

Big Privacy Concerns for Small Practices

[Save to myBoK](#)

By Mary Butler

Anyone who has ever been to a doctor's office or mental health provider where the seating area is sparse can quickly ascertain that they're giving up some modicum of privacy to see that doctor. Tiny waiting areas with chairs or benches for only two to five individuals (or less) make it hard not to notice your fellow patients. By continuing to see that practitioner, patients are signaling that the benefit of the healthcare provider is worth the risk of running into someone they know.

Provider waiting rooms like this are more prevalent in rural areas and small towns, and with providers that are not affiliated with a larger integrated delivery system. The "office managers" for these physicians are often the physicians themselves, according to Barry Herrin, JD, FHIMSS, FACHE, founder of Herrin Health Law.

Compliance with federal and state privacy laws is as easy or as difficult as a practice chooses to make it—and violations have the same consequences whether a violator is a small or large practice. It's privacy breaches at large metropolitan health systems that get more media attention, as well as all the scrutiny that other providers can learn from. However, smaller practices are at just as high a risk and don't have the luxury of employing a privacy officer to keep them apprised of new threats. Without the broader resources of a large health system and staff to take care of security patches, software fixes, and legal counsel on staff, these smaller providers may have to exercise more caution and do some of their own research. A thoughtful approach to patient privacy is still possible for the "little guy," even in small towns where everyone knows each other's business.

The Nature of Violations in Small Practices

In some respects, HIPAA compliance is easier in small or solo practices because all the health information leaving a provider's hands is given out on a need-to-know basis. If a doctor doesn't have a nurse or an office manager or receptionist, the risk of the wrong person sticking their nose in patient files and leaking information goes down significantly. And the smaller the practice, the smaller the risk of being targeted by ransomware and hacking.

"Small offices also aren't trying to sell de-identified data to a drug company, they're just doing their job. For them, HIPAA wasn't a big deal because they've had to comply with state laws. Smaller is easier because you're doing fewer things with data," says Kirk Nahra, JD, a partner at the law firm Wiley Rein.

According to Herrin, in small practices—particularly in small towns—there are two particular scenarios that cause privacy problems. One is a loose-lipped office manager who leaks protected health information to friends and other patients. The other is specific to plastic or cosmetic surgery practices that use photos on their websites.

"The problem in aesthetic practices is, they don't hire the people they need to. So when they do a 'before' and 'after' picture, they don't scrub the metadata from the picture and put it online. They got consent [from those photographed] but didn't have it anonymized. I've had six cases with this in the last three years," Herrin says.

Herrin adds that this is much less of an issue in large metropolitan areas where, for example, a neurosurgeon might do consults in a small one-off clinic, where there's an office manager, though the bulk of their work is done in a hospital.

Barb Beckett, RHIT, CHPS, system privacy officer for Saint Luke's Health System in the Kansas City, MO-area, has seen this, too, although not within her large system. She has volunteered in the past to help clinics with HIPAA basics, such as writing Notices of Privacy Practices (NPPs), accounting of disclosures, and amendments and restrictions.

"I feel like the office manager, sometimes that is the physician also, have limited knowledge of processes. They may have received education on the regulations and on processes that go with compliance, but I'm pretty sure that goes by the wayside," Beckett says.

Beckett has also found that some small practices don't even have IT security knowledge, that they use Google (Gmail) as their clinic email, and that they have no idea about encryption. Any major breach would put these practices out of business quickly, in her estimation.

Protecting Small Practices

Of course, HIPAA has been the law of the land since 2003, so nobody is getting a pass on compliance. Small practices can outsource their privacy and security operations to any number of vendors and consultants. The US Department of Health and Human Services (HHS) has ample resources for providers of all sizes—after all, HIPAA was designed to be scalable.

Judi Hoffman, BCRT, CHPS, CHP, CHSS, Catholic Health Initiatives' regional privacy officer, worries that many small clinics and single physician groups may think that they are off the radar of HHS' Office for Civil Rights. That could lead to the healthcare industry seeing more privacy and security events from these small facilities, especially those clinics that outsource their IT resources, she says.

"As we know, providers need to ensure they have the basics completed, with a risk analysis performed and solid policies and procedures in place," Hoffman says. "Even small clinic settings within a large corporate structure could be at risk of ignored privacy and security events and not fully vetted with a breach risk assessment, just from either the lack of education or fear of reporting."

Nahra says that small practices just need to make a concerted effort to think through all of their processes and identify vulnerabilities—and this is just as true for large practices.

"The primary obligation under HIPAA is to think through your business activities. What do you do? What do you collect? What do you do with it? ...Is your business driven by testimonials? If that's the case, get a process," Nahra says. "If you think it's an important part of your business you have to think of a way to do that that's sufficiently privacy protected."

Mary Butler (mary.butler@ahima.org) is associate editor at the *Journal of AHIMA*.

Article citation:

Butler, Mary. "Big Privacy Concerns for Small Practices." *Journal of AHIMA* 89, no. 9 (October 2018): 32-33.

Driving the Power of Knowledge

Copyright 2022 by The American Health Information Management Association. All Rights Reserved.