



The Security of Web-based Systems

Reasonable doubt exists and some have questioned the security of web-based dental systems when compared with legacy, office-based, client/server based systems. While the question is reasonable, the answer is very clear. Web-based systems have the capability of providing substantially greater security than any on-site, client/server based system.

While web-based systems have the capability, that on its own does not ensure that all web-based systems meet the requirements for world class security.

This paper will discuss the importance of data security in the dental environment. It will also explore and address several key points associated with the high level of security required of protected personal health information. Comparisons will be made to other markets where valuable assets are protected by third parties in a similar fashion as web-based dental systems.

Importance of data security in a dental environment

The security of Dental Records should not be brushed aside. A lax or haphazard approach to the protection of personal health information in a Dental Practice can result in patient dissatisfaction at the least and some combination of financial and social ruin at its worst.

There are many potential problems associated with the typical security in most modern dental software systems. They include:

Unauthorized release of personal and legally protected health data. Imagine if you had a well known patient (perhaps a local businessperson of prominence or a city council or school board member, perhaps an entertainer or other person) and that patient's HIV

positive status, or some other personal data were released to the public by an unauthorized source originating in your office. That type of disclosure could cost you your practice and your reputation.

Theft of valuable technology. Consider what the high priority items are that a burglar might seek to steal in your office. The first thing on their mind is not your schedule book, but that is just what they will get when they take the computer server that is running your practice. In addition to the potential of unauthorized release of data, a theft can result in complete chaos in a practice.

Lost productivity while systems are being restored. How long will it take before you can have a system up and running again? What production will you lose as you purchase the replacement hardware and then configure the system and then try and restore your last backup? Think back to when you installed your system for an idea of the cost of the equipment. Now add the lost production and you are well into strong five figures.

HIPAA. Though prosecutions for HIPAA violations are not widespread, the law still permits prosecution. Care should be taken to ensure an office is in compliance with these federal requirements. Most client/server based systems are inherently at a disadvantage and fall short by providing between 4 and 6 of the 19 mandated HIPAA physical and technical security requirements, while web-based companies have the capability of providing all 19 of the same requirements. Unfortunately, it's not the software company's obligation to comply, it's your obligation. The more that your software vendor can provide for you, the less you have to do for yourself. There is a cost in both time and dollars when you are left to fulfill the requirements that your vendor is unable to assist with.

Software Updates. Software needs to be maintained and updated to remain secure. With client/server systems, this requires a manual process that frequently results in disruption to the office or sometimes needed reconfiguration of servers and drivers.

Finally, there is the simple peace of mind when you have confidence in the security of the core business tool used in your practice.

Risk associated with a typical dental installation

Let's consider the typical dental office setup for client/server based dental software system.

First, there is a file server - typically located either in a "broom closet" or under a desk somewhere. Access to that server is available to most anyone in the practice and definitely to anyone who might break in. Expensive technology products are among the first to be stolen in an office break-in. Also, disgruntled or careless staff can put the data at risk.

Next, the database is usually directly addressable by anyone on the network. In other words, someone could easily come in, and using simple "drag and drop", copy the entire office database onto a removable media like a CDROM or thumb drive. No record of that copy would ever be made and there is no accountability for that stolen information.

Software updates are typically a manual process where staff are required to install updates from a CDROM onto each workstation in the office. There is not usually any automated or certification process that ensures that these upgrades actually happen. It is not uncommon to require the assistance and expense of an outside IT professional to install the update and correct any needed or sometimes unintentional changes that may have occurred to the network or workstation setup.

Office based client/server based systems require constant vigilance and maintenance of virus protection software.

Backup processes at most dental offices are manual processes that do not require validation of the backup medium. Basically, someone has to remember to backup the data. If they forget or are in a rush, the backup doesn't happen. Validation of the backup is typically overlooked in most dental office settings.

This validation is needed to ensure that the required files are indeed being backed up.

Many studies have been done that show between 40 - 60% of backups are bad. Some reasons for backup failure include backup scripts that address the wrong files, scripts that backup some but not all necessary files, and backup media that have flaws. Each of these will make a restoration impossible. This last point is particularly true of portable magnetic media (like backup tapes) that is used multiple times. Also, scratched digital media can cause restore failures. The result is that a large percentage of offices that feel secure regarding the quality of their backups, are actually walking time bombs of system failure.

Finally, the backup media may be taken off-site. Though having backup media taken off-site may provide an incremental level of redundancy, it does introduce a security nightmare if not done professionally. What is the typical security of the off-site location? Commonly it is a nightstand or home office desk - perhaps simply an office manager's purse. It may provide for off-site storage, but the security of it is of dubious quality.

Quality Web-based systems reduce risk

Now, consider a quality architected web-based solution. The data does not reside in the office. Instead, the data is located in multiple tier-4 secure facilities designed specifically for storage, maintenance and security of important electronic data. These facilities cost millions of dollars to build and substantial resources to maintain. Though the office staff access information through office based computers, there is no patient data on any computer in the dental office - it all resides at the redundant hosting facilities with several layers of security and backup.

