

7/30/01

Remote Access Technology: The Great Enabler

Leslie Ann Fox, MA, RHIA, And Patty Thierry, MBA, RHIA, CCS

Thank you to Advance Magazine for permission to use this article

Leslie: I have been watching e-health evolve for the past two years, and I am very excited to see how the use of the Internet and remote access technologies are enhancing the delivery of health care. It seems every week I read a story about physicians remotely checking test results, ordering new tests, viewing radiology images and conducting “electronic rounds.” Remote access is becoming commonplace in health care and presents a great opportunity for health information management (HIM) professionals to demonstrate their data management expertise. It also opens doors for the development of telecommuting programs.

Patty: Remote access has improved the way other industries operate and deliver services and will inevitably have the same impact on health care. As you can imagine, remote access is a critical issue for health care’s chief information officers (CIOs) because of the pressing business needs to provide access to patient data, share data with business partners and support the trends in telecommuting. Today’s environment not only includes physicians accessing patient information from their offices (and downloading to their palm devices), but also includes employees such as coders and transcriptionists working from home, and business partners performing their services remotely.

Leslie: Based on what you are saying Patty, it seems so important for HIM professionals to participate in the development of remote access strategies for physicians, telecommuters and business partners who will be accessing administrative, clinical and financial data.

HIM professionals have addressed the issue of access to patient information for decades, albeit in a paper environment. Now we see our information technology (IT) counterparts struggling with the same issues. While IT professionals understand the technologies that enable access, HIM professionals have long provided leadership on what should be accessed and by whom.

Patty: It is one of the ways in which we fulfill the function of “keeper of the records.” Even electronic records have to have a “keeper,” and that is not a role HIM should abdicate to others. I know that HIM professionals have so much on their plate already, but I feel strongly that we can play a key role in defining who should access what remotely. It seems that today’s remote access strategies revolve mostly around physician’s gaining access to patient data, which is the best place to start. However, these strategies can’t end there. Health care providers and employees who are involved in “back office” functions have a strong business need to be able to remotely complete these tasks. For example, if your physicians complete records online by electronically viewing and signing test documents or images, they should have this capability remotely as well. Often, an organization’s remote access strategy will include patient data access but not departmental workflow functions.

Leslie: What about remote access to perform HIM functions like coding, data quality reviews and transcription? HIM employees who are part of a telecommuting program will need access to the applications

they would typically use at work, such as e-mail, dictation systems, encoders and abstracting systems. If they create files and store them on the local area network (LAN), they will need to have access to these as well. We know from experience with our clients that just because an organization has a remote access strategy doesn't necessarily mean that HIM telecommuters can access all of their applications and files.

Patty: That's correct Leslie. In fact, to access most encoders, the information systems (IS) department may need to work with the encoder vendor to enable remote access to their system. Sometimes it may require the encoder to run under a specific operating environment, for example Windows NT® vs. Microsoft® Windows 2000 and in other cases the encoder version may not support remote access at all. For our colleagues who are using the older DOS encoders, remote access to these systems is typically limited to using remote control products like pcAnywhere™. This method is slow but used in many organizations as a short-term solution while the overall remote access strategy, including upgrading applications from DOS to windows, is being built.

Leslie: What are some of the remote connectivity technologies used today?

Patty: Organizations that already leverage Internet technologies (have a Web site, Intranet or Extranet) are best positioned to provide remote access. These organizations usually implement a virtual private network (VPN). A VPN is a secure, stable and economical method of connecting hundreds of geographically dispersed remote users. Most likely it will become the best practice method of remote access in health care.

Some organizations may choose to lease dedicated T1 lines to connect remote offices and users to their system. Leased dedicated lines may be the most secure of all technologies, but this solution is very costly and is best used to connect remote offices and business partners.

A common method used today includes the use of leased telephone lines for multiple users to dial in using dial-up networking. Users connect to a dial-in server, which then connects them to the network using network and/or proprietary software. This method requires a modem pool, is costly because of the telephone costs and limits the amount of individuals who can access systems simultaneously.

Many health care facilities use remote control solutions as their remote access method. There are two types of remote control technologies: standalone and networked based. The most common standalone product used in health care is Symantec's pcAnywhere™ remote control software. Using pcAnywhere™, a remote user dials into a PC on the LAN that contains the applications to be used by the remote user and takes control of the PC. This requires a separate PC on the network for each remote user. This method is considered costly, slow and not very secure. The user interface is also sometimes confusing. Using the network remote control method, the remote user dials into a server on the LAN and connects to a host computer on the network, which contains the applications used by the remote user. This is a more secure and faster method than its standalone counterpart but as more users are added, performance becomes an issue. An example of networked based remote control is the Citrix® WinFrame® product.

Leslie: I have heard a lot of hype about VPNs. How does a VPN work?

Patty: A remote user first connects to the Internet using his or her own Internet Service Provider (ISP) or an ISP provided by the health care facility. Remote users can use dial-up access, cable modem, DSL or satellite. Once an Internet connection is made, the software necessary to access the organization is then opened on the remote users computer. This software is usually referred to as the VPN client software. The remote user enters their username and password. The VPN server and firewall on the health care facility's network verifies that the Internet user (in this case the remote user) meets specific security criteria to access the private network from across the Internet. When the user passes the firewall, and successfully authenticates, they have created

the VPN and can now access the LAN.

Leslie: I understand that VPNs are very secure. Is this the case and do they meet the Health Insurance Portability and Accountability Act (HIPAA) security requirements?

Patty: VPNs use what is known as tunneling protocol and encryption. When a remote user successfully connects to the VPN server, a tunnel is created. Data travels the Internet in packets. When it travels in a VPN, each packet is encrypted and encapsulated. The packets are then transmitted via the Internet until they reach their destination. Once they reach their destination, the packets are re-united and decrypted.

A VPN server on the network side acts as the gatekeeper of the private network. It consists of a router, firewall and the necessary hardware and/or software to protect against unauthorized access to information on the network. A VPN server also acts as a policy server because it contains the list of who has access to what. As you know, the HIPAA security regulations do not tell you what security solutions to implement. VPNs do meet the security requirements spelled out in HIPAA provided that the full breadth of a VPN is implemented.

Leslie: Sounds like the IT folks have their hands full. How would you advise HIM professionals to define their role in remote access usage?

Patty: First off, find out what the remote access plan is for your organization. Offer to participate in testing remote access and be a champion of the technology. Work with the IT and human resources department to develop telecommuting policies for employees and remote access policies for physicians and other authorized users. These policies help standardize the types of hardware and software to be used on remote workstations, what applications will be accessed and who has access to what.

Leslie: As I think about what you have been telling me, I hear two essential messages. First, as medical records become more electronic, health care organizations must reap the full benefit of productivity improvements afforded by remote access technologies. That means users must not only gain access to records from remote locations, but they also must be able to enter information to complete efficiently record keeping tasks. Second, the HIM professionals must take the lead in performing the critical function of “keeper of the records,” by crafting appropriate policies for access to patient information in a secure environment. To know that the environment is secure, they must understand remote technologies and collaborate with IT professionals as systems are designed to support medical record applications.

Leslie Ann Fox is president and chief executive officer, and Patty Thierry is vice president and chief information officer of Care Communications Inc., a Chicago-based HIM services company whose newest service is remote coding with CAREcoding.com and YourStaff-@Home. They invite readers to send their thoughts and opinions on this column to lfox@care-communications.com or to pthierry@care-communications.com.