



HIPAA compliance: Invest or roll the dice?

By Jeff Broudy
CEO of PCIHIPAA

Many believe HIPAA compliance is a “set-it-and-forget-it” exercise. Well, not exactly.

HIPAA compliance is an ongoing requirement, whether you are a small organization with a limited budget or a large OMS practice with multiple locations. There is no HIPAA certification.

HIPAA compliance is an environment that you must demonstrate with written proof upon audit. It is unlikely the HIPAA “police” (Office for Civil Rights) will knock at your door. It is more likely you would experience a data breach or a patient complaint that would turn into an investigation.

Maybe a lack of time, knowledge or resources have impacted your HIPAA compliance for your OMS practice. The goal is to have information to accurately plan and predict what your compliance budget should be.

HIPAA compliance considerations

The cost of HIPAA compliance depends on many variables. Some of the key factors to consider are:

- **Your organization’s size** – The more employees, programs, computers, protected health information (PHI) and departments your practice has will increase the number of vulnerabilities you might encounter.
- **Your organization’s culture, knowledge and risk tolerance** – If you have been keeping up with the news about cybersecurity and it has become a top priority, you have most likely invested in a portion of a compliance and cybersecurity program. If not, the costs to implement and maintain the requirements under the HIPAA Privacy and Security Rules will be higher.

- **Your organization’s environment** – If cybersecurity was considered when purchasing, implementing and maintaining devices, the costs to comply with HIPAA should be lower for your practice. This includes computers, software, firewalls, servers and more.
- **Your organization’s dedicated HIPAA workforce** – A dedicated HIPAA team or third-party provider will help determine what requirements your practice needs.

The cost of a data breach

If the Health and Human Services (HHS) estimate of compliance seems daunting, the costs related to non-compliance are even greater. For not protecting PHI, a practice can face the following fines and penalties:

- HHS fines – up to \$1.5 million per violation per year
- Federal Trade Commission fines – \$16,000 per violation
- Class action lawsuits – \$1,000 per record
- State attorneys general/potential fine assessment – \$150,000 to \$6.8 million
- Patient loss/not returning to doctor due to breach – 40 percent
- Free credit monitoring for affected individuals – \$10 to \$30 per record

continued on next page



- ID theft monitoring – \$10 to \$30 per record
- Lawyer fees – \$2,000-plus
- Breach notification costs – \$1,000-plus
- Business associate changes – \$5,000-plus
- Technology repairs – \$2,000-plus
- Credit card replacement costs – \$4 to \$5 per card

Data breaches happen

In 2019, according to the HHS Breach Portal, more than 40 million patient records were compromised, mostly because of a hacking incident or some other type of unauthorized use.

Ransomware has become an epidemic throughout the healthcare industry. Software company Emsisoft identified the following ransomware attack trends:

- **Cybercriminals target Managed Service Providers (MSPs)** – Cybercriminals are increasingly targeting software used by MSPs and other third-party service providers to simultaneously attack service providers and their customers.
- **Ransoms are increasing** – Cybercriminals want to maximize their profits and, as such, are increasing their ransom requests.
- **Cyber insurance drives ransom payments** – Organizations that leverage cyber insurance are more prone than others to pay cybercriminals' ransoms.
- **Cybercriminals prioritize email and remote desktop protocol (RDP)** – Emails and RDP attachments represent the top choices for cybercriminals to launch ransomware attacks.

You should start thinking in terms that a ransomware attack or data breach will happen. What precautions should you begin implementing today to reduce your overall exposure? Practically, this is where implementing a comprehensive HIPAA compliance program makes sense. Even though the rules are hard to follow, the overall intent is to protect the privacy and security of your patient information. And that information has proven to be under attack.



