Health Information Compliance Alert

Case Study: Recent Settlement Highlights Small Practice Vulnerabilities

Put some thought into your HIPAA security or pay the price.

Small practices often place HIPAA security on the B-list of their administrative and fiscal priorities. However, the first enforcement action of 2020 suggests that providers of every size and shape should manage their risks accordingly - or be ready for the feds' wrath.

Context: Due to failures to address HIPAA Security Rule violations related to a business associate (BA) issue and 2013 breach, the Ogden, Utah-based gastroenterology practice of **Steven A. Porter, MD** settled with the **HHS Office for Civil Rights** (OCR) to the tune of $100,000. The practice also agreed to a two-year corrective action plan (CAP) that requires the firm to implement new policies and procedures, better risk management, and more.

During an OCR investigation into the organization's breach and HIPAA protocols, the agency discovered that the gastroenterologist dropped the ball on risk analysis and management. The compliance failures left Porter's small practice, which services just over 3,000 patients annually, vulnerable and resulted in OCR's heavy enforcement.

Plus: According to the resolution agreement, "the practice's breach report claimed that **Elevation43**, a business associate [BA] of Dr. Porter's electronic health record (EHR) company, was impermissibly using the practice's patients' electronic protected health information (ePHI) by blocking the practice's access to such ePHI until Dr. Porter paid Elevation43 $50,000."

The resolution agreement does not name Porter's EHR vendor.

Review the resolution agreement and CAP at www.hhs.gov/sites/default/files/porter-ra-cap-508.pdf.

"All healthcare providers, large and small, need to take their HIPAA obligations seriously," warned OCR director **Roger Severino** in a release. "The failure to implement basic HIPAA requirements, such as an accurate and thorough risk analysis and risk management plan, continues to be an unacceptable and disturbing trend within the healthcare industry."

Understand the Necessity of Skilled Cybersecurity Experts

Small or rural practices often push HIPAA security to the bottom of their compliance to-do lists. Many reason that it's too expensive or too complicated to enlist topnotch cybersecurity experts to advise them on how to address their risks. Another issue is location and the lack of IT resources in rural areas. For these reasons and others, small practices aren't always equipped to handle major data incidents and follow up on the risk management that follows a breach.

"Small practices are at a distinct disadvantage when it comes to procuring IT and cybersecurity services. This is especially true in rural areas," explains **Adam Kehler**, principal consultant and healthcare practice lead with **Online Business Systems**. "Often they will hire the only local IT shop or an independent person that someone at the practice knows."

Kehler adds: "I've seen practices where the doctor's spouse, sibling, or niece/nephew becomes the de facto IT person. The challenge is that just because someone can configure a firewall, doesn't make them knowledgeable in information security and compliance."

Remember: The health IT field is diverse and nuanced. Some may lack the necessary skills to circumvent cyber attacks and deal with maintaining compliance of the various HIPAA rules, too.

"Many people believe their IT people are cybersecurity professionals," reminds **Jen Stone, MSCIS, CISSP, QSA**, a security analyst with **Security Metrics** in Orem, Utah. "This critical misunderstanding happens in practices of all sizes, whether they have on-site staff or outsource their technology needs. While some IT groups do know and implement security, that isn't their primary function."

Resource: See the case details at www.hhs.gov/about/ news/2020/03/03/health-care-provider-pays-100000-settlement-ocr-failing-implement-hipaa.html.

Pose These 5 Questions to Your IT Vendor

Whether your practice HIPAA security is lackluster or you're in the market for a boost to your health IT, a great way to revamp your 2020 protocols is with a fresh perspective. But, before you sign the dotted line and update your IT vendor, you may want to ensure that your new partner knows what's required. "When outsourcing, be sure to ask about security specifically," recommends **Jen Stone, MSCIS, CISSP, QSA**, a security analyst with **Security Metrics** in Orem, Utah. Consider posing these five questions to IT security experts, suggests Stone:

1. What security framework will you implement for my practice?
2. What kinds of logging, monitoring, and alerting will you conduct?
3. How will you conduct vulnerability management? Does it include all systems and software in my practice?
4. If you encounter indicators of compromise in my systems, do you have an incident response plan? Has that plan been tested?
5. Have your security services been assessed by a third party?