS and OCR following your audit.

The auditors are coming. It is no longer a question of ***whether*** you will be audited, but only a question of ***when***. The government is expediting the implementation of its auditing program. ***The time to make sure you are in compliance is now, not when the auditor shows up.***

References

1. http://www.hhs.gov/about/news/2015/09/02/750,000-dollar-hipaa-settlement-emphasizes-the-importance-of-risk-analysis-and-device-and-media-control-policies.html.
2. http://www.hhs.gov/about/news/2015/11/25/hipaa-settlement-reinforces-lessons-users-medical-devices.html.
3. http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/health-plan-photocopier-breach-case/index.html.
4. http://www.natlawreview.com/article/hipaa-phase-2-audits-to-start-early-2016-ocr-states-response-to-oig-recommendations.
5. http://thomas.loc.gov/cgi-bin/query/z?c104:H.R.3103.enr:
6. HIPAA Security Standards §164.306 & §164.308.
7. HIPAA Security Standards §164.308(a)(1)(i).
8. HIPAA Administrative Requirements §164.530 (b)(1).
9. HIPAA Administrative Requirements §164.530.
10. http://www.modernhealthcare.com/article/20130423/NEWS/304239958/audits-find-organizations-unaware-of-new-data-privacy-rules.