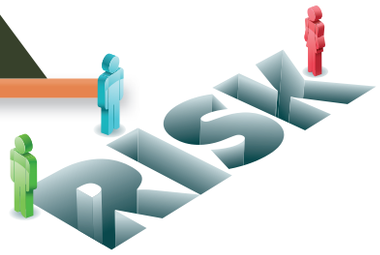

Potential privacy problems with cloud-based storage

Question: In my private counseling practice, I work with an Internet-savvy population of adult and adolescent clients. Some have suggested using Internet-based storage sites such as Dropbox, Google Drive and iCloud to exchange "homework" that I recommend for certain issues. Does use of such sites present any special privacy issues, especially for those of us who are considered to be HIPAA covered entities?

Answer: You raise a very timely issue. Cloud-based storage can pose privacy problems, especially if information is not properly encrypted. In evaluating the risk involved in using cloud-based storage, counselors should find a company that is willing to assume risk by signing a HIPAA (Health Insurance Portability and Accountability Act) business associate agreement.

The federal government recently published one specific example of a major privacy headache for a health care entity using cloud-based storage. On July 8, St. Elizabeth's Medical Center in Boston entered into an agreement with the U.S. Department of Health and Human Services Office for Civil Rights to resolve a HIPAA-related complaint that involved an Internet-based sharing and storage application. The actual agreement may be viewed online at *hhs.gov/ocr/privacy/hipaa/enforcement/examples/SEMC/ra.pdf*.

The complaint against St. Elizabeth's originated in 2012 and claimed that workforce members used an Internet-based document-sharing app to store documents containing patients' electronic protected health information (PHI) without first having analyzed the associated risks of such use. Additionally, the Office for Civil Rights' investigation discovered that St. Elizabeth's failed to:

- Identify and respond to a known security incident in a timely manner
- Attempt to mitigate the harm
- Document the incident and resolution

To add insult to injury, a separate security breach of unsecured electronic PHI from a workforce member's personal laptop and USB flash drive was reported by St. Elizabeth's to the federal government in 2014. The settlement calls for St. Elizabeth's to pay a $218,400 penalty in addition to adopting a vigorous correction plan designed to address deficiencies in its HIPAA compliance program. See details at *hhs.gov/ocr/privacy/hipaa/enforcement/examples/SEMC/bulletin.pdf*.

One useful tool for counselors with questions such as yours related to HIPAA/HITECH (Health Information Technology for Economic and Clinical Health Act) privacy, security and breach notification is the *Guide to Privacy and Security of Electronic Health Information* (Version 2.0, April 2015), published by the Office of the National Coordinator for Health Information Technology. This guide, designed especially for small health care organizations, may be accessed at *healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf*.

Also remember that states may have their own laws regarding privacy breaches. State attorneys general are often charged with investigating breaches and enforcing applicable laws.

~

The question addressed in this column was developed from a de-identified 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. To access additional risk management Q&As, go to *counseling.org/ethics* and scroll to the bottom of the page for the ACA members-only link to the Risk Management section of the website. ❖

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*