Ask An Attorney

BY ANNA E. LYNCH, ESQ., UNDERBERG & KESSLER LLP

Q **My medical practice has a compliance plan and all staff are trained on HIPAA. However, my practice manager is insistent on implementing some electronic security measures that I believe are too stringent. What is enough?**

A We have all heard of data breaches at large nationwide stores and health insurance companies. Hijacking records for ransom at hospitals and large health systems is also big news. What isn't making as many headlines is hackers stealing patient identities through physician practices. Even though it's not in the news, it is happening every day. Hackers realize tremendous value in stealing patient information that they can then use to commit several types of fraud.

Generally, we recommend physician practices seek advice about cybersecurity issues from technical vendors. However, there are some steps any practice can take on its own.

The practice's computer network system must be secured. Never share the network password with non-employees. If necessary, create a guest network with password.

All mobile devices should be encrypted and have password protection, including mobile phones, tablets and laptops. These devices should never be left unattended in the office without being secured. When traveling, do not use unsecured WiFi – for example, airport WiFi generally is not secure and is a haven for hackers. And of course, install anti-virus software and keep it updated. For breaches from unprotected laptops, a practice can expect fines, the requirement to notify all effected patients, and possible credit monitoring for patients whose data has been compromised.

The office should require strong passwords (not "password" or "321321")! Require use of at least eight characters with a variety of letters, numbers and symbols. Every user in the office should have a separate user name, and there should be a requirement to change passwords at least every 60 days.

Consider purchasing cyber insurance. First check to see what coverage you may have through your malpractice and general liability policies. Do you have coverage for costs to notify patients in the event of a breach? Other costs to consider include state and federal fines, public relations costs, technical help for reconstruction of data, and credit monitoring. If not, look for cyber insurance that fits your practice needs.

In this day, it is increasingly important for physicians to take all necessary precautions to secure patient records, both paper and electronic. The costs for not doing so, both financially and reputationally, can be significant.

**Reprinted with permission from The Bulletin - Aug/Sept 2018,
the official journal of Monroe County Medical Society.
www.mcms.org**