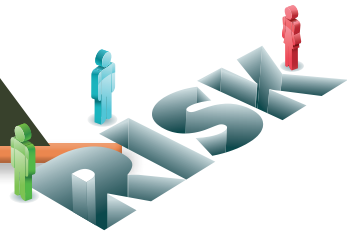

Of software patches and privacy breaches

Question: I am a licensed solo counselor. I engage in electronic transmission of health care claims, and I am considered a covered entity by the Health Insurance Portability and Accountability Act (HIPAA). However, I am not an expert in technology, and trying to keep up with privacy requirements can be frustrating. I was at a conference recently where the speaker was talking about HIPAA, and I became overwhelmed when he started talking about software patching and why HIPAA requires it. When I returned home and looked at my notes, they made no sense. Can you shed any light on what I, as a counselor, need to do in this regard?

Answer: I certainly understand your frustration. Although I may be dating myself, when I was young, "patching" was something we did to old blue jeans. It has a very different meaning in the era of technology.

The speaker at your conference may have been referring to "Guidance on Software Vulnerabilities and Patching," published by the U.S. Department of Health and Human Services Office for Civil Rights in its June 2018 cybersecurity newsletter (available at *hhs.gov/sites/default/files/cybersecurity-newsletter-june-2018-software-patches.pdf*). The document highlights the importance of identifying software vulnerabilities and underscores the *requirement* that every HIPAA covered entity perform a "risk analysis." This is a complete assessment of potential risks and vulnerabilities that could jeopardize the confidentiality of electronic protected health information. In essence, several major software vulnerabilities were discovered in 2017 that affected computer processors manufactured over the previous decade. These have led to malware attacks and serious health care privacy breaches.

How might a counselor mitigate such software risks? This is where patches come into play. It may be that your electronic health records vendor routinely applies such patches as needed. However, you should ask your vendor what is being done to update your software. If your software or electronic hardware itself is outdated, patches may not be available. You may need to implement other controls, such as restricting network access or disabling certain functions.

You should also check your contracts to see what type of assistance might be available to you. If you enter into future contracts, consider opting for ongoing support. If you use the services of an information technology (IT) professional, remember that you may need to execute a HIPAA "business associate" contract with that professional for that person to access electronic protected health information. Sample business associate contract provisions are available at *hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html*.

I often recommend that counselors in private practice seek recommendations from colleagues regarding local health care attorneys and IT professionals. This is important at the time of setting up a practice, when negotiating and executing electronic health records contracts, when a privacy breach is suspected and periodically when conducting risk analyses. I understand that there is an expense involved with this process, but the cost may be far greater if breaches actually occur. You might consider speaking with colleagues at the state and local levels to see if you can negotiate such professional services at a group discount. ❖

Anne Marie "Nancy" Wheeler is an attorney licensed in Maryland and the District of Columbia. The information presented here is for educational purposes only. For specific legal advice, please consult your own local health care attorney.

Letters to the editor: *ct@counseling.org*