# Six Ways to Make Your Dental Practice HIPAA Compliant

**By Amy Wood, President of ACS Technologies, LLC**

Do you think you've got everything covered with HIPAA? The growing numbers of reported data breaches say otherwise. Let's start with the real reasons why dental professionals are confused by HIPAA.

You know you need to do something about HIPAA, so you start with an inexpensive do-it-yourself solution. Seems easy enough, but most are written by lawyers and unless you went to law school, you probably have no clue what it all means. And how can you, when they ask questions such as: *"List all the locations where your PHI is located."* Most people typically answer "the server" or "my paper charts".

So, you task a staff member or office manager with being in charge of HIPAA compliance for your practice. They are just as confused, do a couple of tasks and call it good – leaving your practice with much vulnerability. A trained professional will know where the danger lurks and will ask about such things as email, cell phones, inactive paper charts storage, hard drives from decommissioned computers and much more…so what about these? To further complicate the situation we have unqualified people jumping on the HIPAA bandwagon because they hear there is money in it, further putting you at risk. *So what is a dental practice to do?*

**1. Acknowledge and Accept that it Applies to You**

HIPAA has applied to covered entities for 20 years, and there are still dentists who avoid complying. Even if a practice doesn't process electronic claims, chances are they provide other "covered transactions" such as: emailing referring doctors, transmitting x-rays using Dropbox, portable drives, or have digital data on computers, servers, or laptops. It's time for all dentists to acknowledge that they maintain a lot of private information on their patients – enough information, if breached, that could result in identity theft. Your patients trust you. Shouldn't the logical and ethical thing be to protect that information with an acceptable level of protection?

**2. Do Something About It**

Start a process and stick to it. Far too often, practices will start a program, do a couple of things to address HIPAA and then stall out. While there is some credit given for doing something, it doesn't help long-term if you don't continue improving. The same goes for HIPAA. It's an ever evolving process that requires adjustments as technology and vulnerabilities change.

**3. Get a Risk Assessment**

Have an *experienced* risk assessor come into your practice, preferably one who has gone through a data breach with their assessment. This can be scary since all of your vulnerabilities are suddenly front and center. However, identifying your risks allows you

to work a plan to close the gaps before they open the door to a breach. Self-assessment tools are another option; however, incomplete risk assessments are often listed as one of many deficiencies in a data breach settlement. Whenever possible, hire a professional to guide you through this complex process.

**4. Train Your Staff**
There are many available options for HIPAA training. Most training is not exciting to do and may take several hours; however, a reportable breach is significantly reduced when your employees know how their actions or inactions affect the overall compliance of your practice. Many state dental boards require proof of HIPAA training as part of continuing education and most providers can provide CEU's.

**5. Know Your Business Associates**
Any person or vendor that creates, receives, maintains or transmits Protected Health Information as part of their engagement with a dental practice is required to comply with HIPAA regulations just as you do. Some examples are: IT Providers, Vendor Support, Appointment Reminder Companies, Email Providers and more. Make sure you have a solid Business Associate Agreement assigning appropriate risk and financial liability if a business associate breaches your patient data. It's also good practice to require a security evaluation of each Business Associate to determine what level of risk their internal practices pose to you.

**6. Hire a "Healthcare" IT Provider**
IT providers *specializing* in healthcare have HIPAA regulations and compliance as a Business Associate. Just as you have the obligation to diagnose and treat the patient's oral health needs with maximum benefits, so is the IT provider obligated to identify any technology security deficiencies in your office and offer you the best solutions to remediate and protect your data. Many IT companies (Managed Services Provider) now offer proactive service models with an affordable monthly fee to manage your network. This will prevent many issues, including those that could cause data breaches and very expensive downtime. With the current Cybersecurity risks, it is important to work with an experienced provider who understands your risks. An amazing resource to find dental specific (HIPAA ready) IT in your area is the Dental Integrators Association.

This is by no means an exhaustive list of all the things you should do; however, it is a good overview of where to start.

*Amy Wood is President and HIPAA Compliance Officer of ACS Technologies, LLC, a firm based in Santa Rosa, CA, specializing in Data Breach Investigations, Breach Mitigation and comprehensive HIPAA Compliance and IT for dental practices.*
*Amy can be reached at: amy@acsdt.com*