4 areas of focus

Many practices do not know where to start, or they go online and try to find the answers. Here are four areas to focus on:

1. **Basic cybersecurity** – Check with your IT provider and make 100 percent sure your data backup is offsite (in the cloud), encrypted and your data can be restored in less than 24 hours if an incident occurs. Also, be sure you have multiple backup sets in case one fails. Finally, deploy up-to-date firewalls and antivirus software to protect your network from outside threats.
2. **Take a risk assessment** – The HIPAA Security Rule requires you have taken a risk assessment of your vulnerabilities and documented an action plan to fix them. It's the law, and it's a good idea.
3. **Train your employees** – Obtain an updated set of policies and procedures and train your employees about them. They are your first line of defense. If they do not understand the risks and what is required, they will not be able to identify threats and help protect your practice.
4. **Obtain cyber insurance** – You are more likely to use a cyber-insurance policy than your general liability or malpractice policy. A comprehensive cyber policy will financially protect you in case of ransomware attack, data breach, HIPAA fine or other types of security breaches.



Estimated compliance costs

Whether you decide to take on HIPAA compliance internally or seek a trusted advisor, some of the material costs you should expect to incur have been outlined. The key considerations will impact your investment decisions.

If you are a private healthcare provider, annual compliance costs are outlined approximately on an a-la-carte basis. Companies combine some or all these services. This will give you a good idea of the range you should consider for protecting yourself from potential losses:

- Risk analysis and management plan – \$1,000 to \$2,000
- Employee security and privacy training – \$2,000 to \$3,000
- Policy development – \$1,000 to \$2,000
- Email and data backup – \$500
- IP scanning and PCI certification – \$250
- Business association management and documentation – \$500
- HIPAA compliance documentation and audit support – \$300
- Emergency and incident response planning – \$1,000
- Cybersecurity insurance – \$2,000 (not required; recommended; depends on revenue)
- Additional technical safeguards – (password management, device monitoring, firewall and antivirus updates) – \$1,000 to \$2,000

Larger practices and hospitals can expect to pay many multiples above these costs.

Importance of compliance strategy

HIPAA is often viewed as a bad word throughout the healthcare industry. However, protecting the privacy and security of PHI is something every healthcare provider should take seriously.

When developing a HIPAA compliance strategy for your office, you will need to balance the resources you allocate to compliance with your risk tolerance.


With the right strategy and advisors, you can make progress quickly and easily and prevent the ramifications of HIPAA non-compliance, a ransomware attack or a data breach. ■

PCIHIPAA is a leading cybersecurity and compliance firm. CEO Jeff Broudy leads a team of cybersecurity and compliance experts that helps protect organizations nationwide. Learn more at PCIHIPAA.com/AAOMS.




This is number 173 in a series of articles on practice management and marketing for oral and maxillofacial surgeons developed under the auspices of the Committee on Practice Management and Professional Staff Development and AAOMS staff. Practice Management Notes from 2002 to present are available online at AAOMS.org.

All articles in Practice Management Notes are published only with the consent of the authors, who have expressly warranted that their works are original and do not violate copyright or trademark laws. AAOMS is not responsible for any violations of copyright/trademark law on the part of these authors.




your
clinical
skills
your
goals
your
future



MEMBERSHIP DESIGNED FOR

Download an application at AAOMS.org/AlliedStaff and become a member today!



AAOMS Allied Staff Membership Benefits OMS Staff and the Practice

AAOMS allied staff membership has something to enhance the knowledge and skills of all professional staff members in the practice and is a bargain at only \$40*!

- Reimbursement staff have first-hand access to coding and billing advice that can reduce claim errors and shorten reimbursement time.
- Practice managers learn the latest in infection control and management strategies to help them excel in their many roles in the practice.
- Clinical staff education includes anesthesia courses, assisting skills labs and protocols for managing office emergencies.

- All AAOMS allied staff members receive direct online access to *AAOMS Today* and other important publications such as the OMS Staff Communiqué.
- Participation in the AAOMS CareerLine, the official job board of AAOMS.

Allied staff members receive discounted registration rates on the many courses and programs available through AAOMS. **More than 1,000 allied staff members are already taking advantage of the benefits of AAOMS membership. Join today!**

**Applications received Jan. 1 to Sept. 30 pay \$40 for membership through the end of the calendar year. Applications received Oct. 1 to Dec. 31 pay \$55 for membership through the following calendar year. These rates apply only to new applicants. To reinstate a lapsed membership, please contact membership@aaoms.org or call 800-822-6637.*



American Association of Oral and Maxillofacial Surgeons

Oral and maxillofacial surgeons:
The experts in face, mouth and jaw surgery*