Security systems include both physical and logical security. Some of the industry's most sophisticated physical safeguards are implemented including restrictions only to authorized persons verified by a combination of physical pass keys, digital fingerprint scans, likeness matching on photo ID badges, and in some cases retinal scans and other recognition technologies. The locations are not published to reduce the ease in identifying the location as a data warehouse. Ultra secure bulletproof doors and walls restrict forced entry and multiple layers of locked access points, using various types of mechanisms, make

simple lock picking extremely unlikely. These facilities are guarded by armed officers on a 24/7/365 basis. Also, these facilities implement the best and most expensive software and hardware “firewalls” protecting access to data from un-authorized hackers. The systems are virtually virus proof and are built and managed by the industry’s best and brightest software security professionals.

Additionally, the software is updated on a regular schedule to all users without user intervention. No office time is spent in this process and no outside technical staff is needed to be employed in the process. This automatic process ensures currency of the application and a certainty that the latest enhancements and fixes are implemented the same day they are available.

This overall security plan is well beyond any dental office in type, scope, depth, function, and expense. You just can’t purchase it any other way.

Redundant systems hold office information so that if any individual computer component breaks, another is ready to pick up where the one left off, without losing any data. Full redundancy provides significant protection against data loss and improves the security of access. Additionally, redundant physical facilities add the ultimate layer of access confidence. Basically, your data will be in two separate locations in separate geographical regions, both of which are capable of providing full access and service. All data is recorded back to both locations simultaneously. Then, a separate backup is created every hour of every day. This is not a volatile backup tape or flimsy CD. It is a full disk to disk backup that is electronically taken to a third secure location just in case the unimaginable happens and a restore becomes necessary. A history of these backups is kept. Each backup is validated against the source data to ensure that it is a perfect copy, ready to be used at a moment’s notice. Most quality hosted solutions have never had to resort to this final backup level, but it’s there just in case.

With this background, it is relatively easy to understand how a professionally managed web-based solution is easily several orders of magnitude more secure than an office-based client/server system.

Other markets have adopted web-based technologies

Though the Dental industry is just beginning to adopt these mature web-based technologies, other industries have had widespread adoption for many years, and in some case almost complete domination of web-based solutions.

The fastest growing medical office management system in the United States is a web-based product that was introduced to the industry in 1999. It has better than 99.95% uptime from inception and supports a broad spectrum of medical specialties across every state of the Union. The sales force automation and CRM industries have many web-based systems and sports one of the largest and fastest growing public companies. As a web-based product, Salesforce.com has become a venerable competitor in many industries that require sales tracking.

Virtually every bank in the world has adopted web-based technologies and offers on-line banking to every banking patron. Consider that every dollar in every bank account, including savings, checking, retirement accounts, etc. throughout the world, are all on-line and available for transactions through web-based products. Security is an absolute must, and is best delivered through web-based technologies.

On top of these core business applications, the industry is chock full of consumer directed web-based products. Consider eBay, Google Earth/maps, PayPal, e-Trade, and thousands of ecommerce web sites. It is actually hard to find an industry that does not have a significant, if not dominant web-based product offering. Though lagging other industries, web-based solutions are now being offered to the dental industry as well.

Analogies

Consider your retirement account. You work hard, save and invest. Do you keep your savings at home, in a nightstand or under your mattress? Would you feel more or less secure having your accumulated wealth on-line with a bank or physically in your home? The answer is painfully obvious – it’s most secure in a bank. Why? Because a bank spends the required resources to secure it. They purchase really big safes with very substantial locks (the type you just can’t pick very easily). Banks also institute best practices and appropriate processes to ensure data safety

and security. Hired staff have background checks and are trained professionals specializing in banking security. It is just not possible to have the same type of security at home . . . so you use a bank.

Does putting your money in the bank make it less accessible? No, quite the contrary. It is more accessible with a bank. You can access it using a check, debit card, wire transfer, or an ATM if you like. You don't need to have the cash in your wallet to use it. That reduces the risk of loss from theft or carelessness. The same is true of web-based systems and your data. It is more accessible and more secure at the same time.

Conclusion

The last 10 years of web-based technology development and infrastructure have created a more secure and available solution for storage, backup, and access of data than is possible with legacy client/server systems. A well architected and maintained web-based dental software system is inherently more secure than any office-based client/server system.

About Curve Dental

Curve Dental is a dental software company that delivers practice management solutions via the web. Our customers can schedule, invoice, manage recall, manage insurance, chart, and much more using only a browser and Internet connection. If you can bank, shop and book a vacation on-line, why can't you manage your practice on-line? When it comes to web-based dental software, Curve Dental leads the way with simple technology and impeccable customer service. For more information visit www.curvedental.com or call 1-888-910-4376.

©2009 Curve Dental, Inc.