HOW THE CLOUD HELPS YOU COMPLY WITH THE HIPAA SECURITY RULE

BY LORNE LAVINE, DMD

As many dentists are aware, there are federal guidelines that control the privacy of patient information and security of that information in the dental office. These are all part of HIPAA. The HIPAA Security Rule states that any entity that creates, receives, maintains, and transmits protected health information (PHI) is required to ensure confidentiality, integrity, availability of the data, protect against reasonably anticipated threats to the security of the data, protect against reasonably anticipated and unauthorized uses or disclosures of the data, and ensure compliance by its workforce. Of course, for many dental practices using standard practice management software, this can be a real challenge at best.

The unfortunate reality is that many practices are unaware of the current HIPAA regulations (and its cousin, the HITECH Act), but they would probably take heed if they knew about the potential fines. First-time offenders can be charged up to $50,000, and if found guilty of “willful neglect,” the fines can go as high as $1.5 million. Obviously, doing everything we can to take the necessary steps toward compliance is critical.

A new type of dental software, though, which is web-based and often referred to as cloud computing, can make HIPAA compliance much easier. There are many advantages of the cloud when it comes to specific areas of the HIPAA regulations. Some are listed here:

- **PHYSICAL SECURITY** — The typical dental practice does not physically secure the server. Anybody can touch it, kick it, or walk away with it (which is very likely to happen in the event of a theft). And, of course, fire and flood are no friends of a server. With the cloud, the data is physically protected by such measures as perimeter fencing, biometric access controls, video surveillance, and professional security management. These companies take data security very seriously; these are not a bunch of servers sitting in someone’s garage!

- **ELECTRONIC SECURITY** — The typical dental practice relies on consumer-grade firewalls and routers, such as Linksys or D-Link. Any nerdy high school student is capable of hacking these measures within five to 10 minutes. While there are better firewalls such as those made by SonicWALL and ZyXEL, they are still not 100% bulletproof, especially since many dental practices have open ports to allow for remote access software. With the cloud, data centers employ world-class firewalls and intrusion detection systems. It’s simply not pragmatic for the typical dental practice to invest in the same caliber of equipment and security measures employed by a professional data center.

- **BACKUP INTEGRITY** — Most practices back up their data, but by some accounts, less than half will be able to restore their data due to corrupted data or not backing up the right data. In many cases, the backup is not physically removed from the practice, and backup disks removed by a team member are not secured. And, a more pressing issue is the one of disaster recovery — having a good copy of your data doesn’t get you back up and running until there’s a new server and all programs are reinstalled, which is often a multiday process. However, with the cloud, data at a professional data center is mirrored by multiple servers, in multiple locations — you basically have a backup of the backup. Data is typically no more than two hours old at any given restore point.

- **EMERGENCY AVAILABILITY** — In the event of a local disaster, HIPAA requires the PHI must still be available for retrieval, which means not only having a copy of the data but also having a way to set up the data for retrieval, which can be expensive and time consuming. The dental practice must have immediate access to server/hardware, be able to install necessary software, and be able to restore data, not an easy feat. With the cloud, all you need is a computer with Internet access and a browser.

- **IT MANAGEMENT** — For a practice using client-server software, because the PHI resides in the office, the burden of backup, disaster recovery, security, and documentation rests on the shoulders of the doctor. With the cloud, doctors eliminate nearly all of the IT management headaches associated with managing PHI.

Client-server systems represent a huge compliance risk to the typical practice. With web-based software, though, the cloud helps the typical practice become and remain compliant with the HIPAA Security Rule. DE

Readers may request a comparison of how cloud-based and client-server applications assist the doctor in meeting every HIPAA Security Rule requirements by sending a request to info@curvedental.com.

LORNE LAVINE, DMD, practiced periodontics and implant dentistry for more than 10 years. He is an A+ certified computer technician, as well as Network+ certified. He is the president of Dental Technology Consultants, a company that assists dentists in all phases of technology integration in the dental practice. He can be reached at dlavine@thedigitaldentist.com or by phone at (866) 204-3398. Visit his website at www.thedigitaldentist.com.