COSMOS
Navigate the Compliance Universe

Compliance Today - March 2022
The weakest link in securing communications

By Drew Williamsen, MHA, CHC, CHPC


Drew Williamsen

Drew Williamsen (dwilliamsen@gmail.com), Area Compliance Program Director, Banner Wyoming Medical Center, Banner Health, Casper, Wyoming.

- linkedin.com/in/drewwilliamsen/

As compliance and privacy officers, we receive a lot of questions inquiring whether it is permissible to send protected health information (PHI) to physicians or other entities in a seemingly endless array of random situations. Many of these questions do not always fit squarely into a "yes" or "no" response. The fact that we receive these kinds of questions is a positive sign that someone is thinking about what it is they are doing and whether it is HIPAA compliant.

Ten to 15 years ago, many companies in the healthcare space did not have secure communication methods for PHI. Most companies' methods of communication fit the definition of "unsecured."[1] Employees would often email or text PHI without a second thought of whether it was compliant, as many were simply unaware. I responded to an issue years ago where an employee sent PHI via their personal, unencrypted email to a fellow employee's work email. The employee didn't think there was an issue: After all, they had been doing that for some time, and no one ever said anything about it, so how would the employee be aware?

In today's healthcare universe, it is almost unthinkable that a company would be so rogue as to not make an effort to encrypt an email or to use secure texting. Obviously, there are nuances and one-off circumstances that can occur (e.g., a brand-new provider who doesn't know the organization's policies on texting PHI) that certainly keep us compliance and privacy officers busy, but overall, healthcare organizations are trying. We all realize that no one is immune to a breach or mistakes, but appropriate levels of vigilance are necessary to stave off the inevitable for as long as possible.

The past and present

Early on in my career, I worked for an organization that—when I started—did not have secure email or secure texting. HIPAA was still somewhat new, and the organization wasn't alone in not being compliant with all the rules. At the time, many organizations were still trying to figure out what secure meant. I recall working with IT to implement a process so the company could protect itself by protecting PHI contained in emails and texts. I remember being so excited when we rolled out the secure texting application! I loved telling doctors that they could now text PHI; the surgeons could text pictures of wounds, tumors, and injuries and send them to staff to upload to the patient's electronic medical record. I thought I was delivering the best news. The physicians were so excited, until they found out they still needed to carry around a pager! They all wanted a paging system included in the texting app, but unfortunately it wasn't an option at the time.

I mention that story because I remember having numerous discussions with IT and others about what "addressable" meant and trying to get them to understand the company had to at least look and see what level of encryption was appropriate for them. In my experience, many mistakenly thought that if they didn't want to address it, they didn't have to. Eventually, all systems got squared away, and secure communication was possible

between all parties involved.

Fast forward to today, you'd be hard-pressed to find a healthcare company that doesn't have some form of encryption for both email and text messaging. One of the biggest security concerns we face today is one that has always existed and that comes from a lack of adequate training provided to employees regarding appropriate steps to safeguard data. Privacy has come a long way in the past two decades. As technology keeps evolving, companies keep adapting to keep up, but the biggest challenge remains whether the staff can keep up by properly following procedures specifically designed to keep PHI safe and secured when emailing and texting.