Health Information Data Security: Low-Tech Action in the Trenches to Thwart High-Tech Threats

LEGAL PERSPECTIVE FROM JEFF BRECHT

The U.S. Department of Health & Human Services Office of Civil Rights' (HHS/OCR) so-called "Wall-of-Shame" — an online list of breaches (and breachers) of unsecured protected health information (PHI) that affect 500 or more individuals — has grown substantially in 2017. According to the list, this year's jumbo-sized PHI breaches range from improper information disposal to hacking to plain old theft, and the location of those breaches run the gamut from emails to network servers to portable electronic devices. In some instances, the type of breach is enigmatically categorized as "loss" and the location described as "other," leading at least one person (namely, this author) to wonder if the Demogorgon from Netflix's *Stranger Things* may have appropriated PHI and squirreled it away in the Upside Down.

Then, in mid-May, "WannaCry" happened. As a (perhaps unnecessary) reminder, WannaCry is a strain of ransomware that hit health care providers hard around the world. In some cases, *very hard* — encrypting data so that doctor and nurse access to medical records were, at least temporarily, blocked. There were even reports that WannaCry infected certain medical devices in the U.S., including radiology imaging devices. Those negative impacts appear to support the theory that medical providers are often targeted for cyberattacks because, among other things, failure to promptly pay the ransom demanded to obtain the key to unencrypt data might harm patients by delaying care or causing clinical mistakes. Though software patches and some clever reverse engineering slowed the May ransomware incident, it was yet another reminder that health care providers must remain proactive and vigilant to protect PHI.

Of course health care providers should continue to work with data security experts to properly comply with the HIPAA obligation to conduct a thorough evaluation of electronic PHI risks and vulnerabilities in their particular organizations. Data security experts can also help with technical measures such as making sure software is up-to-date; installing and maintaining encryption technology on devices; and implementing an appropriate password protection software. But what about health care staff, the people in the trenches who actually work with and rely on the PHI to perform their jobs? Turns out that even as our technology becomes more advanced, there continues to be some simple and effective, low-tech steps that health care providers can take to keep health care staff actively involved in protecting PHI. Here are a couple examples:

STICKY NOTES: On my computer monitor, I have a sticky note on which I wrote: "Stop and Think Before You Click That Link." It's a gentle and persistent reminder to help me avoid a ransomware or other malicious software attack by taking a wary look at the emails I receive, especially where they have attachments or include internet links. Health care providers could easily do the same thing. They could even make a game of it by handing out sticky notes to staff and encouraging them to come up with their own anti-virus slogans to stick on their computers. Make it a weekly or monthly contest and offer a coffee or movie gift card to staff who create particularly clever slogans.

WORK AREA SIGNAGE: Hang up in work areas (where patients are not present) a modified version of the typical factory "Days Without Injury" sign. Your sign, which would be updated daily, could instead say something like "This Department Has Worked [ ] Days Without a Privacy Breach. Do Your Part to Comply With HIPAA."

An important benefit of these type of low-tech steps is that they can help raise

and maintain staff awareness of privacy and data security issues long after workplace HIPAA training has been conducted. These types of steps can also help foster the team atmosphere that is essential to implement effective privacy and data security policies. Moreover, these type of low-tech data security steps can be extremely effective at preventing many of the types of breaches featured on the HHS/OCR Wall-of-Shame. Finally, HHS/OCR HIPAA guidance stresses that there is no one-size-fits-all blueprint for securing and protecting private data. Health care organizations can include low-tech data security measures that best fit their particular risks. ■

Jeff Brecht is member of Lane Powell's Privacy and Data Security Practice Group and has more than 20 years of trial experience representing businesses and individuals in state and federal court. Jeff also regularly advises and represents long term care and senior living businesses and professionals. Reach him at 503.778.2162 or brechtj@lanepowell.com