



HIPAA and Beyond

Overview

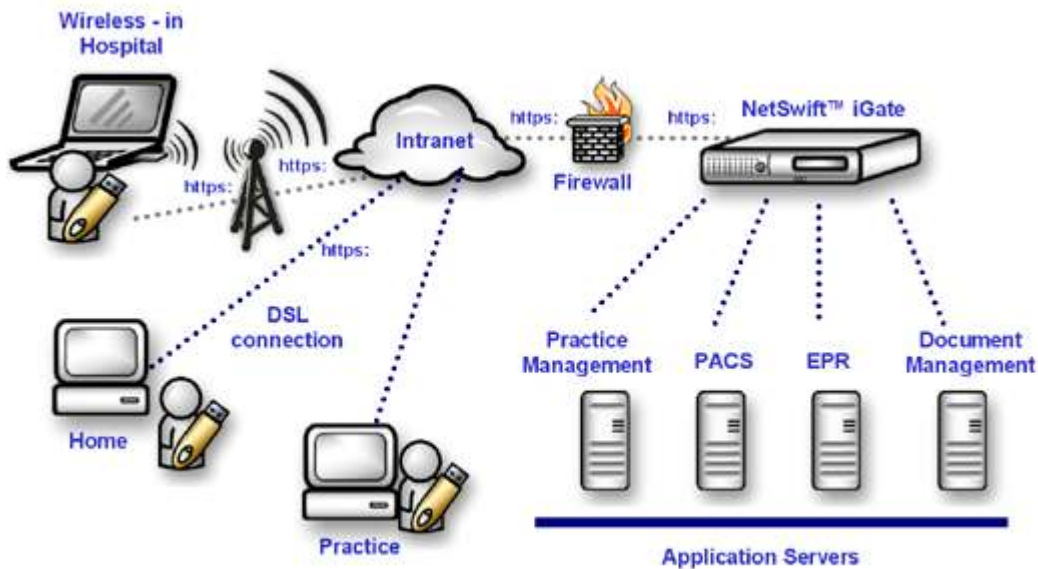
One of the biggest challenges that the healthcare industry face today is improving patient care with new technologies while maintaining patient confidentiality, streamlining operations, and reducing costs. As more industries need to remotely access their applications to improve efficiencies, the healthcare industry is finally following suit and looking at secure remote access solutions as well. A rapidly increasing number of healthcare professionals are beginning to believe in wireless technology – that it will provide improved data accuracy, reduce errors, and result in an overall improvement of patient care.

Until recently, it was impossible to imagine physicians retrieving patient data or lab results while out of the office, scheduling appointments online, or communicating with other hospital staff via wireless access. Instead, the stereotypical scene was the doctor being paged during lunch or while sleeping and going in to the office or hospital, whether day or night. Although it is an advantage to be able to contact medical professionals around the clock, what the healthcare industry failed to realize was that they were wasting valuable time. The time healthcare staff spent contacting the doctor, obtaining patient histories, lab results, x-ray images, or pharmaceutical information could have been better spent on patient care. Now doctors don't have to stay at the office all hours, but can view images from home via scanned images available online. Additionally, outsourcing initial diagnosis is starting to expand, as organizations want their images given a preliminary review immediately and can't render this service at night.

The healthcare industry had been slow to move to remote access solutions out of patient privacy concerns, and now with the passing of the Health Insurance Portability and Accountability Act (HIPAA), there is an even higher demand for the security and privacy of electronic healthcare information. The importance of HIPAA is the fact that compliance is not an option - it is a requirement of every entity involved with electronic health care information - health care providers, health plans, employers, public health authorities, life insurers, billing agencies, information systems vendors, service organizations, universities, and even single-physician offices. Implementing a remote access solution for everyone involved seems like a daunting task, but with the right solution healthcare organizations can lower costs, raise productivity and improve patient care. More importantly, healthcare professionals frequently require timely access to confidential patient information in order to provide the highest quality care, which in some cases can mean the difference between life and death.

Benefits of Remote Access

Physicians are increasingly utilizing remote access solutions to retrieve vital medical information while working from home or local clinics as they become more technologically savvy. Physicians first starting using dial-up services to help them connect from home, and as the need for remote access to hospital applications increased, they turned to VPNs. Now with the increasing popularity of Web-based applications and the accessibility of the Internet, physicians are demanding simple and secure access to their applications over a Web browser. Having all of a patient's information in one digital place makes it very easy for a doctor to access it from anywhere he or she might be located – including remote sites outside of the facility or from their laptops. More than one person can even access the information at a time so that a doctor at one end of the hospital and a lab technician at the other can view a patient's medical history or lab results simultaneously. From a home PC, a physician can view a patient's medical history, radiology images, vital signs as they are happening, and lab and test results as they come in and give proper care instructions to an on-site nurse or physician. With anywhere, anytime access to patients' information, doctors can provide them the highest levels of care. The diagram below depicts how easy it is for doctors to access information wherever they need access.



