curve DENTAL® ORANGE PAPER

The Security of Cloud-based Systems

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

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

This paper addresses the importance of data security in the dental environment. It also explores and addresses several key points associated with the high level of security required of protected personal health information.

The importance of data security in the dental environment

The importance of secure dental records should not be minimized. A lax or haphazard approach to protecting personal health information in a dental practice can put the business at risk.

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

1. Unauthorized release of personal and legally protected health data

Imagine if you had a well known patient (perhaps a prominent local businessperson or a city council member), who'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.

2. Theft of valuable technology

Burglars look for big ticket items--typically computers, servers and other electronics. Imagine the impact of unauthorized release of data to compound the chaos a break-in can have on your practice.

3. 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, configure the system and then try and restore your last backup? Think back to when you installed your system to estimate the cost of the equipment. Now add the lost production and you are well into five figures.

The importance of data security in the dental environment (continued)

4. HIPAA

Though prosecutions for HIPAA violations are not widespread, the law still permits legal action. Care should be taken to ensure the dental 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 cloud-based companies have the capability of providing all 19 of the same requirements. Unfortunately, it's not the software company's obligation to comply. This rests on your shoulders. The more that your software partner 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 cannot meet.

5. 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 needs 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.

First, there is a file server - typically located in a closet or under a desk somewhere. Access to that server is available to most anyone in the practice including burglars! 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 accessible 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 removable media like a CD-ROM or thumb drive. No record of that copy would ever be made and there is no accountability for that stolen information.

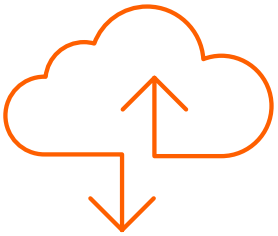
Software updates are typically a manual process where staff must install them from a CD-ROM onto each workstation in the office. There is not usually any automated or certification process that ensures that these upgrades actually happen. It is not uncommon to require the assistance and added expense 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.

Risk associated with a typical dental installation (continued)

There are myriad ways to back up data and cloud-based options have become increasingly popular. But this comes at an additional cost for traditional server-based solutions, while Curve, for example, includes it with our monthly subscription. If you do choose an off-site option, it introduces a security nightmare if not done professionally. What is the typical security of the off-site location? Does it offer the level of security that lets you sleep well at night?

Quality cloud-based systems reduce risk



Now, consider a quality architected cloud-based solution. The data does not reside in the office. Instead, it's 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 accesses 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.

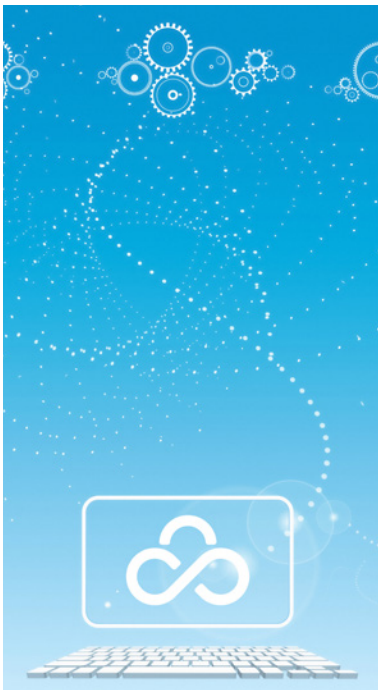
Security systems include both physical and logical security. Some of the industry's most sophisticated physical safeguards are implemented including restrictions only to authorized persons verified by a combination of physical pass keys, digital fingerprint scans, likeness matching on photo ID badges, and in some cases retinal scans and other recognition technologies. The locations are not published to reduce the ease in identifying the facility as a data warehouse. Also, these facilities implement software and hardware "firewalls" protecting access to data from unauthorized 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 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 update ensures 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 store 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. All data is recorded back to both locations simultaneously. Then, a separate backup is created every hour of every day; 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.

Other industries have adopted cloud-based technologies



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

The fastest growing medical office management system in the United States is a cloud-based product that was introduced in 1999. It has better than 99.95% uptime from inception and supports a broad spectrum of medical specialties across the country.

Virtually every bank in the world has adopted cloud-based technologies and offers online service to all customers. Consider that every dollar in every bank account is online and available for transactions through cloud-based products. Security is an absolute must, and is best delivered through cloud-based technologies.

Curve Dental customers have the peace of mind knowing that their data is automatically backed-up, saved and stored professionally in a top-tier Amazon Web Services (AWS) data center. They've embraced the benefits of Curve's cloud-based dental practice management software and the security of knowing that their data is both safe and accessible from any device with an internet connection.

About Curve Dental

Founded in 2004, Curve Dental provides cloud-based dental software and related services to dental practices within the United States and Canada. The company is privately held, with offices in Provo, Utah, and Calgary, Alberta. The company strives to make dental software less about computers and more about user experience. Their creative thinking can be seen in the design of their software, that's easy to use and built only for the web.

curve DENTAL®

Visit us at www.curvedental.com