

Data Security in the Dental Office

By David C. Post, Managed Backup Solutions and Data Security (MBS)

In the last ten years, computer use in dentistry has moved beyond accounting, billing, charting, treatment plans, and scheduling. With the advancements in processor speeds, it's now possible to add digital x-rays and photos. Many practices utilize patient-education software and marketing material to help educate patients about various new treatment techniques and high-tech diagnostics, like digital shades or periodontal probing. With these exciting new advancements come greater responsibilities to protect your data.

After working in IT and data-security related areas in the dental industry for more than 15 years, I've identified three major areas of concern:

1. Server and workstation hardware and OS (operating system) security
2. HIPAA-compliant backup solutions
3. Direct internet connections

Following are a few scenarios related to these areas of concern that will help you understand the importance of data security.

Server and Workstation Hardware and OS (Operating System) Security

Pressured by financial difficulties, an employee has made a deal to sell electronic health records for 75 cents each. Using a USB thumb drive, she begins a download. She wants all the records, but 15 minutes later, time is running out and she's only able to get half the records. Darn computer is running slow; need to get the doctor to call the IT guy on Monday.

With little risk of going to jail, the employee has pulled off the perfect heist with nothing more than a thumb drive purchased at Wal-Mart, and gets paid \$2,000. Months later, the data breach will be discovered by the fraud investigator, and will tie the ID thefts to the dental office. Channel 11 will interview the angry former patients, and it will be assumed that the doctor's computer was hacked because there is no trail. No one will be specifically blamed, but the incident will bankrupt the once thriving dental practice; all for just \$2,000.

Hardware and OS security problems begin with one central issue: passwords. Whether you're running a domain or workgroup environment, or a single computer, inadequate strength and permissions surrounding the password can make you more susceptible to security breaches. To simplify this process, many practices are moving to biometric devices that can be set up to recognize the user by fingerprint, and immediately login that person with the proper permissions.

Lock down your computers to ward off data theft. USB, floppy drives, and CD/DVD drives should be disabled to all but the office manager, doctor, or system administrator. If an intruder can't get into the computer, he can't do anything to it. Your computers are the key to maintaining a safe and profitable practice, and should be protected at all costs. Microsoft, to its credit, has developed many new tools and applications which are available to Windows genuine software owners to virtually lock down the server or workstation from any and all malicious activity—both internal and external.

HIPAA-Compliant Backup Solutions

The call wakes you at 2:30 A.M. It's your security service, saying there's been a break-in at your office, and the police are on its way. Your first thought is, "all my computers!" You arrive, and the police officer says, "It looks like they just took the computers, and not the monitors." Great, my server was under that front counter. Two days later, your computer guy is replacing the computers covered by the insurance company, and he asks for your latest backup. Well, you know how this story ends.

Following are questions to ask yourself to determine if your current backup solution is compliant:

1. Are my backups regular? (Once a day is suggested.)
2. Do I test for restorability? (Once a week is suggested.)
3. Is my backup in an encrypted state? (With at least bank-level security, AES 256?)
4. Is my backup removed from location daily?
5. Is my backup copy located in a safe and secure location?

With all the new technology surrounding good backup solutions, this should be the easiest data security measure to deal with, but it always seems to be the most ignored. I'm a strong proponent of Internet offsite backups, because of its very nature. Creditable offsite backup companies will house your data in two, geographically-different, secure locations, maintain redundant fail-safe systems, keep it in encrypted state at all times, and ensure its restorability 24/7/365.

Direct Internet Connections

You're looking at your computer screen, and the mouse pointer is moving, but you're not touching it. You open Microsoft Internet Explorer, and 50 windows open asking you to buy magazine subscriptions. Your system is so slow that you can't get your day's schedule to come up. What's up? You've probably been hacked!

Looking back to 1979, the year I started using the Internet, I remember thinking this was going to be the greatest technological event of the decade; and I was right. But what didn't dawn on me at the time was the dark side that was to follow this great new age of information and convenience. To my dismay, over the years, I've spent too many hours reloading, rebuilding, scanning and throwing computers in the garbage because of viruses, Trojans, and worms that have destroyed my home and business computers. Direct connection to the Internet—either through a server or directly to the workstation—is the greatest risk to your entire office network. So where does that leave us? If you must have the Internet, here are some basic guidelines that will help you protect your computers and data.

Keep your Firewall Turned On.

A firewall helps to protect your computer from hackers who might try to delete information, crash your computer, or even steal your passwords or patient information from your practice management software program. When someone on the Internet or on a network tries to connect to your computer, we call that attempt an "unsolicited request." When your computer gets an unsolicited request, Windows Firewall blocks the connection.

Keep your Operating System Up-to-date.

High-priority updates are critical to the security and reliability of your computer and data. They offer the latest protection against malicious online activities. Microsoft provides new updates, as necessary, on the second Tuesday of the month. The Windows Update service provides a single location for all the updates for your

Windows XP and Vista-based PC. Automatic Updates routinely checks for the latest high-priority updates for your PC; then downloads and installs them for you automatically.

Use Updated Antivirus Software.

Antivirus software detects, prevents, and takes action to disarm or remove malicious software programs, such as viruses and worms. Computer viruses are software programs that are deliberately designed to interfere with computer operation, record, corrupt, or delete data, or spread themselves to other computers in your office network and throughout the Internet. When considering an antivirus software program, make sure it updates automatically on a regular basis to help prevent the most current viruses.

Use Updated Anti-Spyware Technology.

Anti-spyware helps protect your computer against pop-ups, slow performance, and security threats caused by spyware and other unwanted software. Spyware collects and relays personal information, or changes the configuration of your computer, without appropriately obtaining your consent first.

Technological advancements in the dental-care industry have created many new security challenges in assuring the confidentiality, integrity and availability of electronic protected health information (ePHI). By securing your computers, maintaining a good backup strategy, and controlling Internet usage, you can protect your most valuable practice asset: your data.

MBS is a TDA Perks Program partner, and a Texas-based company with more than 15 years of experience dedicated exclusively to the dental industry. As data security experts knowledgeable in all the major practice management software packages, the management team at MBS has more than a decade of experience in managing large-scale technology implementations and data security solutions at Fortune 50 companies. For more information regarding MBS's services, contact David Post, TDA Perks Program's MBS representative, at (877) MBS-0787. For more information regarding other TDA Perks Programs, visit tdaperks.com, or call (512) 443-3675.