Lessons from the COVID-19 pandemic

By Jeff Broudy
CEO, PCIHIPAA

COVID-19 caused a fundamental evaluation of how practices manage everything, including compliance. So what is your practice doing now?

During the pandemic, many practices closed or went largely remote in the initial phase and then had to return in a totally new environment.

A PCIHIPAA survey of more than 1,400 healthcare practices found the pandemic resulted in them making changes in major areas, including remote work and PPE, with a renewed emphasis on OSHA and HIPAA planning and training.

To help ensure your practice is protected, the following key areas should be addressed on an ongoing basis:

Protect employees and patients

Three components are needed to protect your staff: PPE, policies and training. Now is the time to confirm your practice is covering employees on every base. The survey found 67 percent of the practices said, "Daily OSHA guidance about COVID-19 requirements and best practices" would be helpful or very helpful, and 61 percent said OSHA training for employees relating to COVID-19 would be helpful or very helpful.

OSHA defines and enforces standards that include policies and training for worker safety. More than 900 healthcare workers have died due to the pandemic – a reminder of the importance of verifying your practice is OSHA-compliant to ensure the safety of your staff as they face the day-to-day challenges of COVID-19.

The pandemic created an enormous focus on PPE to protect employees and patients. The ensuing PPE shortage proved how essential it is to plan far in advance for worker safety. OMS healthcare providers are at one of the highest risks of exposure to COVID-19.

Step 1: Update respiratory plan, policies – Your practice must create a preparedness and response plan. The two OSHA standards most closely related to the pandemic are the Respiratory Protection Program and Aerosol Transmissible Diseases (specific to California) standards. You also must properly train employees for the increased risk of contracting certain airborne infections due to their work activities.

The consequences of not having a plan in place can be damaging. During the pandemic, an Ohio nursing facility received $40,482 in penalties from OSHA after seven employees were hospitalized for coronavirus-related reasons. OSHA cited this facility for failing to have a written respiratory protection program and not providing medical evaluations to determine employees' ability to use a respirator at work.

This unfortunate situation shows the financial impact the pandemic may have on a practice on top of the threat it poses to patients' and employees' health. Ensuring your practice has policies and procedures in place and has properly trained employees can be the difference between your employees staying healthy or contracting an aerosol-transmissible disease such as COVID-19, influenza or whooping cough. It also can protect your practice from financial liability.

Step 2: Look at OSHA compliance – Health and safety events can be a catalyst to review compliance and safety plans. Some states have their own OSHA requirements, so it is important to also review any state-specific guidelines.

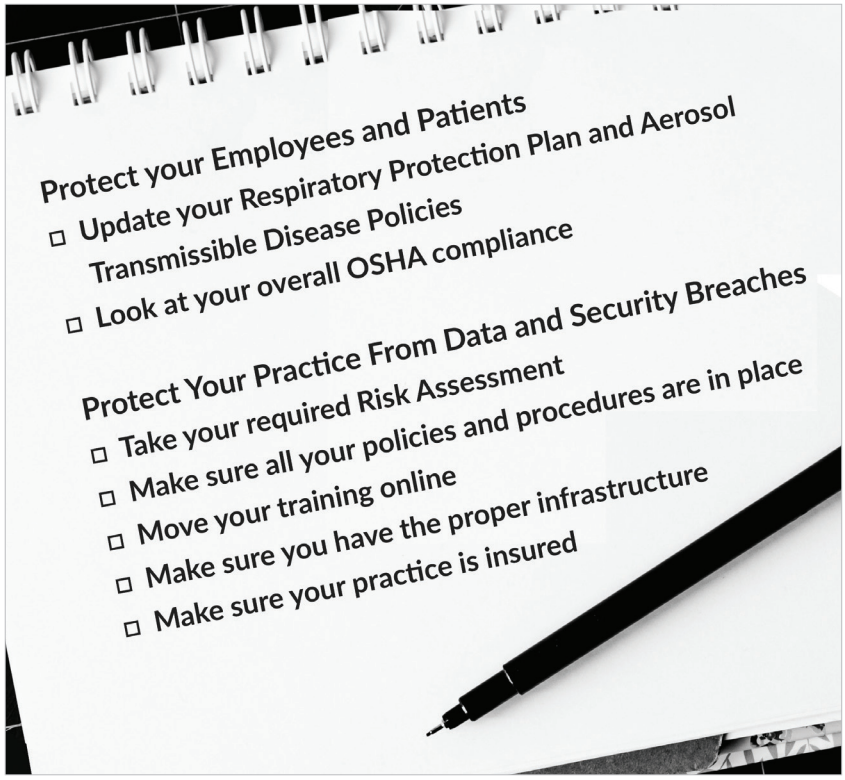
Additional steps include verifying bloodborne pathogen policies and employee training are in place. The OSHA Bloodborne Pathogens Standard could be a framework to assist in controlling some of the sources of the virus, such as exposure to body fluids.

