Ask An Attorney

By David H. Fitch, Esq., Underberg & Kessler LLP

Q My general practice partner and I have noticed a sharp increase in the number of patients who wish to communicate by email or text. What concerns should we have about this electronic exchange of HIPAA-protected information?

A Smart phone technology, and its recent meteoric rise in use, has provided a completely new platform for care providers and patients to communicate. Whether texting or emailing, these electronic mediums allow physicians to treat more patients than actually walk through the door, and enables patients to provide symptoms and information, and receive treatment recommendations, in real-time without the delay or "inconvenience" of the traditional callback, page, or in-office visit.

Notwithstanding these advantages, physicians must be cognizant of the requirements under HIPAA and the HITECH Act (together, HIPAA) when they or their staff email or text with patients. A practice's failure to protect the personal health information (PHI) of its patients could result in significant HIPAA penalties. The security rules under HIPAA relating to electronic PHI require care providers and their business associates to implement appropriate physical, administrative, and technical safeguards to ensure the confidentiality, integrity, and availability of all electronic PHI they create, receive, maintain, or transmit. Aside from just making sure such communication is made part of a patient's chart, this includes conducting risk analyses, securing network servers in locked locations, training staff, shielding screens from unauthorized viewers, implementing secure passwords, and encrypting messages sent and received.

The Office of the National Coordinator for Health Information Technology (ONC) has outlined five steps for care providers to help manage the secure use of mobile devices. First, a provider, practice, or organization must decide whether mobile devices will be used to access, receive, transmit, or store patients' health information. Next, a risk assessment that analyzes the threats and weaknesses of the personal health information being maintained should be conducted. Although the size of an organization, and the complexity and reach of its practice, will determine the methods used, all providers are required to conduct an appropriate risk analysis. Third, a mobile device risk management strategy which includes security and privacy protections should be created. This may include the use of third-party messaging solutions to ensure a secure communication platform for texting or emailing on approved, password-protected mobile devices, including those personally-owned by staff, and the safe disposal of those devices. Mobile device policies and procedures must then be created and implemented throughout the practice. Finally, in-service privacy and security training for all medical staff must be provided. This requires being vigilant of changes in the regulatory landscape, which may include additional guidance from ONC and the enforcement of electronic communications-related HIPAA violations. For more information, visit: www.healthit.gov/providers-professionals/five-steps-organizations-can-take-manage-mobile-devices-used-health-care-pro.

The advent of the digital age and recent technological advances in electronic communication has forever changed how care providers interface and treat patients. This provides significant opportunities for physicians and their staff to render more efficient, high-quality care to more people, but it's imperative to first understand and implement HIPAA-required safeguards to protect patients' health information.

Reprinted with permission from The Bulletin - May/June 2016.
Published by Monroe County Medical Society. www.mcms.org