Remote Access for Healthcare – HIPAA and Beyond

Challenges and Solutions for the Healthcare Industry

One of the biggest challenges that the healthcare industry faces today is improving patient care with new technologies while maintaining patient confidentiality, streamlining operations, and reducing costs. Healthcare professionals realize that timely access to confidential patient information is essential to providing the highest quality care; in some circumstances it can mean the difference between life and death. With these concerns in mind an increasing number of healthcare professionals are beginning to evaluate secure remote access and mobile wireless solutions that improve efficiency, increase data accuracy, and improve patient care.

Until recently it was impossible to imagine physicians retrieving patient data or lab results while out of the office. The stereotypical scene entailed the paging an on-call doctor who then trekked to the office or hospital. Although it is still advantageous to contact medical professionals around the clock during emergencies, the healthcare industry realized that valuable time was wasted while the doctor was commuting, and 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 can view diagnostic images, examine patient charts, schedule appointments, or communicate with hospital staff from home via online remote access or wireless technology.

Initially, the healthcare industry was slow to move to remote access solutions due to patient privacy concerns and with the passing of the Health Insurance Portability and Accountability Act (HIPAA), there are even greater demands on the security and privacy of electronic healthcare information. Under HIPAA health care providers, health plans, employers, public health authorities, life insurers, billing agencies, information systems vendors, service organizations, universities, and even single-physician offices handling patient medical data must comply with strict rules designed to protect confidential patient information. Implementing a remote access solution that adheres to these regulations while permitting many different healthcare entities to access it is a daunting task, but with the right solution healthcare organizations can lower costs, raise productivity and improve patient care.

Remote Access Solutions

As healthcare organizations leverage the Internet and Web-based applications to connect medical professionals, patients, hospitals, teaching facilities, insurance, and health product manufacturers, choosing the right remote access solution to connect healthcare providers and protect sensitive records is absolutely critical. In light of recent HIPAA requirements, the need for a solution that maintains the confidentiality and security of that information is even greater.

Many traditional remote access solutions have proven too costly and introduced their own security and privacy concerns. Toll charges, complex or poorly designed security policy implementation, complicated deployment, high ongoing maintenance costs, and lack of scalability have forced healthcare organizations to move away from traditional approaches like dial up and leased-lines and consider more flexible or economical alternatives.

SafeNet
The Foundation of Information Security

Virtual Private Networks

Virtual private networks (VPNs) have emerged as best method to provide connectivity between remote sites and secure remote access to hospital resources. VPNs create secure, encrypted connections, known as tunnels, between two locations through another network, such as the Internet. VPNs are ideal for site-to-site connections between to clinics, labs, and mobile practitioners, while still allowing for large, constant data transfers between insurance providers and hospital data centers. VPNs also permit controlled access within the a single physical location to prevent unauthorized access to sensitive data on a large network – for example human resource or finance departments may wish to implement VPNs to control access to confidential files.

VPN solutions have been used for some time and are considered one of the most secure methods to remotely access to corporate networks. A VPN is attractive because users are presented with a desktop interface almost identical to the one they are accustomed to when they are in the office; the VPN client handles the connections in the background to create a seamless network browsing experience that allows users to access files, email, and applications as if they were physically connected to the network. On the downside, traditional VPN solutions require the installation and configuration of client software or network gateways, and may not function properly with some network settings (for example, through a firewall).

Benefits of Remote Access

Physicians are increasingly utilizing remote access solutions to retrieve vital medical information while working outside of hospitals, clinics, or private practices. With the increasing popularity of the Internet and Web-based applications, physicians are demanding simple, secure access to their information and applications through a convenient Web browser interface. Dial-up services were initially used for remote connectivity, but as the need for remote access to hospital applications increased, virtual private Networks (VPN's) are emerging as the preferred solution.

Immediate remote access to patient information allows doctors to provide highest levels of care. Storing digital patient records in one logical location on a network makes it easier to find information and simpler for a doctor to access it no matter where they are located. By removing the reliance on physical copies of charts, x-rays, and lab results, multiple physicians can access the same information simultaneously to facilitate group evaluations and accelerate diagnosis and treatment. From a home PC or laptop, a physician can review a patient's medical history, radiology images, and vital signs in real time, access test results as soon as they are available, and issue care instructions to an on-site nurses or physicians.

