WRITING SAMPLE

5 Unique Challenges for Dental Cybersecurity

By Gretchen Heber

Just like many small businesses, dental practices are not immune to cybercrimes. Sophisticated cyber criminals have developed numerous nefarious methods of stealing and exploiting the personal and medical of dental patients, for example, putting dentists in danger of violating the Compliance with the Health Insurance Portability and Accountability Act (HIPAA). Any violation of HIPAA could land a dentist in deep trouble with regulators and result in the loss of his or her practice.

In order to take steps to keep their practice safe, dentists should be aware of these five dental cybersecurity challenges they'll face in keeping their patients' data safe and ensuring their technology performs as expected day in and day out.

Phishing Attacks

Cybercriminals might craft phishing emails specifically targeting the dental community. Describing a new product or an upcoming conference, these emails often appear to be sent from a reputable organization. Unsuspecting office staff might click on a link in one of these emails, enter sensitive information, and unwittingly endanger the security of the firm. Other emails might have attachments that, once downloaded, compromise the office's entire network.

New Technology

If your practice is continually updating technology to offer your patients the best and most current care, keep in mind that each of these upgrades is an opportunity for a cybersecurity failure. New technology will make your business processes run more smoothly, or enable you to offer your patients a best-quality result, but, improperly installed or maintained, can also be a dental cybersecurity risk.

Patient Records

Your business systems contain sensitive patient data, including home addresses, insurance information, and payment information. Perhaps more importantly, you keep on file your patients' medical records, including information about the following:

- Chronic and acute health conditions
- Medications
- Prior surgical procedures

This is very private information that you absolutely don't want to fall into the wrong hands. In fact, a breach of this type triggers strict reporting protocols that are part of the HIPAA Breach Notification Rule. The steps that must be taken in this dental cybersecurity scenario could damage the credibility of your practice to a fatal degree, particularly if the data of minors is involved.

Ransomware

Clever hackers can use a variety of ways, including the phishing emails mentioned above, to infiltrate your systems. They encrypt your data, making it inaccessible to you and paralyzing your practice. Your business is essentially shut down unless you pay a hefty sum for the encryption key, which allows you to regain access to your applications and data.

Remote access

If your dental practice is thriving, staff may have to log in to your systems from home on occasion to catch up on work. If you do not have proper security procedures in place for this type of work, however, remote access is a dental cybersecurity risk.

All of these challenges add up to a potentially scary scenario for an unprotected dental practice. Fortunately, a qualified team of cybersecurity experts can ensure your data and applications are safeguarded against all types of attacks.