Word Count: 965

Social Media, "BYOD," and HIPAA: Legal Risks for Physician Practices

By Daniel F. Shay, Esq.

Alice G. Gosfield & Associates, P.C.

Social media as a technology has been adopted at a staggering rate in the United States. Between 2005 and 2016, social media usage by adults skyrocketed from 8% to 77%.[1] At the same time, smartphone and tablet technology has become ubiquitous. Physician practices may see the benefit of using social media as a marketing and patient outreach platform, and may likewise see the cost benefits for allowing employees to use their own mobile devices for work (a practice known as "BYOD" or "Bring Your Own Device"). Yet both technologies come with risks. Meanwhile, employees are also likely using social media for personal uses, creating additional HIPAA risks for the practice. This article addresses some of the HIPAA pitfalls posed by social media and mobile technology, and offers some practical advice for navigating them.

The Risks

While practice physicians and staff are likely well trained to restrict their disclosures of PHI in a "real world" context, the key problem with respect to HIPAA disclosures online arises in recognizing when PHI is actually being disclosed while posting on social media. Ideally, with effective training, physicians and staff alike can be taught to think twice before posting, and to recognize when their post might unintentionally include PHI.

In most cases, improper disclosures on social media are unintentional. For example, our firm represented a physician clinic where a front desk employee almost unintentionally posted PHI. The employee was given an apple by a patient from the patient's orchard. Delighted by the gift, the employee took a photograph of it on her desk, and posted the photo to social media, with a comment about how much she loved her job and the patients there. Unfortunately, the apple sat atop a charge sheet, listing partial names, medical record numbers, and other identifying information. Fortunately, the apple dominated the picture and obscured the PHI to the point where it was rendered unreadable, but it was a close call for the client.

In the BYOD context, improper HIPAA disclosures may occur when colleagues communicate with each other through unsecured, unencrypted methods, such as the built-in text function on a smartphone (as opposed to a secure texting app). This would risk the message (1) being stored on unsecured (for HIPAA purposes) "cloud" storage offered by a mobile carrier, or (2) including patient data alongside personal information, such as a photo of a patient's condition

[1] Social Network Use, Pew Research Center, http://www.pewresearch.org/data-trend/media-and-technology/social-networking-use/.

next to a picture of the family dog on the smartphone's "camera roll." In addition, a lost or stolen smartphone likely will risk the security of any PHI on the device. Similar circumstances have been the basis for several multi-million dollar HIPAA settlements with government enforcers.

Practical Advice

The first step to address HIPAA risks arising from the use of social media or BYOD devices is to conduct a security risk assessment (SRA). The SRA is required under the HIPAA Security Rule. The Department of Health and Human Services' Office of Civil Rights (OCR) has described an SRA as "foundational" to HIPAA compliance. Without one, a physician practice is flying blind; and any policies or procedures crafted will likely be deemed ineffective by the OCR if the practice is investigated. The SRA should specifically consider the risks posed by the use of social media and, if the practice is adopting one, a BYOD policy. The next step is to develop policies and procedures to address the risks identified in the SRA. These should address issues such as training of physicians and practice staff in the proper usage of social media and use of their BYOD devices.

With respect to training, physicians and staff alike need to understand PHI in context. This means going beyond the mere definition of the term or descriptions of the concept. Most likely, they are already aware that names, birth dates, social security numbers, etc. are PHI. But consider the example of the apple on the charge sheet, described above. This is a classic case of PHI in context. The employee didn't think she was posting a picture of PHI. She thought she was just posting a picture of an apple. She probably also did not consider the implications of the photo being stored on her phone, and what it would mean if her phone was stolen or lost, while storing a picture with PHI in it.

Adopting a BYOD policy exposes a practice to increased risk regarding the loss or theft of BYOD devices and the disclosure of stored PHI. Therefore, policies should address issues such as what security controls the device must have in place (e.g., longer passwords, requiring biometric information to unlock, etc.); what apps are approved or required for use for work purposes; and whether to include "killswitch" technology that can remotely wipe PHI off the phone in the event of its loss or theft. Another option is to require the use of the employer's own wifi or other IT infrastructure while at work, which itself should be rendered secure for HIPAA purposes.

Conclusion

With 77% of American adults using social media, the genie is clearly out of the bottle; prohibiting any use of social media relating to work or at the workplace is likely unenforceable. Many physicians may prefer to use their own phone for work purposes, rather than carry an additional work phone with limited functionality. Offering a BYOD policy can also be helpful in

offsetting expenses for the practice. This only makes confronting the risks imposed by social media and BYOD policies more pressing, and highlights the need for effective policies and procedures to address their use. Knowledgeable health care counsel can help in the crafting of such policy, and should be consulted. In designing policies as well as when problems arise when they are implemented.