Safe at Home: Remote Coding Meets HIPAA

by Tim Keough, MPA, RHIA

Remote coding offers big benefits and unique security challenges. Here's how one organization moves patient data securely across the Internet.

"Whatever, in connection with my professional practice, or not in connection with it, I see or hear, in the life of men, which ought not to be spoken of abroad, I will not divulge, as reckoning that all such should be kept secret." These words, written by Hippocrates, the father of medicine, demonstrate that preserving patient health information in a confidential and secure manner was as of extreme importance in the fifth century B.C. as it is today.

Tremendous modern advances in information technology add an entirely new level of complexity to keeping secret that "which ought not be spoken of abroad." Health information management professionals face the challenge of leveraging the power of information technology while simultaneously preserving patients' rights to confidentiality and security. Perhaps nowhere is this challenge more acute than in organizations employing the benefits of remote coding technology under HIPAA privacy and forthcoming security rules.

Finding a Remote Coding Solution

In 2001 Community Medical Center's HIM department faced the common issues that confront most acute care facilities at some time or another: lack of space, an abundance of paper-based patient medical records, need for simultaneous access to patient records, a desire to improve employee satisfaction, and of course, a need to reduce the revenue cycle by attracting and retaining the best and the brightest coders to the facility.

For Community—a 596-bed, acute care facility with a volume of more than 225,000 visits per year, part of the Saint Barnabas Healthcare System in Toms River, NJ—home-based coding was the answer. Allowing coding to be performed off site would give Community the ability to accommodate improved coding processes, provide authorized clinicians with simultaneous access to patient information, and allow coders to work out of their homes.

Community's HIM department, in conjunction with the center's information technology and services department, reviewed many vendor product offerings, seeking a cost-effective and operationally efficient document imaging system. Of equal importance was the need for the chosen system to meet confidentiality and security requirements for protected health information (PHI), both as they exist today and as they will evolve with the implementation of HIPAA's security and electronic signatures standards in April 2005.

Community chose a feature-rich and secure system that captures scanned images and transmits them to authorized users. The process is administered through a third-party vendor, the application service provider (ASP) who developed the software. The system offers high-speed scanning, essential and intuitive coding work flow tools, and advanced supervisory controls. In addition, the system could be implemented without great expense for hardware, since the hospital already had the network infrastructure and sufficient bandwidth to accommodate the transfer of image information.

Prior to making the final purchase decision, a project management team reviewed the goals of the project and identified the operational, confidentiality, and security risks and challenges that such a system would present. To accomplish this review, expertise was sought from representatives of the HIM department, the chief privacy officer, the information technology and services department, physician leadership, and representatives from clinical departments including the emergency department, cardiology, and nursing.

The project management team reviewed the risks and potential weaknesses of an electronic record system and began to design work flows and network topologies to establish a secure approach to remote coding. The figure below illustrates the final work flow of Community's home-based coding system.

Multiple Locations, One Set of Security Regulations

The proposed HIPAA security regulations provided the project management team with the security goals for the new coding system. The tenets of the security rule indicated that there was no recognized single standard but that any standard chosen would be technology neutral. The rule also noted that technical solutions should be flexible and scalable for providers, clearinghouses, and plans. The general approach within the rule states that covered entities must ensure that electronic information pertaining to individuals remains secure.

The security rule delineates recommendations in three distinct categories: (1) administrative procedures; (2) physical safeguards; and (3) technical security services and mechanisms. Given Community's remote coding work flow, the center had to address the recommendations for three types of workers in three types of facilities. Here's how the center approached these requirements.

Administrative Procedures

Generally, the security rule requires that covered entities establish administrative procedures and measures to protect data and regulate the conduct of employees in the use of PHI. Complying with this requirement was fairly straightforward, since Community already had established policies and procedures for information management that addressed data validity and integrity, security and control, and confidentiality. In addition, the center also had a clearly defined sanction policy for confirmed breaches of confidentiality.

In addition to policies governing use of information, employee training related to the HIPAA rules and confidentiality and security in general were very important. These issues are addressed upon hire during employee orientation and are reinforced throughout the year in mandatory code of conduct classes, departmental meetings, and a biweekly employee newsletter.

