axiUm Ascend

Keeping Patient Information Safe and Secure in the cloud

Take Cover

The costs of exposing or losing patient information can ruin a dental organization. Cloud-based solutions offer protection for your business and your patients against these threats:

- Unauthorized release
- Lost productivity
- Backup failures
- Virus and malware infection

As every part of our world becomes more digitized, privacy is becoming an even bigger hot-button issue for all types of organizations, including dental institutions. Consumers hold the businesses with which they share personal information to the highest security standards and react negatively when that trust is broken. When it comes to dental health records, no organization can afford the risk of losing the trust and confidence of patients or facing the legal and financial costs that can come with a security breach. It's no wonder, then, that for modern dental clinics, safeguarding patient privacy comes second in importance only to providing high quality patient care.

With the stakes set so high, it's natural for dental organizations considering the possibility of moving to a cloud-based practice management solution to ask, "How secure is my patient information?" The question makes perfect sense to ask. The answer is that connecting to your EHR (Electronic Health Record) solution over the Internet rather than relying on a private on premise system can provide the security you desire while maximizing the flexibility and efficiency that web-based solutions can offer.

To see how cloud-based solutions can actually improve the security of your patients' private health information, it's important to take a step back and consider the nuts and bolts of cloud computing.

Anatomy of a Cloud-Based Solution

“The Cloud” is a popular buzzword these days, but as with any new technology trend, there’s still some confusion about exactly what it all means. At the most basic level, cloud computing simply means moving the computing resources your organization depends on from your own local servers to professionally managed offsite server farms that you access through a secure connection on the Internet

This approach transforms the software you use every day from something you purchase, install and maintain on your own machines into a service you access securely over the Internet—through a browser. This type of web-based solution is also commonly referred to as “Software as a Service” or “SaaS.”

All Internet Security Is not Created Equal

Sometimes the Internet may get a less than stellar reputation for protecting privacy and maintaining security—largely due to a few highly publicized security breaches of popular websites. But in most cases, this lack of confidence is misplaced. Cloud solutions can offer more advanced, enterprise-level security capabilities than a typical on-premise system. Of course, potential and reality are two very different things, so it’s important to understand the security capabilities and reputation of every cloud solution you consider using—especially when it’s something as important as your dental organization's EHR system.

Finding World-Class Security in the Cloud

Security is serious business any time you’re dealing with sensitive health care information. A small breach can cause embarrassment and angry patients. Larger problems can lead to serious legal consequences, fines and other regulatory actions. Unauthorized releases of private information, physical and virtual theft, and loss through system failures or viruses all threaten the well being of your institution. Technology allows cloud-based solutions to protect both your patients and your organization by tapping into environments that provide high levels of security technology and expertise.

"Security is perceived as an inhibitor of cloud, but it can also be viewed as an enabler."

~Neil Readshaw, the lead architect for IBM's cloud security

Keep Confidences

Your dental organization has an ethical and legal responsibility to keep patient information private unless a patient authorizes its release. Right now, your patients' financial and health care records may be kept on a server that's under someone's desk or in a back closet. Though it might feel safer to have your data stored in-house than in the cloud, this client-server model means you're probably storing a lot of sensitive data on unsecured servers, laptops and other devices, which actually makes it more vulnerable. For example, a lost or stolen laptop could lead directly to a major security breach if it falls into the wrong hands.

Access control is another major issue. When everyone in your organization can access all of the data on any machine in your office, that information is extremely susceptible to unauthorized release—through carelessness, innocent over-sharing or even deliberate actions by disgruntled employees.

Meet Your Full-Time Security Team

Who monitors your data on nights, weekends and holidays? Chances are, the answer is no one. But with cloud-based solutions all of your electronic records are always housed in state-of-the-art data centers created specifically to store sensitive electronic data. These advanced facilities put multiple layers of protection measures in place.

Restrictions Apply

With cloud-based solutions, sensitive information is not stored permanently on your PCs or other devices in your office. Your data is always available from any machine with an Internet connection, but that sensitive information remains protected by security measures. Cloud-based dental software also allows you to specify which members of your institution can access different types of information. This type of control makes it easy to safeguard sensitive data from the risks of overcurious or malicious employees who may be tempted to look at or take information they shouldn't. With cloud-based solutions, your first step is to verify your identity. That isn't the case with server-based solutions.

What about Hackers?

If all of your patient data is stored at an offsite data center and accessed over an Internet connection, does it make you more vulnerable to attacks from hackers? The truth is that hackers are equal opportunity criminals who target the weakest systems they can find—whether they're located in your office or in the cloud. A recent study showed that the most significant patient data security breaches were actually caused by physical theft of hard drives and paper records. Hacking was only responsible for six percent of the incidents. With reputable cloud-based services, the risk is reduced, because you're placing your data in the hands of world-class security professionals who specialize in designing sophisticated, multilayered firewalls and other advanced protection to keep the hackers out. Most dental organizations—even large ones—simply don't have the resources or expertise to maintain that same proactive vigilance.