Remote access to electronic medical information helps healthcare providers reduce inefficiencies, administrative costs, and clerical errors while expanding accessibility and ultimately offering better, faster care. Hospitals can easily connect to branch clinics, insurance companies, laboratories, medical transcription services, and other support organizations. Data from medical imaging equipment can be sent electronically in real-time, eliminating the wait for the results and saving courier costs while guaranteeing the quality of images since they are managed in a central location. Overall communications costs are reduced as telephone, cell phone, fax, and pager usage is curbed in favor of electronic communication.

With hospitals able to access a patient's information from a single, centralized location, patients and clerks no longer need to fill out tedious paper work multiple times, dramatically reducing errors in the admissions and billing process. Patients can switch doctors without having to transfer their entire medical history. Forgetting a prescription slip isn't an inconvenience because the pharmacy can access a patient's prescription record online. Patients can even access their own records and check appointments online allowing further reductions in administrative time and cost.

Authentication Solutions for Remote Access

VPNs provide a method for the secure transmission of sensitive data across public networks. However, while protecting the confidentiality of patient information during transmission is critical, it is equally important to ensure that patient records are guarded against unauthorized access. HIPAA legislation requires that "individually identifiable health information" is only available to people who have a direct need to access it. To control access to information, a mechanism to uniquely identify and authenticate individuals is needed.

Passwords

Passwords are the most common means of authentication as they are the easiest to deploy. However, passwords are also one of the weakest forms of authentication: if passwords are too short or easy to remember they may be easily circumvented with brute force or dictionary password cracking utilities; if more stringent password rules are enforced, users may write them down because they are too difficult to remember them. There is also the ongoing concern of users sharing passwords.

An easily guessed password or a password written on a notepad is an open invitation to the network making a hospital more vulnerable to security breaches and unauthorized network intrusions. IT departments often waste valuable time maintaining password issues that may take time and resources away from other projects.

Passwords ultimately give a false sense of security due to human limitations. As a result, hardware based authentication solutions have been designed permit strong authentication that is still convenient and easy to use.

Biometrics
Biometric solutions, such as fingerprint or voice scanners, have enjoyed newfound popularity because they offer a sense of increased security and inspire confidence with their attendant ritual and "high-tech" gadgetry. Biometric solutions take a unique physical characteristic from the user – a fingerprint, retinal pattern, or facial geometry – and derive a set of data from that feature that is then used as to authenticate the individual.

Biometric solutions are not without their drawbacks: fingerprint scanners can be easily fooled and are not a practical solution for employees working with chemicals or wearing gloves; retinal scanners can be intrusive and uncomfortable to use; and voice print systems are slow and require training to ensure accuracy. Biometric readers are still expensive compared to other solutions, suffer from false positives and false negatives, and are prone to the same type of replay-attacks as passwords. Hackers can still intercept the data from the scanners during transmission to a host computer and obtain the "password" – in this circumstance, unlike changing a password, the user cannot replace their finger or eye with one that has not been compromised. Biometric adoption, in particular fingerprint scanning, also suffers from the social stigma and privacy concerns stemming from their traditional association with criminal investigations and their immutable, one-to-one relationship to their owner.

Smart Cards
Smartcards are another common choice for authentication. They feature a microchip that stores user credentials and performs cryptographic operations embedded in a familiar credit-card sized form factor. Smartcards are also PIN protected, establishing a mechanism for two-factor authentication. Two-factor authentication requires the user present both a tangible object that the user carries (the smartcard) and a piece of intangible information that only they know (their PIN) to successfully authenticate. The requirements of two-factor authentication create one of the strongest forms of authentication, yet users are only required to remember a single 4-8 digit PIN instead of multiple awkward passwords.

Although smartcards offer many advantages, their primary downfall is the high cost of hardware and labor required to deploy a comprehensive smartcard system. While smartcards themselves are relatively inexpensive, smartcard readers are still a costly peripheral, a cost that adds up when thousands of smartcards are deployed. Each smartcard must also be issued to their respective owners, often a complicated logistical undertaking itself, and smartcard readers require installation and configuration card on every user workstation requiring authentication, a requirement that extends to patients or mobile physicians that wish to ensure on-line privacy. Vendor specific integration issues that can lock a hospital to a single vendor's software, hardware, and support also hamper Smartcard systems.

