HOW MUCH WOULD A HEALTHCARE DATA BREACH COST YOUR DENTAL PRACTICE?

by Darby TechForce

As a dental professional you know all about the importance of preventative care. You tell your patients that brushing and flossing, along with routine cleanings, are the best defense against bigger and more expensive dental problems down the road. The same mentality can be applied to safeguarding your office from a healthcare data breach. Implementing technology to help protect sensitive patient information requires an investment up front, but not taking steps to thwart potential issues can result in a much pricier recovery.

What is a data breach, exactly?

A data breach is an incident where confidential data – like your patient files – is accessed in an unauthorized manner. Cyber thieves like to attack the healthcare industry because the files contain protected health information. Once they have possession, these criminals can sell your patients' names, birthdates, and social security numbers on the "darknet" – a computer network with restricted access used almost exclusively for illegal file sharing.

The scariest part about a data breach is that a person doesn't have to be a sophisticated hacker to wipe out an entire health system's network. While criminal attacks are the primary cause of data breaches in the U.S. (52 percent), system glitches and human error, such as an employee who downloads an infected email attachment, are almost equally as responsible (48 percent). Unfortunately, the costs of recovering from such a disaster extend far beyond those inevitable HIPAA fines.

The devastating costs of a healthcare data breach

According to a 2017 study sponsored by IBM Security and conducted by Ponemon Institute, data breaches cost U.S. companies an average of $225 per compromised record. The healthcare industry is hit even harder at $380 per record, making data breach costs for dentists, doctors, and other healthcare providers the highest among all surveyed sectors for the seventh year in a row. Do the math for your practice – if you dare.

On top of aggressive HIPAA fines, which often soar into the millions, there are significant costs associated with cleaning up a data breach. Dental practices are responsible for paying for reporting information to the media, notifying the U.S. Department of Health & Human Services (HHS), conducting a forensic investigation, and setting up credit monitoring services for affected patients. To make matters worse, a healthcare data breach may invite a single-person or class action lawsuit, which makes for an even more costly recovery.

While the direct costs of a data breach are devastating, the indirect costs represent a significant part of a dental practice's total loss. Unfortunately, these elusive expenses linger long after the investigation, lawsuits, and fines have ended – and the impact is severe. Ponemon Institute states that lost revenue and brand value make up an estimated 40 percent of the total cost of a data breach.

How to protect your practice from a data breach

There's no question that dentists need to take measures to protect their practices from costly data breaches. Organizations with chief information security officers, or a team of dental IT experts, are best equipped to detect attacks as fast as possible and respond. In addition to data loss prevention (DLP), including server monitoring, offsite data backup, and a disaster recovery plan, dental practices should consider firewall security, workstation monitoring, virus protection, and data encryption to further protect patient information. Practices can add an additional layer of protection by running security risk assessments once or (ideally) twice a year.

DLP solutions, along with regular employee training on security policies and procedures, have been shown to decrease data breach costs by more than $9 per compromised record. A dental practice's due diligence to employ cyber security measures is becoming increasingly important as connected devices become more common, but it can be difficult to take on such a big task if you're already struggling to keep up. That's where we come in.

We protect you, so you can protect your patients

As a healthcare provider, you never want to send your patients an apology letter informing them that their personal health information has been compromised. Not only is recovery from a data breach really expensive, breaking your patients' trust can seriously damage your practice's reputation. That's why it's so important to have data loss prevention solutions in place from the start.

At Darby TechForce, we have 20 years of experience in dental IT integration and security compliance. And we specialize in dental technology, which means we have a clear understanding of HIPAA compliance and the security issues your practice faces every day. Whether you're looking for someone to handle all of your technology needs or to supplement the work of your existing IT team, our services can be tailored to your exact specifications. From 24/7 server monitoring, maintenance, and AntiVirus protection to off-site data backup and rapid recovery, we build a secure perimeter around your data to make sure your patients' information and your dental practice are safe.

Ready to learn more? Give us a call to chat with one of our friendly tech experts at 800-886-2093.