Turning Major Disaster into Minor Inconvenience

There's simply no way around the fact that the PCs and other computing devices in your organization will fail from time to time, whether the cause is a bad hard drive or a spilled cup of coffee on a laptop keyboard. But when your EHR solution is cloud-based, these inevitable breakdowns become a minor inconvenience, because your data and software engine are kept at business-class data centers and immediately accessible on replacement equipment. When one of your machines breaks you can simply grab any replacement machine with a web browser, log in and keep working.

Does Your Backup Have Your Back?

Studies show that as many as 40-60 percent of backups are not properly conducted, which results in data that is ultimately unrecoverable.

Backup to Forward Thinking

How do you know your backup is working? Most organizations recognize that creating regular, reliable backups is an essential part of keeping their important information safe. Unfortunately, too many dental institutions rely on manual or incomplete backup processes that are fraught with potential failures, including things like forgetting to perform backups at scheduled times, using low-quality media with high failure rates and storing backup tapes or disks in locations where they can get lost or damaged. In addition, with no dedicated IT department to manage backups, this critical and time consuming task often falls to an office manager or some other member of your staff with little or no IT experience. As a result, some organizations are unable to restore their lost data 40-60 percent of the time. Even worse, without a process to check and validate backups, you may not even realize there's a problem with your backups until it's too late.

Tap into a Complete, Redundant Backup Architecture

With cloud-based solutions, all of the usual backup and recovery issues and headaches disappear. Every server, hard drive and other major hardware component in the data center is backed up immediately, so your information is always complete and up-to-date. You should research solution providers to ensure your data is always stored in two completely different locations in separate geographic zones, so you don't have to worry about a natural disaster destroying both your primary system and your backups. Backups are monitored and validated by a staff of IT professionals, so there's never a question about whether you can recover your information when you need it. As a result, there is always a backed-up copy of all your latest data ready to take over the instant something goes wrong. And thanks to sophisticated high-availability software, the switch from a primary system to a backup system happens automatically and nearly instantaneously. That means even if a hard drive goes bad or a server fails in the data center, your EHR system stays up and running without disruptions.

Your Data Can't Afford a Sick Day

Today, malware is a constant distraction and ever-present threat. One missed software or antivirus update on your server can lead directly to productivity losses and downtime for your entire dental organization. But once again, a cloud-based solution can minimize the risks of malware, because your core EHR system and all your data are consistently monitored by security experts and protected by the very latest anti-malware technology. This creates a level of security against malware that's difficult to duplicate with typical on premise systems and networks.

Learning from other Industries

Although it's just now emerging as a viable option in the dental industry, cloud-based computing impacts the lives of virtually everyone who uses a computer. Most people don't think twice about shopping on an e-commerce site or using Google Maps to pinpoint their location and get directions. And millions of people trust their most sensitive financial information to PayPal or other online banking services every day. We also send private correspondence via email through Yahoo and Gmail, which store all kinds of personal information in the cloud. And while the dental industry has lagged behind a bit, millions of medical records have been stored on cloud-based systems since the 90s.

When it comes to evaluating the safety of cloud- and Internet-based services, it's helpful to look at the experiences of other industries. For example, nearly every dollar in every bank around the world is available through online banking. In these cases, security is obviously paramount, and we have become comfortable that even the most sensitive financial and personal information can be sent over the Internet safely and securely. With cloud-based EHR solutions your dental organization can experience the benefits of cloud-based access and availability other industries have enjoyed for years. And as these other industries have shown, storing sensitive information on cloud-based systems and accessing it over secure Internet connections—if it's done carefully and correctly—is a safe and proven model.

How Much Will You Pay for Peace of Mind?

Your dental institution relies on highly personal and private data, which is vulnerable to malicious and overt threats such as theft and malware as well as loss through accidents and human error. With the development of cloud-based software solutions and the availability of axiUm Ascend, you now have a much less expensive alternative for managing and eliminating these serious threats. With axiUm Ascend, you can enjoy the confidence of knowing that the personal data that lies at the heart of your organization is housed in a state-of-the-art data center, protected by business class security structures and technology, and monitored and maintained constantly by a team of security experts—all for an affordable monthly fee.

axiUm Ascend

axiUm Ascend, the new cloud-based practice management system from Henry Schein, protects your data with multiple security measures. But it's more than protection. axiUm Ascend also delivers the advanced EHR management capabilities you need—all built around a convenient, well-organized overview screen that places the focus on your patients. With Ascend, all of the clinical, front office and patient management capabilities your organization needs are available for one monthly price—with no expensive add-ons, extras or additional fees to worry about.

For more information on how axiUm Ascend can protect your sensitive data records from theft and loss, visit www.exansoftware.com/ascend

HENRY SCHEIN®