USB Tokens
Similar to smart cards in functionality, USB tokens address three of the main drawbacks inherent in smartcards: lack of a ubiquitous reader; reader compatibility with PCs; and cost of deployment. Virtually every PC manufactured after 1998 features multiple USB ports, eliminating the need for a separate reader and allowing deployment of USB tokens to users without requiring the installation of any additional hardware on desktop PCs. USB token are also appealing because they cost approximately half as much as a smartcard and smartcard reader solution.

Convenient enough to fit on a key ring, the USB token is user-friendly and not intrusive. The USB token's compact, rugged housing makes them more durable than thin plastic smartcards, allowing them to be carried on a keychain or ID lanyard.

USB tokens offer two-factor authentication similar to smartcards: the token stores the user's credentials requiring the user only needs to enter their PIN to authenticate to the network. If lost or stolen, the token is useless to anyone else without the PIN; after a fixed number of unsuccessful attempts to guess the PIN, the USB token is locked until reset by a trusted administrator.

Secure Access with an 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 remotely over the Internet. SSL is standard on all modern web browsers and is designed to protect data traveling over insecure public networks, like the Internet, by providing user authentication, data encryption, and message integrity verification over TCP/IP connections. SSL is the cornerstone of online banking, e-brokerage, and web retailing, securing millions of online transactions daily; SSL has also proven to be an excellent protocol for VPN use and is ideal for remote access to corporate data.

SSL VPNs provide a number of advantages that make it particularly suitable for the healthcare industry. SSL is an integral component in almost all Web browsers, eliminating the need to purchase, install, and configure dedicated VPN client software and sparing resource-strapped hospital IT departments additional time and money. SSL VPNs also provide a centralized gateway to web-based applications freeing IT staff from the tedium of constantly installing, updating, and maintaining software on hundreds of remote PCs.

Without the need for specialized software or complicated configuration, SSL VPNs can be deployed quickly to any PC; users can even use their home PC to access information. Physicians, technicians, mobile caregivers, and even patients can access medical records, billing information, test results, and diagnostic images securely via the Internet using only a Web browser. Business partners, billing organizations, insurance companies, and labs can easily access and update information immediately.

Most importantly, SSL VPNs allow network administrators to add additional security measures, such as granular access control, two-factor authentication, and encrypted communications to protect their network and the data that resides on it. A two-factor authentication solution, such as a USB token, allow SSL VPNs to provide strong authentication for remote users and prevent unauthorized access to healthcare information. After users are authenticated, their access privileges are restricted to those defined by their profile; user permissions and policies grant access to specific users, limiting access to only the data and applications they need. These access controls compartmentalize sensitive or private data, ensuring that only physicians can access patient information, while billing companies' are restricted to payment information.

Conclusion

Businesses everywhere are turning to the Internet and Web-based applications to share data and distribute applications in order to streamline operations, increase accessibility, and maximize efficiency. For the healthcare industry, the collision between the open - and often insecure - realm of the Internet and the strict privacy requirement of HIPAA are inevitable. SSL VPNs offer the anytime, anywhere remote-access needs of the healthcare industry, while complying with the security demands specified by HIPAA regulations. While every healthcare provider needs to analyze their specific requirements and security policies individually before selecting the solution that is most appropriate for their situation, SSL VPNs offer a cost-effective, easy to use, easy to deploy, high security remote access solution that is uniquely suited to the needs of the healthcare industry.

For More Information

SafeNet (SFNT:Nasdaq) is a global leader in information security. Founded more than 20 years ago, the company provides complete security utilizing its encryption technologies to protect communications, intellectual property and digital identities, and offers a full spectrum of products including hardware, software, and chips. ARM, Bank of America, Cisco Systems, the Departments of Defense, and Homeland Security, Microsoft, Samsung, Texas Instruments, the U.S. Internal Revenue Service, and scores of other customers entrust their security needs to SafeNet. For more information, visit www.safenet-inc.com.