HITECH Act: The Power Behind the HIPAA Punch

Discover how the HITECH Act gives power behind the punch of HIPAA compliance and learn what to do to make sure your office is compliant.

Olivia Wann, RDA, JD | Owner, Modern Practice Solutions

I've often heard dentists say that HIPAA compliance is not a big deal because there are no HIPAA police. The HITECH Act, signed into law February 17, 2009, changed that by giving HIPAA's Privacy Rule additional protections. Are you prepared for a HIPAA complaint, data breach, or perhaps a compliance audit? Whether you are a dentist or a consultant, you must seriously embrace the additional protections in the HITECH Act.[1]

I like to think of HIPAA's Privacy Rule as a fence with a gate that ensures the protection of patient's protected health information (PHI) while allowing the flow and exchange of information. The HITECH Act acts like a guard at the gate.

It introduced enforcement provisions for the HIPAA Privacy Rule, including breach notification requirements and increased fines and penalties for non-compliance. Basically, HITECH gave the power behind the HIPAA punch. Additionally, HITECH paved the way for periodic audits with the Office for Civil Rights (OCR) conducting the investigations.

Are you prepared for a HIPAA complaint, data breach, or perhaps a compliance audit? Whether you are a dentist or a consultant, you must seriously embrace the additional protections in the HITECH Act.

What is Protected Health Information?

Conduct a risk assessment of your data and then determine the level of compliance your practice has achieved versus what is necessary to implement. Keep in mind that the core of HIPAA compliance involves understanding what PHI is. According to the code, PHI is defined as individually identifiable health information transmitted or maintained by electronic media.[2]

The practical requirements regarding the meaning of "protected information" may vary state to state based on the state's statutes. For example, Tennessee's "protected information" means first name/initial, last name and social security number or driver's license/ID card number, or first name/initial, last name and account credit card/debit number with a password that would permit access to the account. However, Texas defines "sensitive personal information" as first name/initial and social security number, driver's license/ID card number, or account/credit card/debit number with a password that would permit access to the account. However, Texas also includes information that identifies an individual and relates to their physical/mental health/condition, provision of health care, or payment for provision of healthcare.[3]

Assess Your Risk of a Data Breach

As you can see, it is highly important that your dental practice assess not only the federal requirements but also your individual state's requirements, particularly when determining the breach notification requirements. You must also assess the type of information collected through the patient registration process. Keep in mind: if you collect it, you protect it. Therefore, do not collect information you do not need. For example, if a patient pays for their services in full with cash and is reluctant to provide you with a social security number, you should question why your office even needs the number.

Analyze the flow of information, from the registration process to the transaction of services and billing insurance plans. PHI may be stored on flash drives, external hard drives, computers, laptops, mobile phones, CD-ROMs, and other media devices. Conduct a thorough analysis of how data is transmitted and stored in your practice and prepare an inventory of where the data is stored. Most dental practices are at risk for a data breach with information stored electronically. Common breaches include: 1) lost, missing, or stolen laptops or other portable devices; 2) improper disposal of documents and outdated computers; 3) hacking; and 4) third-party mistakes. Prior to HITECH Act, there was no federal requirement to notify patients of a healthcare privacy breach.

In addition to the federal HIPAA requirements, most state legislatures have also enacted breach notification laws. Currently, the only states that lack data breach notification on a state level are Alabama, Kentucky, New Mexico, and South Dakota. Obviously, you need to take heed to avoid a compliance blunder. Consult with your information technician, consultant trained on HIPAA compliance, or healthcare attorney in conducting a risk analysis. If you use Dentrix PowerPay or PowerPay LE, you can conduct your own risk analysis using the PCI Manager created in partnership with Moneris and Trustwave. Browse to www.dentrix.com/pci-compliance for more information.

If a breach occurs, you must file a breach report as required by the HITECH Act's Breach Notification Rule. Blue Cross Blue Shield of Tennessee reported that 57 unencrypted computer hard drives containing the PHI of over one million individuals had been stolen from a leased facility in Tennessee. They agreed to pay $1,500,000 to settle HIPAA violations. This enforcement action is the first resulting from a breach notification. They also agreed to a corrective action plan which includes reviewing, revising, and maintaining their privacy and security policies and procedures, training employees, and performing monitor reviews to ensure compliance.[4]

Breach notification may be a costly process. As indicated earlier, the notice requirements vary state by state. For example, Tennessee requires written notice of a breach. Or, the practice can provide email and substitute notice if they demonstrate that the cost to provide notice to affected parties would exceed $250,000, the affected class of persons to be notified exceeds $500,000, or the business does not have sufficient contact information for the affected parties. Substitute notice consists of electronic mail notice if the business has the email addresses, conspicuous posting of the notice on website if a website is maintained, and notification to statewide media.[5]

Protect Your Data

Data that is transmitted or stored must be encrypted. Encryption is the process of transmitting information using an algorithm to make the data unreadable. Therefore, make sure your stored data, such as your external hard drive, is encrypted and your offsite backup is encrypted. Dentrix eBackUp encrypts your data when you back it up, so you don't have to go through two separate steps of backing up data and then encrypting it. For more information about Dentrix eBackUp, visit www.dentrix.com/ebackup.

Safeguard Your Practice from a Breach

According to the Department of Health and Human Services, more than 30,000 healthcare data breaches affecting more than 7.8 million people were reported to the Office of Civil Rights from September 23, 2009 to December 31, 2010. To protect your file server, assess the physical security of your building. Consider updates such as an alarm system and a secure file server closet. From a technical perspective, enable passwords in Dentrix and require individual log-ins and password rights that limit users' rights to their job duties. Additionally, use a commercial grade firewall that offers greater network security than a typical setup for home use. You should also ascertain whether you have adequate insurance coverage to cover cybertheft.

Business associates are third parties (such as consultants, accountants, trainers, hardware technicians, and others) who have access to your database. Obtain a business associate agreement that provides you with reasonable assurance that this individual or group will appropriately safeguard the PHI it receives or creates on your behalf. If, for example, a hardware technician removes a notebook computer from your office to repair at their location and it is stolen, who is responsible for the breach notification process? Ironing out these wrinkles when you contract third-party services will prevent much grief and stress later on.

Avoid HIPAA complaints and pass a compliance audit by having the necessary policies and procedures in place that address HIPAA's Privacy and Security Rule as well as the HITECH Act. A binder full of blank templates does not satisfy compliance requirements. Provide and document training for employees, including clinical and administrative team members. Obtain an acknowledgment of your HIPAA policies for their personnel records in addition to standard confidentiality agreements.

Your goal should be to close the gap in your HIPAA compliance program to minimize the possibility of a data breach and help your practice sail through a compliance audit. DM

Olivia Wann, RDA, JD is a healthcare attorney in Dover, Tennessee. She provides national compliance consulting with her company Modern Practice Solutions and also practices law in Tennessee. She is the author of "HIPAA Compliance and Data Management." You may contact Olivia at (931) 232-4529 or olivia@modernpracticesol.com.

---

[1] *The HITECH Act was enacted as part of the American Recovery and Reinvestment Act of 2009, Pub. L. 111-5. Codified at 42 U.S.C. § 17932*

[2] *42 U.S.C. § 160.202*

[3] *Tenn. Code § 47-18-2107 and Tex. Bus. & Com. Code §§ 521.002, 521.052, 521.053, & 521.151*

[4] *www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/bcbstagrmnt.html, accessed on August 23, 2012*

[5] *Tenn. Code § 47-18-2107*