The Small & Medium Sized Practice's Guide to HIPAA

As a general rule, small healthcare providers have a difficult time keeping up with HIPAA (Health Insurance Portability and Accountability Act of 1996) compliance, when compared with larger, more resourced organizations. While practices at the smaller end of the scale may be disadvantaged due to a lack of personnel, time, and budget, The HHS Office for Civil Rights (OCR) - the agency responsible for enforcing the HIPAA Privacy and Security rules - makes no exceptions on practice size when it comes to ensuring patients' health information remains protected.

To highlight this, in 2016 the OCR announced an initiative to more widely investigate HIPAA breaches that affect fewer than 500 people. While this announcement wasn't solely directed at small practices - small breaches can happen at large organizations too - it was a stark reminder of the OCR's commitment to improving privacy and security standards across the healthcare industry as a whole, and that no HIPAA covered entity is exempt from the rules.

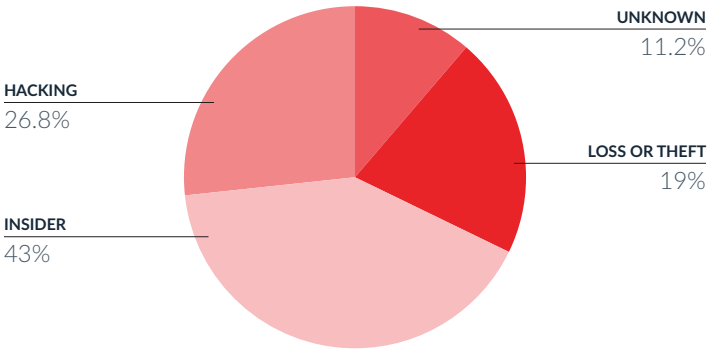
Small Breaches, Huge Consequences

According to a 2016 survey of America's physicians, there are approximately 800,000 practicing physicians in the U.S, approximately 70 percent of whom work independently or in practices consisting of 30 physicians or fewer. Just over half of all physicians - approximately 400,000 based on the figure above - work independently or in practices consisting of 10 physicians or fewer.

Physician practice size in the U.S.	2016 Percentage
Solo	16.8%
2-5 physicians	21.4%
6-10 physicians	13.5%
11-30 physicians	16%
21-100 physicians	12.4%
101 or more physicians	19.9

Source: 2016 Survey of America's Physicians by The Physicians Foundation & Merritt Hawkins

Now, consider that around a third of small practices do not have a HIPAA compliance plan in place, and it becomes clear why healthcare was the most targeted industry by cyber hackers in 2016. According to a report by Protenus, the healthcare industry averaged at least one data breach per day in 2016, affecting more than 27 million patient health records in total. Whatsmore, insiders were to blame for most of these breaches, suggesting that lack of education on HIPAA rules is a large part of the problem.



Types of Incidents, 2016 Health Data Breaches

Failure to comply with HIPAA rules can result in both civil and criminal penalties, and this applies to covered entities and business associates of all sizes. Civil penalties, which are enforced by OCR, are monetary and vary from $100 to $1.5 million, while criminal penalties, enforced by the U.S. Department of Justice can be even more severe. Unfortunately, there are many examples of small to medium sized organizations that have learned this the hard way in recent years.

Organization	Breach Overview	Fallout
Phoenix Cardiac Surgery	Posted surgery and appointment schedules on a publicly accessible online calendar	Fined $100,000 and required to take corrective actions
Center for Children's Digestive Health	Failure to provide a signed Business Associate Agreement (BAA)	Fined $31,000 and required to take corrective actions
Adult & Pediatric Dermatology	Loss of USB thumb drive containing unencrypted PHI of more than 2,000 individuals	Fined $150,000 and required to take corrective actions

Examples of HIPAA breaches affecting small practices

Naturally, smaller breaches do not receive the same national press attention as larger breaches, and often slip under the public's radar entirely, as OCR is not required to publish breaches affecting fewer than 500 individuals on its Breach Portal, or 'wall of shame', as it is more commonly referred to. However, in the digital age bad news travels fast, meaning it doesn't take long for news of even a small data breach to reach affected patients via the likes of social media, review sites, and local news pages.