However, to drive the point home for users of the home-based coding system, additional administrative measures were taken to ensure data integrity, confidentiality, and privacy. These include:

- **Home-based coding telecommuting policy and agreement.** A new policy was developed for eligible employees requiring them to maintain confidentiality and security of information in their home by providing a private and secure workplace. The policy also requires that use of computer equipment is for coding purposes only. The agreement must be signed by all employees after it is reviewed with them by their supervisor.
- **Electronic record policy and procedure.** This new policy and procedure was developed to enhance the existing information management policy and to address new processes of accounting for records in an electronic format, scanning and indexing charts, and home-based coding and online viewing of records by authorized clinicians and HIM staff members.
- **Down-time procedure.** If for any reason coders are not able to perform their work due to Internet connectivity issues or other technical problems, the supervisor has the ability to recall the employee to work from the hospital until the problem is resolved. Currently Community has this ability because all employees live within commuting distance of the hospital. For clinical staff needing access to records during down time, the HIM department will retrieve the paper-based chart and bring it to the requesting department.

Physical Safeguards

The HIPAA rule addresses the physical protection of computer systems from events such as fire or environmental hazards and the use of locks or other security features to control access to systems and facilities. Since Community was implementing a remote coding program managed by a third party, the center had to address three areas for physical safeguard compliance: the vendor facility, the hospital, and the employee's home.

The Vendor

Since Community's new system involved sending scanned medical records via the Internet to be stored at the vendor's location, much attention had to be given to the physical safeguards of the vendor's facility. During the request for proposal process, the safeguards listed below were identified and verified:

- All servers located at a secure location monitored 24/7 by security personnel and closed-circuit television
- Access to locked server location only through badge-card scan and palm scan
- Access to server location limited to authorized technical staff only
- Servers backed up on digital tape drives on a nightly basis
- Servers have short-term battery back-up power and long-term diesel back-up power
- Data stored as mirror image on two computer drives; in the event that one drive fails, data may be removed from the failed drive on the fly. Secondary cooling fans available to keep equipment at safe operating temperatures

The Hospital

To effectively code from home, employees needed access to all the tools and systems available at the hospital. Just as radiology reports, lab findings, or other clinical findings may be missing from a paper chart at the time of coding, they may also be missing from the scanned electronic chart. While working within the hospital, coders had access to laboratory, radiology, and clinical information systems in addition to encoder and fax servers.

To replicate access to these systems and to provide for an additional layer of security, Community installed a secured socket layer (SSL) virtual private network (VPN). This system enables coders to connect to all necessary hospital systems through their home-based computer and a Web browser. Data and information flowing from hospital-based systems are protected behind a firewall, and information is encrypted between the SSL VPN site and the home-based coder.

Other physical safeguards used by the hospital include storage of computer equipment in locked, climate-controlled computer rooms where access is controlled through identification cards.

The Coders

To enhance physical computer safeguards for the employee working from home, Community had to take a realistic approach. Naturally, it was not cost effective or practical for the center to install dry fire-extinguishing systems or elaborate computer rooms in each coder's home or for the center to provide back-up systems. However, there were reasonable and practical things that Community could do to improve safeguards, keeping in mind that safeguards must be scaled to what was reasonable for an employee's home.

The first safeguard was the requirement that computers placed in the employees' homes are used exclusively for home-based coding. Employees sign a user's agreement and receive training so that they understand they may not alter or circumvent Web browser restrictions, which could open the computer to unsecured Web sites and increase the risk of exposure to viruses or hacking attempts. Further, all connections to the Internet are regulated through routers that include built-in firewall protection. Employees working from home also acknowledge in the user's agreement that they should not install any other personal software on their home-based coding computer.

The service provider's software does not allow the employees to print, screen capture, or transmit an electronic record from their computers to any other users. Further, following completion of coding, the program does not store copies of patient records on the home-based computer's hard drive, either as files or as cookies. Programming in the software negates this possibility. PHI is not stored on the computers.

Technical Services and Mechanisms

HIPAA requires that technical security services and mechanisms be in place to prevent unauthorized access to data transmitted over a communications network. Community's home-based coding program met these recommendations through a number of measures. The center employs digital certificates and data encryption, and all systems run updated virus protection software and are protected behind a firewall.

