HIPAA Compliance: What You Need to Know About the New HIPAA-HITECH Rules

Counselors who have not already done so will need to update their policies and contracts to comply with new HIPAA rules added by the Health Information Technology for Economic and Clinical Health Act (HITECH). If you think HIPAA is no big deal or don't have a clue what HITECH means, this could be a wake-up call.

On January 17, 2013, the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) issued the final omnibus HIPAA-HITECH rules (45 CFR Parts 160 and 164) with an enforcement date of September 22, 2014.

Unfortunately, pleading ignorance won't get you very far with HHS or the attorneys general of your state. The term "did not know" is actually one of three penalty categories for violating the new HIPAA-HITECH rules, along with "reasonable cause" and "willful neglect." All of them come with penalties. In the "did not know" category, a breach will cost you $100–$50,000 for each personal health information (PHI) item.

If it has been a while since you brushed up on HIPAA-HITECH, you may be surprised to find that PHI and electronic PHI (ePHI) includes any of the following pertaining to a client: first name, last name, e-mail, ZIP code (yes, ZIP code), city, county, phone number, IP address and more (18 items in all). But hey, at least there's a $1,500,000 annual cap on penalties! Bottom line, it would not be an overstatement to say these penalties would be devastating to a private practice or one's professional career. It is time to get serious about HIPAA-HITECH.

Enforcement is not just in hospitals anymore. HHS.gov cites several case examples of enforcement in mental health centers and private practices. (Those listed at the link are just examples.) The likelihood of getting caught is rising, as HHS has been training state attorneys general who, through the HITECH act, are empowered to bring civil action on behalf of their residents for HIPAA-HITECH violations. The chances of being reported are also increasing—complaints of breaches were the highest yet in 2013, and anyone can file a complaint through a convenient online form.

There are some shortcuts you can use to get up to speed. First, find out if you are a "covered entity." This really depends on the type of work you do and agencies with which you interact. If you're not a covered entity, you might find that in order to interact with agencies that are covered entities, you'll need to comply with the same laws. Then, read the overview of HIPAA-HITECH and other HHS health information privacy resources.

The summary of HIPAA for small providers explains the key elements for understanding and implementing the rules. The September 22 deadline pertained to the contracts you (should) have in place with vendors and others who have access to personal health information. It would be a good idea to take a survey of your practice and identify all of the vendors that have access to your office, computers, computer network, etc. and make sure you have a business associate agreement (BAA) signed by them on file. Make sure your BAAs include the updates required by the final omnibus rule. If you already have a BAA on file, you might only need to add an addendum with the new provisions. These include language that the contractors and vendors are to comply with the HIPAA Security Rule, provisions for the Privacy Rule and a clause stating that they are subject to direct enforcement by HHS. The OCR has created Sample Business Associate Agreement Provisions from which you can adopt language for your contracts.

On a side note, you need to read through any BAA handed to you or downloaded from the Internet. They are not all the same. Microsoft, Amazon, Google and others are now digitally signing BAAs, but in the (very) fine print, some of these contracts absolve these companies of all responsibility if very strict conditions pertaining to the movement of data and storage of ePHI are not met. A vendor could produce a BAA that leaves you with all of the responsibility for actions by the company that are out of your control. So, it is always advisable to have your healthcare attorney review any contracts.

Obtaining full HIPAA-HITECH compliance is achievable and necessary. There are specific steps you can take to protect the client's PHI, your practice and your career. The Office of Civil Rights could serve notice to enforce HIPAA-HITECH in your practice. Consider one of the following continuing education courses to ensure you'll have a better response than "I didn't know."

http://www.zurinstitute.com/hipaa.html

http://www.personcenteredtech.com/training/ce-program-offerings/heart-centered-hipaa-and-ethical-security-for-client-and-clinician-protection-level-i-ii/

https://content.crosscountryeducation.com/prodcontent/WebContent/pdf/brochure/270657.pdf

Jay Ostrowski is an NCC and the Director of Product and Business Development for the National Board for Certified Counselors (NBCC).