Cybersecurity: A necessity for oral surgeons

By Sam Munakl
Chief Executive Officer, Cytek

Healthcare has been at – or near the top – of the list of industries at greatest risk for cyber intrusions over the past two years. Cybersecurity Ventures predicts global healthcare cybersecurity spending will exceed $65 billion cumulatively from 2017 to 2021.

The oral surgery space is continuing to digitize all its information, and OMSs today are relying on more technology – including cone beams, intraoral scanners and 3D printers – to provide the best patient care.

Why OMSs?

As a result of their reliance on electronic data, OMS and dental offices have become vulnerable to cybersecurity threats. The growing volume and sophistication of cyberattacks suggest OMS practices will have to grow increasingly vigilant to ward off these threats.

A breach of cybersecurity will inevitably lead to significant expenses, both financial and reputational, which can be devastating to a practice.

Unfortunately, the mindset of many doctors is the belief that cybercriminals are not a threat to their small practice. However, many hackers specifically target small practices because they know they will be an easier target than a large bank or corporation.

Many practices have hundreds of patients, which means they are responsible for vast volumes of personal data, including names, personal addresses, dates of birth, Social Security numbers and credit card information.

All this electronic data stored on computers across a network make OMS practices a desired target for hackers who use all these data as currency and sell it on the black market.

The worst thing you can do is be uninformed about the risks and assume your office is not a target because it is a small, independent practice.

Attacks are costly

According to the latest Ponemon Institute study, the healthcare field has the highest cost per breached record of any industry: $402. That adds up to $4 million for 10,000 records.

How did they come up with this number? There is the cost of remediation/mitigation (fixing the security issues that led to the breach), the expense of notifying affected individuals and the cost of changing vendors (if the breach was caused by a business associate).

Also, most organizations offer credit and ID theft monitoring to their patients, which can run as high as $25 per month per patient. Office for Civil Rights fines and penalties, state fines and penalties, the expense of reestablishing accreditation and the soaring cost of lawsuits should not be forgotten. First-time civil monetary penalties can be as high as $50,000 per breach, while repeat violations within a year cost $1.5 million. Class-action lawsuits following a breach can be very costly to litigate or settle.

When it comes to cybersecurity and breaches, it is difficult not to mention the big impact on reputation as well. While it is difficult to quantify reputation loss from a security breach, it is safe to say most of your patients and referrals will be less inclined to trust your practice with their data in the future.

Protecting a practice

Therefore, it is crucial for OMSs to take steps to ensure their practice is in compliance with HIPAA provisions regarding computer security.

Because the majority of data security breaches occur when staff members exercise poor judgment or fail to follow office procedures, the location of computers in the practice is key.

All computers should be placed in areas where the computer screens are not visible to patients and visitors, and each computer should be protected with encrypted passwords.

continued on next page

Passwords should contain mixed-case letters and numbers or symbols and should be changed regularly. Also, passwords should not be kept under keyboards or on desks or surfaces where the public could access them. Doctors should ensure all staff members understand the importance of maintaining the privacy of patient health information.

Every practice should have a policy for safeguarding patient information and should educate staff members about how to comply with the office policy. Best practices include:

- Implement a strict internet and computer policy that prohibits staff members from checking personal email accounts or visiting internet sites that are not work-related.
- Be sure all firewalls, operating systems, hardware and software devices are up-to-date, strong and secure, and that wireless networks are shielded from public view.
- Install antivirus software and desktop encryption on every computer, and then keep it updated and checked regularly.
- Only use trusted Wi-Fi hotspots and never use shared computers when accessing office data remotely.
- Password-protect all smartphones and tablets to prevent easy access to patient information in case a device is lost or stolen.
- Shred all hard copies of documents with patient information.
- Be sure your practice is HIPAA compliant. Data transmitted to payers, health plans, labs and other healthcare providers should be encrypted to ensure a hacker will not have access to the data.
- Conduct a comprehensive risk analysis and to implement safeguards and controls gleaned from that analysis. Taking this important step can dramatically reduce the risk of a breach ever occurring – and can provide protection at a fraction of the cost associated with a breach. ■

Catch the cybersecurity webinar

As the number of cyberattacks increase dramatically, the need to secure networks has never been greater. The 90-minute webinar "Cybersecurity and Compliance" is designed to help master the core concepts of cybersecurity and HIPAA as they pertain to practices. It can be purchased at AAOMS.org/CEonDemand.

This is number 161 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.