Access to the system is restricted by password, which employees choose themselves. The system gives the facility the option of requiring users to change their passwords according to a fixed schedule. Community requires employees to change their passwords every six months.

Access to electronic records is restricted according to predefined rules based on employee role. Community's established roles and privileges are as follows:

- **Administrators** can change system settings, create new users, and delete former users. They also have the ability to delete records or correct record indexing problems.
- **Coders** can only access and view charts assigned to them by their supervisors. This ensures that they only access records on a "need to know" basis.
- **Online viewer** status is granted to clerical employees within the HIM department and authorized clinical staff. Online viewers can be restricted to only viewing records onscreen, or they can be designated to print material.
- **Scan technicians** have the ability to scan, index, and upload images to the vendor's server.
- **Supervisors** have access to scanned records and can assign records to individual coders. They may also set additional rules to select a sample of records to be reviewed for coding accuracy.

In a paper-based world, it is very difficult, if not impossible, to know who has looked at a record, when they looked at it, and what they may have copied from the chart. Community experienced a significant auditing benefit by migrating to the new electronic system, because each employee accessing a record now leaves behind an electronic fingerprint. The audit trail allows the center to enhance its ability to verify that records are only accessed on a need-to-know basis.

Audit trails can be run either by patient name—listing all employees having looked at the electronic chart—or by employee, listing all patients records that an individual has accessed. Reports can be defined by time period, as well. Information captured in the audit trail includes employee name, patient name, date accessed, the function performed, the pages accessed, and the pages printed.

From the onset of scanning paper charts to electronic files at Community, technological security measures are in place, all of which are documented in policies and procedures. Paper-based records are scanned by a designated scan technician within 24 hours of discharge. The images are encrypted and transmitted via the Internet to the vendor's facility. As noted, the vendor protects data in their custody by securing their equipment, limiting access, and providing necessary back-ups and system redundancy.

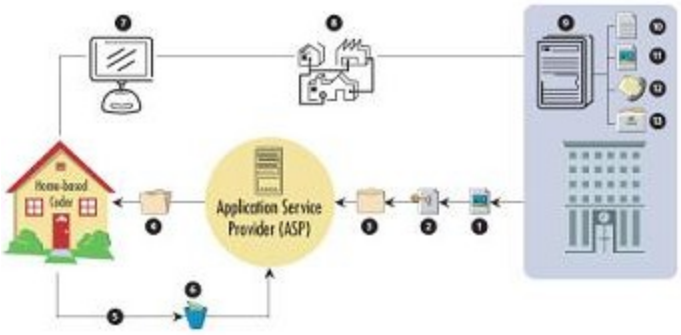
Access to an electronic record can only occur after an authorized coder logs into the system with their user name and password and only after the coder's computer digital certificate is authenticated by the vendor site. For users designated as online viewers, an administrator can restrict viewing capabilities to a specific computer if desired.

A Program Worth the Effort

As with most things that are worth accomplishing, Community found that establishing a home-based coding program was not easy to achieve but certainly was worth the time and effort. To date, the center employs eight coders working from home, processing all emergency department and outpatient records. In the final phase of the program, inpatient medical records also will be coded from home.

Home-based coding allowed Community to accomplish its established goals and to do so without any compromise to the confidentiality or security of patient records. In fact, the features and safeguards of the new system provide better control over records than the center could have ever achieved in a paper-based environment.

Home-based Coding Work Flow



1. Images scanned at hospital
2. Encrypted images transported to ASP server via Internet
3. Encrypted charts assigned to coder; digital certificate assigned
4. Digital certificate at coder's workstation is authenticated; images downloaded from ASP server
5. Access to ASP coding application via Internet
6. Encrypted codes returned to ASP server; images deleted
7. Access to hospital applications via Internet browser
8. Secure virtual private network
9. Hospital server
10. Clinical information system
11. Radiology management system
12. Fax server
13. Encoder

Tim Keough *(tkeough@sbhcs.com) is director of health information management and compliance at Community Medical Center in Toms River, NJ.*

Article citation:
Keough, Tim. "Safe at Home Remote Coding Meets HIPAA." *Journal of AHIMA* 75, no.2 (February 2004): 42-46.

Article citation:
Keough, Tim. "Safe at Home: Remote Coding Meets HIPAA" *Journal of AHIMA* , no. (February 2004): -.