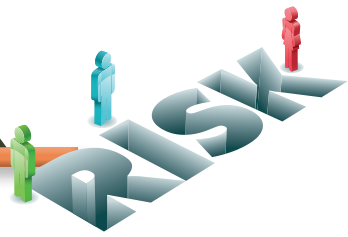

Protecting against ransomware

Question: I work in a seven-person multidisciplinary mental health practice that utilizes electronic health records. Toward the end of a recent staff meeting, one therapist mentioned that we needed to take steps to prevent "ransomware," or else we could be subject to sanctions under HIPAA (the Health Insurance Portability and Accountability Act). What does this mean, and is it truly a matter of concern for a licensed professional counselor in a small mental health practice?

Answer: Most adults have heard of the kidnapping of Charles Lindbergh Jr. in 1932 and the ransom demands exacted in that heinous crime. Most counselors have never dealt with issues of kidnapping and ransom, even if they have counseled victims of serious crime. However, in 2017, it's time for counselors to learn what "ransomware" is and how to prevent it.

I would encourage counselors to read "Fact Sheet: Ransomware and HIPAA," published by the U.S. Department of Health and Human Services and available at *hhs.gov/sites/default/files/RansomwareFactSheet.pdf* (hereinafter called "HHS fact sheet"). As this document explains, ransomware is malicious software, frequently called "malware," designed to deny access to the user's own data by encrypting it with a decryption key known only to the hacker. This process essentially holds the data hostage until the user pays ransom, frequently in the form of currency called "bitcoin" (digital currency). Ransomware can enter the user's system by "phishing," "malvertising" and network penetration.

According to the federal government, in early 2016, there were approximately 4,000 ransomware attacks per day, representing a 300 percent increase over the previous year (see *justice.gov/criminal-ccips/file/872771/download*). Among health care providers, hospitals and large providers may be more attractive targets for ransomware attackers than would be a small practice such as yours because large institutions have greater financial resources than do most small mental health practices. This does not mean, however, that small mental health practices are immune from ransomware attacks. Cybercriminals could target mental health providers, knowing that patients' and clients' protected health information is very sensitive and that providers would want to take all possible measures to safeguard the release of mental health records.

The HHS fact sheet has specific suggestions for preventing and dealing with ransomware attacks, including reviewing your HIPAA security management and performing a thorough risk analysis of vulnerabilities in your record-keeping and electronic communications systems. If you already have specific policies in place, as you should, consider updating them and specifically mentioning what you are doing to avert ransomware attacks.

If you are like most mental health professionals, you didn't go into the counseling profession to be a technology expert. Find a qualified technology professional who will help you evaluate your system and who is willing to sign a HIPAA business associate contract so that he or she can legally access your protected health information. Consider regular backup of your data if you are not already doing that on a regular basis.

You may also wish to consider purchasing a cybersecurity insurance policy to cover the practice in the event of breaches. Remember that breaches of unsecured protected health information require reporting to clients, the U.S. Department of Health and Human Services and, in some cases, the media (see *hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html?language=es*).

Make it your resolution for 2017 that you will take steps to protect your clients' sensitive information while also protecting your own professional practice.

~

The question addressed in this column was developed from a deidentified composite of calls made to the Risk Management Helpline sponsored by the American Counseling Association. This information is presented solely for educational purposes. For specific legal advice, please consult your own local attorney. ❖

Anne Marie "Nancy" Wheeler, an attorney licensed in Maryland and Washington, D.C., is the risk management consultant for the ACA Ethics Department.

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