Securely Implementing Remote Access within Health Information Management

Save to myBoK

by Eugene T. Carroll, RRA, Susan Wright, MBA, and Cindy Zakoworotny, MS, RRA

As technology changes, our definition of the workplace expands, and we no longer are limited to working at our desk in an office. The authors describe technologies that enable us to work from home or on the road and examine security regulations and precautions.

As health information management (HIM) departments become technology enabled, there is no longer a need to process and complete medical records on-site in a centralized area. Document imaging applications, clinical repositories, and transcription capabilities allow for remote processing of health information either in a centralized area or from remote sites.

Following the acquisition of document imaging and PC-based coding and grouping capabilities, the HIM departments of both Hartford Hospital and Veteran's Memorial Medical Center plan to physically merge. Staff from Veteran's Memorial Medical Center, in Meridien, CT, will relocate to the Hartford Hospital campus in Hartford, CT, in spring 1998. Veteran's Memorial Medical Center's patient records will be processed remotely on workstations within the Hartford Hospital HIM department. To prepare for this move, and for the eventual move of the coding and record completion functions to an off-campus building in 1999, staff members have made remote access security a priority initiative. This article provides an overview of remote access approaches and the controls that should be addressed to assure the confidentiality and security of patient and hospital information.

Technology Overview

Connectivity

There is an increased trend in multi-campus organizations providing users access to a centralized data repository. Similarly, there is also a trend toward huge healthcare private networks linking health organizations, hospitals, physician offices, outpatient services, and clinics. Remote computing allows access to information on disposition of patients while they are still in an inpatient facility as well as after they are discharged. Physicians see a great advantage in accessing information remotely from their home or office in order to add to or view a patient's record without having to travel.

Popular remote access software packages such as PC Anywhere, Carbon Copy, Reachout, and Lotus Notes allow workers to read e-mail, troubleshoot problems, and move files. Internet Web browsers such as Netscape Navigator may be used with the latest versions of these products. Some software can even connect older non-Windows PCs to servers running Windows applications. Using older non-Windows PCs for remote site connectivity can also mean cost savings, another plus. At present there are several types of remote communications available; the two principal methodologies are remote control and remote node technology.

Remote Control

With remote control, a person connects to an office PC and controls it from a remote location via modem and telephone line. In effect, the remote user is working at the office PC, controlling its mouse, keyboard, and screen operations. The remote control software runs on the PC at the office, so a minimum of data actually travels over the phone line. Combining this with the constant improvement in modems, such as the recent introduction of 56K modems, remote users can expect to work almost as quickly as they would at an office PC that is directly connected to a LAN.

Remote control may be the best bet for situations in which large amounts of data need to be transmitted, which can cause a lot of network traffic. If data can be transmitted to an office PC rather than on telephone lines, considerable time can be saved.

Remote Node

Remote node, on the other hand, allows a remote PC to directly connect to LAN resources over a dial-up telephone line. A user can still access the same network resources, including printers and files. With remote node technology it appears that a user has a network cable connecting the home and office. This technology requires unique hardware and software.

Remote node differs from remote control in that all application software runs on the remote PC. It is a slower method, since it relies on passing information through a telephone line. A good use for remote node is client/server applications that generate minimal LAN traffic. When its use is limited to applications that perform most of their work on a remote PC, users will find response times tolerable.

Currid & Co. note that "Remote control is generally speedier and more versatile than remote node. Remote control can be used exclusively for remote access instead of remote node, or can be used alongside it. Remote control can also be used to perform tasks that remote node cannot, such as remote support and training. It also can be used for collaborative work between sites, which is difficult with remote node technology." [1]

Remote Control and the Internet

As both remote control and Web browser software evolve, remote control may now be accomplished via the Internet. A remote control product that allows the use of the Internet should employ security that is both strong enough to deter the potential for breach of confidentiality, yet easy enough to configure that users can make use of the security features. Most remote control software on the market today will have some combination of data encryption and virus detection and an audit log to keep track of who has accessed data. All of these features are necessary to make using the Internet viable.

