By Michael Matheson
MAFP Legal Counsel
michael@mathesonlawfirm.com

Maintaining HIPAA Compliance in an Ever-changing World

Just when you think you couldn't be any more compliant with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), someone, or something, reminds you that the rules of data privacy and practical implications for adherence are constantly changing.

Such is the case with the highly publicized Uber, Equifax, Home Depot, and Target data breaches of the past few years. While these examples do not fall within HIPAA, they show that even the largest of companies are not immune to breaches compromising individuals' personal information.

In today's ever-evolving world of social media and mobile apps, protecting patient health information is an increasingly complex and monumental undertaking. As an attorney, I am often asked questions regarding HIPAA compliance. Below is a practical Q&A to help guide you through some of today's hot button issues around protected health information.

While I would like to think that my practice is HIPAA compliant, what measures do you recommend for ensuring compliance?

- Conduct an ***inventory*** of protected health information (PHI) so you know exactly what information you are responsible for securing. You can't protect what you're not aware of. Review the types of data your practice collects, uses, stores, shares, and disposes of, including electronic PHI (ePHI) that may be located outside of your physical office space on network servers, cloud-based applications, laptops, tablets, and other mobile devices.
- Perform a ***security evaluation*** on a regular basis, especially when new employees are hired and/or operational changes are implemented. Review your practice's security policies and procedures, making sure they are up-to-date and aligned with HIPAA's requirements for securing PHI and ePHI.
- Make sure your practice has an ***Incident Response Plan*** in place; establish one, if it does not. The Plan should include forming an Incident Response Team and provide training for members to practice responding to an actual or threatened release of PHI/ePHI. An additional best practice is to include in the Plan an explanation of how team members notify individuals and governmental agencies, when required by law, in the event PHI is released. A Plan that follows these principles will help shield your practice from potential fines, penalties, and costly lawsuits. Keep in mind, however, that a Plan that works for another medical practice may not fit your particular requirements; therefore, tailor your Plan to fit your specific needs.

I'm very busy and not sure if my office manager is keeping up-to-date on the technical requirements of HIPAA. What basic, practical steps do you recommend that my practice adopt to remain HIPAA compliant?

While compliance with the security rules of HIPAA are generally mandatory for ePHI, the following are some basic measures you can take to limit your potential risk:

- Ensure computers and devices are password-protected and ePHI is encrypted.
- Close and log out of computer programs containing patient information, when not in use.
- Do not allow employees to share passwords.
- Make sure up-to-date anti-virus software is installed on all computers and devices.
- If employees are permitted to access patient information when outside of the office, ensure home computers and laptops are password-protected and running up-to-date security software.
- Back up all ePHI, preferably on a HIPAA-complaint cloud server.
- Keep patient paperwork, charts, and records out of view and locked when not in use.
- Always use a cover sheet when faxing PHI.
- Properly dispose of files by shredding.
- Conduct regular and thorough compliance training.
- Make sure employees understand that sharing patient information via social media is a HIPAA violation.

Regarding social media and HIPAA, what are some of the issues I need to be concerned about?

Adoption of a comprehensive social media policy will go a long way toward limiting improper exposure of ePHI. The speed with which physicians and patients can communicate using social media and other technology has permanently altered the way medicine is practiced. When electronic communications are used for assessing and treating patients, these communications must be secure. Remember that a patient does not have to be physically present in your office for your communications to be considered PHI.

While it is impossible to completely monitor every employee's social media activity, especially when much is conducted on personal time, it is important to constantly remind and train employees on the proper use of social media and the preservation of ePHI. In addition to protecting confidentiality, your practice's social media policy should preclude pictures being taken anywhere within the medical facility without the permission of a supervisor. Pictures that capture patient images should normally be avoided in all instances. While labor laws allow employees to discuss their work conditions, details of an employee's work day that relate to patients should never be shared.

I have heard about cases involving stolen or lost laptops that contain patient health information. Should the patient information I have on laptops or tablets be encrypted?

Encryption means that data is encoded so only readers who have the correct "key" can read it. While HIPAA does not specifically mandate email encryption, most experts urge its use to protect both patients and medical practices.

Just this year, Children's Medical Center of Dallas was fined over $3 million for violating HIPAA security rules. The hospital was cited for, among other violations, losing an un-encrypted, non-password protected mobile device at an airport. It was also reported that an un-encrypted laptop was stolen from the hospital's premises. Due to these two instances, the ePHI of over 6,000 individuals was compromised; and, since the devices were un-encrypted, the hospital was required to report the losses.

A disgruntled former patient called my office manager to complain of a billing situation. Unable to resolve the matter over the phone, the former patient came to my office, belligerent and refusing to leave the patient waiting area. While there, she recorded the situation on her cell phone. My patients did not consent to being videotaped and several were upset when the former patient said she would post the video to YouTube. I am concerned about my HIPAA violation risks. What should I do?

HIPAA security standards require that medical practices maintain written security policies and procedures, including those that cover personnel training and sanctions for security policy violations. Therefore, preparing for this type of situation should be included in a general emergency preparedness plan / policy, of which all staff members are familiar. The first step of action in this situation should be to contact local authorities for assistance, as you cannot be assured that the individual will not attempt to harm your patients or staff.

Since HIPAA applies to healthcare professionals, the risk of violating security rules in this situation is minimal, as the person who performed the videotaping is not a staff member and, therefore, does not fall within your practice's HIPAA obligations. Also, regardless of whether the videotape is made public, the presence of a person in the patient waiting area is not likely to be considered PHI. However, your practice would be in violation of HIPAA privacy rules if the disgruntled former patient gained access to patient data and made it public. ■