Hazard communication also requires an exposure plan and training for employee safety and practice compliance.

An additional step for your practice's OSHA compliance is maintaining Safety Data Sheets (SDSs). OSHA requires every chemical onsite to have an SDS. Your SDSs must be in order and accessible at all times to your employees. Many practices keep a SDS binder, but the best way to ensure compliance is to use an online database that provides access to virtually all chemicals your practice might have onsite and can easily be changed and updated.

continued on next page

Protect from breaches



Hackers are constantly targeting healthcare practices, so your practice needs to be prepared for the threat of a security breach. Hackers have leveraged the panic of COVID-19 and intensified their efforts. The chance of ransomware – a type of malware that can lock you out of your computer systems and files – has increased.

HIPAA rules restrict healthcare providers from treating patients without access to their data. Providers must follow HIPAA standards and have a plan to protect against the threat of cybersecurity. Remember, a data breach also is a HIPAA violation.

Step 1: Undergo required risk assessment – As circumstances change, such as remote work, first complete federally mandated risk assessment. By completing risk assessment regularly, you will satisfy the Office for Civil Rights' (OCR) requirement and know your practice's vulnerabilities.

The risk assessment covers several areas: Are your policies and procedures updated? Are you regularly training employees? Do you have proper infrastructure to safeguard your practice from hackers? Is your practice insured in the case of a cyberbreach?

Step 2: Check all policies, procedures – Proper protection requires a plan. If your practice is hacked, it is important to have policies and procedures to organize during an already hectic time.

HIPAA outlines regulatory standards for policies and procedures that entities and business associates must develop to stay compliant. Now is the time to confirm your policies and procedures are up-to-date and your employees are aware of them.

Step 3: Move training online – Online HIPAA training is interactive and can include the added benefit of online recordkeeping, which maintains up-to-date information and stores records safely in one place.

Employee training is required to be HIPAA-compliant and essential to protect a practice. Many ransomware attacks begin by targeting uninformed users, so employees need to know how to properly detect suspicious behavior. OCR requires that employees are trained on HIPAA guidelines. Most times a practice violates HIPAA, the circumstance is made worse by improperly trained employees.

Step 4: Verify proper infrastructure – To protect your systems, you must have proper infrastructure. Working with a HIPAA-compliant managed service provider will establish a front line to safeguard your practice's information from unauthorized physical access, tampering and theft.

In the incident of a breach, your practice must have data backup updated regularly. Practices also must use encrypted email solutions to protect email content.

Step 5: Confirm practice insurance – The pandemic has cost healthcare practices enough money. Cybersecurity insurance is essential to protect your practice in the event of a cybersecurity data breach. General liability policies do not typically cover data breaches.

If a data breach occurs, HIPAA fines can cost between $100-$50,000 per incident if the practice is found to have not made a "good faith effort" toward compliance. In addition to HIPAA fines, if your practice's data are hacked, you also may

Three components are needed to protect your staff: PPE, policies and training. Now is the time to confirm your practice is covering employees on every base.

have to pay for lawsuits, ransom, lost wages, direct costs and expenses incurred.

For example, a practice subjected to a ransomware attack incurred $199,484 in legal representation, restoration and decryption of client systems, forensic investigation and the initial cost of ransom.

In the case of a data breach, your practice will not only have to deal with the financial factor but also the hassle of organizing a response. It is important to have an emergency and incident response team to help manage the process of evaluating the breach, dealing with negotiating with the hackers and getting systems back up.

Instill a safety, compliance culture

Protecting your practice is a team effort. It is essential to include your staff in all aspects of compliance and safety. Many OMS practices find the easiest way to ensure a culture of compliance is to use a blend of outside sources and experts to help protect employees, patients and practices.

The following are a few tips for protecting a practice:

- Include staff in policies and procedure discussion and planning.
- Establish formal written plans.
- Create a formal review process for any incidents that occur.
- Hold regular safety and HIPAA compliance meetings.
- Create a safety and compliance portal online.

Ensuring compliance can lighten some of the pressure the pandemic has placed on healthcare workers. Create a solid approach to protect your practice from whatever happens next. ■

PCIHIPAA is cybersecurity and compliance company that focuses exclusively on healthcare practices. It helps to prevent catastrophic losses caused by regulatory non-compliance, data breaches and human error. PCIHIPAA provides solutions to help keep protected health information private and secure and employees safe. For more information, visit PCIHIPAA.com/AAOMS.

This is number 178 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.