Remote access to electronic medical information help healthcare providers to reduce administrative costs, reduce errors, expand accessibility and ultimately enable them to become more efficient operations. Data from medical imaging equipments can be sent electronically in real-time, to the proper physician, saving the time usually needed to wait for the results and the labor needed for delivery. Not only is delivery more efficient, but also the quality of images can be guaranteed if they are managed in one central location. With remote access, hospitals can easily connect to branch clinics, insurance companies, laboratories, medical transcriptionists, or other organizations. When buyers and sellers of medical products and services can do electronic business transactions easily and quickly, overall communication costs can be reduced dramatically.

With hospital administrators being able to access a patient's information in one area, patients no longer have to fill out tedious paper work multiple times. Doctors can be switched without having to relay the whole medical history each time. Patients don't have to worry about forgetting their prescription slip at home any longer because the pharmacy will already have their prescription online. The whole admissions and billing process can be dramatically improved. Patients can even access their own records and check for their next appointments online, as well, again reducing administrative time and cost.

As healthcare organizations increasingly leverage the Internet and Web-based applications as a real-time communication vehicle among medical professionals, patients, partners, and corporations, choosing the right solution for the protection and security for their network is absolutely critical, and even more so in light of HIPAA requirements for protection of confidentiality and security of information.

Remote Access Solutions

Many traditional remote access solutions have been proven costly and along with remote access there are a variety of security and privacy concerns. Toll charges, poor security implementations, deployment complexities, ongoing maintenance costs, and lack of scalability have forced healthcare organizations to move away from traditional approaches such as dial-up remote-access and consider alternatives.

VPN

Virtual private networks (VPNs) have emerged as a method for providing security for hospital resources and connectivity to remote sites, such as clinics, labs or practitioners' offices; VPN's are used for site-to-site connections that require large constant data transfers such as between insurance providers and hospital data centers; for connectivity within the same location, or between the scheduling and billing departments. VPN solutions have been around for a number of years and have been considered one of the most secure methods for remote access to corporate networks because they require special client software, provide a point-to-point secured tunnel, and they require specific configuration settings. A VPN is a very attractive method for remote access for the user because they are presented with a desktop interface almost identical to the one they are accustomed when they are in the office.

However, VPNs do carry some security risks. Although a VPN might be able to securely send information over the Internet, the data itself resides on laptops and other remote devices, which are still vulnerable to loss and theft. In a wireless environment, a VPN connection is even more of a security risk because everyone accessing the wireless connection is sharing the same network segment. If a physician has already logged into the hospital network, a hacker can then use that same connection to access critical medical information. In hacking into a VPN connection, the hacker is already past the firewall and connected to the hospital's network, jeopardizing valuable medical information. Moreover, the password conventions still being utilized with VPNs are not strong enough to protect such critical data.

In addition to the security risks, VPNs are very IT-resource intensive. Unlike IT departments in large corporations, hospital IT departments typically do not have the resources to install VPNs on every PC that requires access. VPNs also need to be updated and maintained constantly, which is very time and cost consuming.

Authentication Solutions for Remote Access

While the integrity of patient information is critical, of equal importance is the actual protection of individual patient records. This requires the ability to uniquely identify and authenticate an individual. HIPAA standards require the protection of confidentiality and integrity of "individually identifiable health information" through authentication and verification of users.

Passwords

Traditionally, passwords have been used as a means of authentication, as they are the easiest to deploy. However, passwords also happen to be one of the easiest to hack. Passwords may be convenient for users if they are short, but they can make a hospital more vulnerable to unauthorized network intrusions and cause security breaches. If the hospital IT department tries to use a complex password convention, users will just end up writing them down because they are too difficult to remember. A password written on a notepad is an open invitation to the network. There is also the ongoing concern of users sharing their passwords with one another. Even if an employee has a complex password, changes it frequently, and does not write it down, passwords can still be compromised with "cracking" software in a matter of minutes. IT departments often waste valuable time maintaining password issues. Passwords ultimately give a false sense of security, which is a danger in itself.

In any good security scheme, human limitations must be factored into the equation. Thus, we have the rise of hardware based authentication solutions to address this very issue.

Biometrics

Biometric solutions have risen in popularity because they are not only secure but also give the user the sense of “high-tech” security that encourages acceptance. But biometric solutions are not without their drawbacks. Fingerprint scans are not a practical solution for employees working with chemicals or doctors wearing gloves. And whether using a fingerprint or retinal scan, there is still the question of false positives and false negatives. Another important factor that is often left out when discussing biometric solutions is that while a user is uniquely identified; most biometric solutions are still only one-factor authentication schemes. Biometric solutions are still large mathematical number derived from unique, immutable biological characteristics that make for a strong password. They are still subject to the same replay-attack as passwords. A hacker could still intercept this transmission and obtain the “password”. While a biometric solution is a strong way to prove “who you are”, it does not address the “what you have” criteria that categorizes two-factor authentication. By taking unique characteristics of individuals, biometric techniques end up, rather, with the stigma of being intrusive.

