previous page

HIPAA Trendy:

How to Prepare Your Dental Practice for HIPAA Audits

(PART 1 OF 2)

By Christine Taxin

HIPAA laws are in the news again. HHS has begun routine audits of groups with fewer than fifteen employees or contractors. In the past, the government only audited small groups after a complaint. Now, you can be audited even if you've done nothing wrong. If the auditor finds any violations of the law, you could face high fines.

For years, many smaller offices have figured their compliance basically began and ended with those annual notifications for patients. Now, with audits looming, dental practices need to be able to prove they comply with all aspects of the law.

HIPAA Compliance: Do and Document

Under HIPAA, it's not enough to create policies and procedures for your practice. You must also document what you've done. Your documents need to cover:

- **Appropriate Officers.** Each practice needs designated privacy and security officers, if you use contractors for most of your technology. These may be the same person.
- **Recent Policies and Procedures.** Your practice should have all HIPAA–related policies and procedures in written form. These should be updated and checked against the law annually. A dusty binder from 2007 isn't compliance, it's neglect. You should also have annual update documents that detail any changes you've made or the reasons you chose not to make changes.
- **Technology Risk Analysis Studies.** Every piece of technology in the office that involves patient data should have an up-to-date risk analysis on file. This includes both software and hardware. If any piece of the system changes, you need a new risk analysis in place.
- **Data Breach Mitigation Plans.** Risk analysis tells you what can go wrong. Mitigation plans tell you what to do if something does go wrong and you have a security breach.

The more complete your documentation, the easier it will be to live through a HIPAA audit, coming out with a list of things to improve rather than a practice-destroying fine.

An Officer and a Document

Your first step in HIPAA compliance should be to appoint appropriate privacy and security officers. Your privacy officer is responsible for overseeing HIPAA-related issues in the practice. They should understand the ins and outs of the law, but also have a good knowledge of how your practice operates and how you handle records and record requests. A good privacy officer can:

- Write and distribute policies concerning patient privacy
- Educate other staff members about their duties under HIPAA
- Ensure that all patients have a current HIPAA disclosure form on file
- Answer questions from patients involving privacy concerns
- Receive and fulfill medical records requests
- Check all releases of information for HIPAA compliance

continued on page 3

continued from page 2

- Act as Security Officer in practices that use contractors for most technology

If your practice handles its software, hardware, and networking technologies in-house, you may need to designate a security officer who is not the privacy officer. Your security officer writes, distributes, and educates about the office's digital security policies. An in-house security officer also completes regular risk assessments for the technology. In offices where most technology is handled by contractors, the privacy officer can be responsible for requesting and documenting risk assessments from them.

The Basics of Good Policy Documents

Each year, your Privacy and Security Officers should review all policy documents and thoroughly document the review process.

Your policy documents should include detailed information on:

- How to back-up patient data and how to recover it
- Security for physical and electronic records, including who can access those records
- Business associate agreements showing compliance with privacy regulations
- Risk management procedures for electronic data
- Policies for dealing with data breaches, including a timeframe for patient and regulator notification
- Information on how staff and patients will be educated about these policies

Even if nothing changes from year to year, you should at least print out a new copy of these policies and note they were reviewed, found in compliance, and reauthorized for the new year. This demonstrates you're actually paying attention to your policies and the law.

Risky Business Technology

All technology carries the risk of hacking and data theft. Since you're dealing with sensitive patient information, you need to be especially aware of weaknesses in your information security. You must have a documented risk assessment for each piece of hardware and software that you use. If technology is used to transmit patient data, you must understand how to protect it and how a hacker could breach the system.

Create a separate document for each piece of technology in the office, including:

- Internal messaging software
- Databases
- Billing software
- Off-site data storage
- Modems
- Wireless systems
- Routers
- Printers
- Cell and landline phones

If a software program or piece of hardware is replaced, remove the old document and insert a risk assessment sheet for the new technology. Review and update your risk assessments each year, even if your technology doesn't change.

Offices that outsource technology installation and maintenance should have their contractors conduct these assessments and provide reports. Get accurate information on how and when your contractors conducted these assessments, as well as any weaknesses they found. No technology is 100% secure. If your risk assessment is blank, it means you didn't conduct a meaningful assessment.

Honored Mostly in the Breach

Finally, you need extensive documentation on what you plan to do when there is a data breach. Notice I said when, not if. In today's information security climate, there will be breaches. You need to have written documentation describing how you will identify breaches, notify injured parties, and remediate your data storage systems after a breach.

If you have contractors in charge of your data security, make sure they can give you a detailed description of their actions in the wake of a data breach. "We've never had a breach" does not excuse you from having a plan in place, especially with all the recent, high-profile medical record thefts.

Ensuring proper compliance with HIPAA regulations may seem like a thankless, pointless, task for a small office. However, in a world where audits are going to become more common, extra attention to detail now can save you big trouble when the auditor visits.

Part II will be published next month. Stay tuned!

Christine Taxin *is the founder and president of Links2Success, a practice management consulting company to the dental and medical fields. With over 25 years of experience as a practice management professional, she now provides private practice consulting services, delivers continuing education seminars for dental and medical professionals, and serves as an adjunct professor at the New York University (NYU) Dental School and Resident Programs for Maimonides Hospital.*

FMI: *www.links2success.biz, 914-303-6464, or ctaxin@Links2success.biz*

continued on page 4