HIPAA and HITECH Changes

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) guidelines established, among others, the Privacy Rule, which granted federal safeguarding to Protected Health Information (PHI). HIPAA was expanded on September 23, 2013 by the Health Information Technology for Economic and Clinical Health (HITECH) Act Final Rule 2013. This act, also known as the "Omnibus Rule," is meant to address the changes in technology that have occurred since 1996, when it was signed into law. HIPAA was meant in large part to focus heavily on the *portability* part of its name.

One of the more common aspects of "portability" occurs whenever we transmit protected health information between ourselves, other practitioners, and/or business associates. Business associates are, in highly simplified terms, covered entities that are not directly involved in healthcare, but that receive and transmit PHI. These might include insurance providers, billing agencies, or billing clearinghouses. PHI has almost been supplanted by the more accurate term ePHI, where the "E" stands for "electronic." Indeed, information of any kind is now more portable than ever. This was what lead to HIPAA rules being outpaced, dated, and in need of updates to match today's standards.

The HITECH change enforcements comes exactly one month after I finished my postdoctoral fellowship and began my career as a neuropsychologist. I decided that when I got out into the working world, I was going to house my patients' data completely electronically, and go the paperless route. Not just an intake interview, or selected parts of the patient record, but the *entire record*. For neuropsychologists, this is a big thing, since the tests we administer either have test responses written on a protocol form or scores printed out on paper. Nevertheless, the gains seemed great: a paperless system would eliminate the need for physical storage and associated costs. I would also have at my disposal an easily searchable file structure of all my patients' data. So, if a patient or an attorney requested a record, I would be able to reproduce and transmit the contents with extreme efficiency. Data loss is a reasonable concern for any covered entity that deals with ePHI, especially if certain (or all) information exists only on a computer or server. One good solution is to have a backup. A better solution is to have more than one backup (e.g., two external hard disk drives (HDD), both of which are encrypted and off-site storage on a HIPAA-compliant cloud server). Both drives would be encrypted using a virtual encrypted disk, with

each being encrypted with one or more 256-bit AES ciphers. By encrypting each drive, I would be able to keep one at work and take one home. After a set period of time, say one month, the drives get rotated after synchronizing to make sure that each one had the same exact data. This solution simultaneously takes care of the problem with ePHI, which would keep me compliant with the HIPAA Privacy and Security rules.

Problems

Those were the pros. Then, I started to think about the cons. My main, overarching concern was: would my patients' data be safe if stored (and possibly transmitted) this way?
Here are some examples of how ePHI could become a victim of an ePHI breach:

- "Hackers" or "bots" that systematically patrol and attack IP addresses.
- Computer or backup hard disk drives get stolen

Also, what would happen if I didn't have the original, physical documentation when I was deposed? Would it look like I wasn't being a good custodian of my patients' data? I was concerned that the opposing side would think that I was being reckless with data, and would call into question my knowledge and understanding of ethics and the law. However, all practicing clinicians are very much in the clear as long as we adhere to the rules and regulations specified in the HIPAA & HITECH standards. To review these new standards, visit the HealthIT.gov Privacy & Security Resources page where you'll find a wealth of useful information.

Penalties for Violations

The office of Health and Human Standards (HHS) has instituted a change in the amounts of penalties for violations of the Privacy and Security Rules. Each violations can range anywhere from $100 to a maximum penalty of $1.5 million over the course of a year. Furthermore, it doesn't matter if you are large or small. The fines are not adjusted for the size of an entity, only for the seriousness of the breach. Any organization is just as likely as another to fall victim to a data breach if proper procedures are not implemented.
It's worth noting that the penalties are not limited to a financial hit, either. There is another type of penalty: public shame. According to the Breach Notification Rule, if a breach involves more than 500 records, then you are required to report it to HHS *and* to those whose data were compromised. Afterwards, your violation gets posted here.

So how do you avoid trouble? Included in the changes that practitioners must make is updating their Notice of Privacy Practices. The updates should include statements regarding how a person's data is to be handled - who it's shared with, for what purposes - and must include an option for them to request that you not share certain things.[1]

Take Action

Despite the scope of changes that must be made in practices large and small over the coming months, there is a light at the end of the tunnel. And it's closer than you think. The good news is that you, or your parent organization, can make great strides towards compliance with relatively little effort.
Here are a few take-home points:

1. Encrypt data on any computer in your office, *especially* laptops. Stolen, unencrypted laptops make up a substantial portion of breaches. Encrypting computers is much easier to implement then you might think it is. The two major operating systems - Windows and Mac OS X - ship with built-in encryption software. You'll need to either read the OS documentation or do a Web search to get the specific instructions for your machine, but the process is generally pretty quick and painless. Once the encryption process is complete, you'll never notice anything different about your computer's performance. You'll have to enter a password every now and again, but that shouldn't be a big deal, given the possible penalties for Security Rule violations.
2. Make sure that emails or other electronic transmissions between yourself and other entities are also encrypted. [2] There are various options for encrypting emails; some email platforms do this automatically. Check through the software manual, or ask your helpful in-house/on-call IT person about whether or not the platform you're using sends encrypted emails. For private practitioners, a good place to start is GnuPG. Once your data are encrypted, you automatically enjoy an incredibly high level of protection and reduced liability per the Breach Notification Rule. Importantly, you are not required to report a breach of ePHI if the data were encrypted to begin with. This is because most modern-day encryption algorithms are secure enough to be considered unbreakable.[3]
3. Update your Notice of Privacy Practices to reflect the new HITECH changes. Let your patients/clients know how you use and store their data, and what you plan to do if you experience a breach (hint: have a Risk Assessment in place *before* you experience a breach). Updating your

Notice of Privacy Practices is also very doable. Download this model Notice of Privacy Practices, courtesy of HHS, and customize it with your practice information using either a PDF reader *or* directly in a web browser.

Take some time over the weekend to review the material linked in this article. Make sure that you're doing what's needed to be compliant. There are several things to consider and changes to be implemented. The first, best step, though, is familiarity with these regulations in the context of your own day-to-day practice.

1. There is a minimum standard of information sharing that still exists, stipulating that some information *must* be shared for treatment and payment purposes.

2. Now would also be a good time to review your contract with them, and make sure that they're compliant with the upcoming changes, too.

3. even if the ciphers are cracked, it can take up to 2×10^{118} years. That's a lot of years, and anyone's PHI will be a nonissue after this length of time for obvious reasons.