In addition, biometric devices are very costly. The technology is still new and not very widely deployed, thus resulting in exorbitantly high prices. If one of the goals of an organization is to reduce costs, it will be difficult for healthcare organizations to justify implementing a biometric solution.

Smart Cards

Smart Cards are also an appealing choice for authentication. They have the familiar credit-card-like form factor with which we are comfortable. Like ATM cards, they are PIN protected, establishing a two-factor authentication. With two-factor authentication, successful access requires not only a tangible object that the user carries, the smart card, but also intangible information that only the authorized user knows, their PIN. As a result, this combination approach constitutes one of the strongest forms of access control. Yet smart cards also have the drawback of labor and cost-intensive implementation. Smart card deployment would mean providing a smart card reader for numerous workstations including patients that wish to ensure on-line privacy. As for cost, smart cards are relatively inexpensive but the associated readers are not. Again, the goal of cost reduction is hindered. Most smart cards only work on readers from the same supplier, where other forms of authentication such as passwords and tokens will work on any computer.

USB Tokens

Over the past few years the USB token has seen an increasing rise in user acceptance. Similar to smart cards in functionality the USB token addresses three of the main smart card drawbacks:

Lack of a ubiquitous reader.
Reader compatibility with PCs.
Cost of deployment.

Because virtually every PC has a USB port today, this solves the problem of both having to deploy a reader and having to worry about compatibility issues. With the reader already built in, the workstation is already configured for use with a USB token. Convenient enough to fit on a key ring, the USB token is user-friendly and not intrusive. They are also more durable than smart cards, which are packaged in a thin plastic casing as opposed to the more rugged housing that a USB token provides.

From a security standpoint USB tokens are identical to readers in that they also require the use of a Personal Identification Number (PIN), establishing a two-factor authentication, as well. For network security, two-factor authentication is not only extremely secure, but also scalable and portable. The USB token stores the user's "credentials" and since the user's secret resides on the token, he or she only needs their PIN to access the network. If lost or stolen, the token is useless to anyone else. In fact, it will lock up after a fixed number of incorrect guesses at the PIN.

From a cost standpoint, the USB token is the most appealing in that it is about half the cost of a smart card and reader. When balancing security versus cost with high-end biometrics at one end of the spectrum and passwords at the other end, the USB token is the most secure, cost-effective solution.

Secure Anytime, Anywhere Access with SSL VPN

VPNs based on Secure Sockets Layer (SSL) technology are quickly becoming the most popular solution for deploying security for core applications being accessed over the Internet. Data travelling over insecure Internet networks are protected with SSL, the same security protocol on all standard Web browsers. SSL provides the server authentication, data encryption and message integrity over TCP/IP connections. Today, SSL is supporting millions of online transactions and corporate data daily and has become the standard for secure online credit card purchases, stock trading and banking.

SSL VPNs provide a number of advantages to the healthcare industry. For one, because SSL is a component of the Web browser, there isn't complex VPN client software to install and manage. This is a big bonus for the already resource-lacking hospital IT departments. The fact that remote users can access centralized applications securely from any Web browser frees the IT staff from having to install, update and maintain application clients on hundreds of remote physician or clinic PCs.

SSL VPNs can be deployed in a matter of days and even hours because they don't impact existing infrastructure, web servers, firewalls or client environment. Within a day, physicians, providers, technicians, mobile caregivers, and patients alike can access medical records and images that they need via the Internet securely using only a Web browser. Business partners, such as billing organizations, insurance companies, labs and others can easily access the information they need, as well.

More importantly, with SSL VPNs, network administrators can combine a number of additional security elements, such as stronger access control and two-factor authentication for added protection. User permissions and policies can be set to limit access to specific applications for specified users as needed. Once users are authenticated, they need to be authorized to have access to certain applications and privileges based on their profile. This is added reassurance that only physicians can access patient information, while billing companies' only access payment information. Utilizing a two-factor authentication solution, such as a USB token, SSL VPNs provide the highest amount of security needed to protect critical healthcare information.

Conclusion

As healthcare organizations increasingly turn to the Web to access their applications, security becomes even more crucial - since confidential health information is becoming available over the Internet – and now under HIPAA, organizations face regulatory requirements for privacy and security. It is critical then that healthcare organizations' security policies be implemented consistently throughout their network. SSL VPNs are well-suited to meet the anytime, anywhere remote-access needs of the healthcare industry in general, while complying with the security demands of the HIPAA regulations in particular. SSL VPNs can provide real-time access to patient health information, while maximizing physician time and productivity. Certainly, healthcare institutions need to choose the solution that is most appropriate for their network, but taking into account its cost-effectiveness, ease of use, ease of deployment, and higher security, the healthcare industry is sure to benefit most with SSL VPNs.

Courtesy ... Cynthia Kawamura
(www.bizforum.org)