Security Requirements

When designing policies related to remote access, it is important to be mindful of certain security issues, such as workstation and software security. It is equally important to implement the appropriate security measures, including validation, use of passwords, and accounting.

Security Issues

There are security issues that need to be addressed with increased remote access. Secure electronic storage, retrieval, and transfer methods for healthcare information are crucial. Security policies and procedures must be in place to define and prevent unauthorized access. Preserving data quality and preventing loss, destruction, tampering, and unauthorized access that might arise from remote access use must also be priorities.

The use of personal computers themselves presents inherent security concerns, both for the remote user and the office user. Screen lockouts after a specified period of inactivity can be effective in preventing unauthorized access. Anti-virus software should be updated every few months to protect against new and mutated virus strains. There should be restrictions on remote access of certain confidential data types. The way in which the network or LAN is set up can provide levels of security, as can lockout features that activate if the wrong password is utilized a certain number of times, preventing unauthorized access to network data.

The spread of computer viruses from the remote PC to the work PC that could possibly infect the server is a major concern, especially if an organization has not established who should be responsible for eradicating the virus and reinstalling programs and files. Paying for purchase or repair of hardware and software is also an issue for remote users using a home computer. Other security issues with remote access are related to the environment. Telephone failure can occur due to hardware failure at the main site, or lines may fail due to damage from natural disasters such as floods and tornadoes. In some areas, hardware damage resulting from power spikes or brownouts due to variable levels of electricity supplied to homes during times of peak demand—especially during the summer months—may be a concern.

There is also a confidentiality issue related to remote users' access of paper documents. These confidential documents must be protected from others and locked in a secure place when not in use. Also, if original documents, rather than copies, are taken from the office for use at home, they must be transported by a secure method. A method to account for the return of these documents must be developed to ensure proper storage and disposal. Confidential documents must not end up in a recycling bin but should be returned to the company for secure disposal. If original documents are used, a method must be developed to protect against unauthorized change or loss. Education of the remote user can be effective in limiting security breaches, and it is always important to have the necessary policies and procedures in place if privileges are abused.

Remote Access Security, User Validation, and Authentication

There are several ways to ensure user validation for remote access systems. Password features such as expiration, grace log-ins, and allowing users to change personal passwords can provide flexibility for both users and administrators. Integrating security features with a remote access system provides ease of management and simplicity, allows for configuration from a single location, and helps eliminate the possibility of security loopholes. Other technological solutions for remote security include the use of data keys and data cards. The use of ID numbers and passwords are also important for securing data. There are emerging trends in the use of biometric methods, including the use of thumbprint scanners and retinal/iris scanning devices for user authentication. Finally, firewalls—consisting of a mix of both hardware and software—protect servers that users access.

Password Protection

The first step in limiting security breaches is to teach users not to write down passwords and keep them in plain sight, and not to walk away from a computer when logged into the network or LAN. Also, the practice of sharing passwords with other users should be actively discouraged. Standard reusable passwords are not recommended for a secure network.

Location Validation and Call Level Security

Location validation employs certain callback methods to confirm a user's location. One methodology is caller line ID, a process in which the phone number of an incoming call requesting remote control access is compared to a log of accepted phone numbers. Access is granted only if the phone number is found in this log.

Another callback method is one in which the system dials a preassigned number. This is known as fixed dial-back, and it has the added benefit of allowing the hospital to assume remote access line costs, thus allowing companies to centralize and better track costs. Security is also improved because a known number or location is called back; thus, an invalid user dialing in will not be called back.

Authorization (Access Control)

Security may be further enhanced through the use of authorization or access control. Examples of this would be allowing remote users access to system resources based on the department they work in or their job description. By using well-defined access control levels, hospitals are further able to control what information is available to remote users.

Accounting

Accounting involves tracking, auditing, and reporting remote activity. Properly implemented and used, accounting allows usage patterns and activity to be monitored. It can also be helpful in detecting attempts to access protected or confidential files. Accounting is carried out either by audit logs contained within the remote access server or by means of a stand-alone security audit program. Well-maintained security audit logs may be instrumental in showing deviations from normal usage or unusual activity such as remote log-in attempts by a user in the office, multiple concurrent dial-in sessions by the same user, or a significant number of failed log-in attempts.

