Sterling Seacrest Pritchard

Top 5 Cyber Mistakes Medical Practices Must Avoid

1. Not having insurance coverage for cyber risks.

A cyber breach can very quickly exhaust all of your financial resources and cripple your medical practice. Typical costs related to a breach include: (i) IT forensics to determine the nature of the breach, the number of patients impacted, and ensuring that the threat actor no longer has access to your patient information; (ii) attorney fees for legal guidance, including patient notification, HHS notification, remedial measures, and possibly defense of a post-breach investigation by the OCR; (iii) establishment of a dedicated call center to handle patient questions; (iv) payment for credit monitoring services for all impacted patients; and (v) possible fines and penalties. Combined, these expenses can quickly add up to a seven-figure number. Most cyber liability policies cover some, if not all, of these costs.

2. Carelessly answering the cyber liability coverage applications.

Cyber liability insurers, like all other insurers, use your application responses to determine whether to issue you a policy and the appropriate premium to charge. Therefore, if you inadvertently attest on your application or renewal application that you use Multi-Factor Authentication (“MFA”), for example, but the carrier subsequently discovers during a post-cyber breach claim investigation that someone in your office turned MFA off for convenience reasons, they could use that application misstatement as grounds to deny coverage. Therefore, complete the cyber application with the assistance of your IT vendors/team, share any material attestations with staff to ensure they are complying, and have the practice owners/executives sign-off on your application responses.

3. Clicking on links in emails.

In general, most cyber breaches result from human error. Along those lines, one of the most common mistakes that office personnel make is clicking on a link in an email which appears to be legitimate. Threat actors are well-aware of this vulnerability and frequently use this tactic to gain access to your IT system and patients’ protected health information. Implement a policy that strictly forbids anyone from clicking on any email link and regularly perform vulnerability testing to check compliance.

4. Changing banking instructions based on an email request.

While you may be able to control IT security measures in the office, you have little if any control over what your employees or their family members do at home in terms of cyber security, such as refraining from clicking on email links as described in No. 3. That said, a common cyber-claim starts with a threat actor gaining access to an employee’s personal home computer, clandestinely watching them draft emails, and then posing as the employee when emailing the practice administrator to inform him/her that they have changed banks for the next direct deposit. This scheme works between companies too. Bottom line, if you ever receive an email that directs you to change the sender’s banking information, wiring instructions, etc., before doing so, call the person first to verify its legitimacy.

5. Waiting to report a cyber breach.

Timely response to a breach is critical, and the first few steps you take could cost or save you thousands of dollars in expenses. Most cyber insurance liability policies provide a 24-hour hotline where you can report breaches and get a “breach coach” engaged immediately to assist. Similar to other “crime scenes,” you often will be instructed to “preserve the evidence” so the IT forensic team can determine what information has been compromised, whether the threat actor still has access, etc. This investigation, in turn, will then be used to understand the extent of the breach and what corresponding notices will be required. Everyone in the office should know who to call if/when they suspect a breach may have occurred.