This presents major reputational challenges for practices. For some organizations, fines can be paid without inflicting too much long-term damage, it is more difficult to regain the trust of patients whose PHI has been compromised. With more and more patients taking to the internet to share their personal health experiences, and influencing others in the process, the effects of a HIPAA breach can be much longer lasting than many realize.

HIPAA Compliance Advice for Small Practices

HIPAA compliance is a constant burden for all organizations, regardless of size. For large organizations, these challenges typically stem from having to manage high numbers of staff across multiple sites; this means more PHI being exchanged on a daily basis, more devices being carried around, and generally more potential entry points for cyber thieves. However, the major advantage large organizations have over smaller organizations are the resources to manage these issues by investing in the right staff, regular training, and market-leading tools.

Conversely, most small businesses simply do not have the resources for managing a full-time HIPAA compliance program in-house, nor the budget to outsource it. With no CIO or compliance specialist to oversee daily operations, responsibility lies solely with medical staff. While in one sense this makes HIPAA compliance easier to contain, individuals face a juggling act between being a medical professional and compliance expert, which can be a risky game.

5 steps to smarter security and privacy

1. Invest in the right tools
When sending, receiving, or storing PHI, it must be done within a HIPAA-secure environment. Text messaging, for example, is not a secure form of communication. Instead, practices should invest in a secure mobile messaging solution that encrypts data during its entire lifespan, ensuring only the intended recipient(s) can view it.

2. Stay educated
Whether working in a solo practice or on a team of 20 or more, education is the key to HIPAA compliance. Taking time to stay updated on HIPAA and cybersecurity best practices is critical for identifying and preventing potential breaches before they occur. If the budget is available, it can be beneficial to appoint a third-party expert to carry out staff training, as this will help ensure all key areas are covered.

3. Don't assume HIPAA is just an IT issue
HIPAA compliance is not just an IT issue. It is equally important to safeguard paper records and discard them properly, or shred them when no longer needed. This was highlighted In 2014 when the OCR reported a data breach involving over 1,500 patients, which was caused by health records being scattered down the street after being thrown in an open top dumpster by staff. The Kansas City-based facility was later ordered to pay $400,000 to compensate the patients.

4. Keep on top of BAAs

Any entity that manages the transmission and storage of PHI on behalf of a healthcare organization is known as a business associate (BA). This may include, for example, messaging platforms, hosting companies, fax and email providers, and EHRs. Under HIPAA, covered entities must ensure business associates enter into a Business Associate Agreement (BAA) to safeguard PHI. Revising business associate agreements is an arduous task for any organization, but it's crucial for ensuring HIPAA compliance. Earlier this year, a small healthcare practice was hit with $31,000 HIPAA settlement due to a business associate's agreement not being in place.

5. Secure all mobile devices

The increased adoption of BYOD (bring your own device) in healthcare environments presents many potential benefits, however according to the HHS, a reported 10 percent of major health data breaches involve a mobile device. This considered, it is critical that practices take necessary steps to ensure that mobile devices do not become a vulnerability in the security chain. As a minimum requirement, all devices that carry PHI, even temporarily, should be secured using strong passwords, encryption, and multi-factor authentication. PHI should only ever be sent, received, or stored using HIPAA-secure applications, and a BAA should be in place with all third-party providers.

This is by no means a complete HIPAA compliance checklist, and we would urge all covered entities to review the information on HHS.gov for a detailed explanation of their responsibilities under HIPAA, and advice for preventing data breaches. If past breaches have taught us anything it is that no organization is exempt from HIPAA, and the repercussions of a breach can be crippling for all involved. HIPAA compliance is an issue that needs to taken seriously, not just for avoiding fines and protecting business integrity, but also for safeguarding the privacy of patients.