Conclusion

As HIM departments become decentralized, practitioners will need to become more familiar with tools such as remote access to better work with data. At Hartford Hospital, a great deal of effort is being expended in implementing the concepts discussed in this article. To this end, both Hartford Hospital and Veteran's Memorial Medical Center HIM professionals have joined forces with their information systems groups. As the technical knowledge of information systems experts is combined with the HIM professionals' understanding of confidentiality, remote access becomes a secure and viable tool.

Note

[1] Currid & Co. "Remote Communications." Symantec White Paper Series, 1997. Available at http://www.symantec.com/pca/wp_remotecomm.html.

References

Chidley, Elise. "Home Based Coding—The Way of the Future?" *For the Record* vol. 9, no. 1 (1997): 21-23.

Currid & Co. "Remote Communications." Symantec White Paper Series, 1997. Available at http://www.symantec.com/ pca/wp_remotecomm.html.

Gellman, Robert, and Kathleen A. Frawley. "The Need to Know Versus the Right to Privacy." *The Computerization of Behavioral Healthcare*. San Francisco: Jossey-Bass and Centralign, 1996, pp. 191-212.

Gordon and Glickson, P.C. "National Survey Reveals Hospital Computers Are Unprepared for the Next Century." *For the Record* vol. 9, no. 12 (1997):14.

Presti, Ken. "Remote Access Hits Big Time." *InformationWeek*, October 27, 1997.

Raylor, Arlowen Jordan. "Healthcare Information Systems...Confidentiality and Security." Paper presented at Computers in Healthcare Interfacing with Nurses meeting, June 5, 1997.

Reback, Andrew, and Ian Smith. "Remote Access Security: An Overview." Shiva White Paper Series, 1997. Available at http://www.SHIVA.com/pacrim/japan/remote/prodinfo/ security/index.html.

Siwicki, Bill. "Health Data Security: A New Priority." *Health Data Management* 5, no. 9 (1997): 48.

Points to Remember

Access

- All access should be through a single, well-managed point of entry to the network (e.g., modem pool).
- All modem phone numbers should be unlisted and out of sequence with existing enterprise phone numbers.
- Modems should not be connected to individual PCs or other systems except in special circumstances, following a detailed risk assessment.
- Users should be identified before any actions can be initiated.
- All access should be controlled by user name and password (no password-free accounts).
- File system privileges should be customizable for each user ID.
- Restrictions on uploading programs (e.g., Trojan Horse or virus-infected programs) remotely should be enforced.
- Where possible, all information (particularly authentication information) should be encrypted.
- Access should be able to be blocked during system maintenance.
- Users should be allowed only one remote connection at a time.

Audits

- Log all activities.
- Audit records should be protected from unscheduled modification (including deletion) by any user (including apparently authorized users).

- Alarms and authentication violations should be recorded in audit records by default.
- Audit records should include date and time, user, origin, type of event, and its success or failure.
- Audit records should be retained long enough to be used for reviews and security analysis.
- Audit information should include each user, device, port, and phone number.
- Security events should trigger alarms to notify the security administrator.

Log-ins

- Users should be provided with last log-in information, such as date and place.
- Identifying information should not be displayed until after an authorized log-in.
- All users should be presented with a warning of the penalties for unauthorized use and informed that all activities are being logged each time they access the system.

Users

- Each user should have a unique identifier (no work group or generic accounts should be allowed).This narrows the range of possibilities in the event of a security breach.
- Time-out facilities should be implemented to deal with users who may forget to log out or who log out incorrectly.
- Passwords should be regularly checked to ensure they cannot easily be guessed.
- Restrict user access to specified time periods where possible.
- Security information should be changed frequently.

Susan Clark *is director of clinical information management at St. Anthony Hospitals/Centura Health in Denver, CO.* ***Patti Leri*** *is a coding/reimbursement specialist for the Colorado Mental Health Institute in Pueblo, CO.*

Article Citation:

Carroll, Eugene T., et al. "Securely Implementing Remote Access within Health Information Management." *Journal of AHIMA* 69, no. 3 (1998): 46-49.