

2/12/01

### **Remote Coding: An Ongoing Dialogue**

*Leslie Ann Fox, MA, RHIA and Patty Thierry, MBA, RHIA*

*Thank you to Advance Magazine for permission to use this article*

**Leslie:** Last month when we were discussing remote coding solutions, I raised the issue that health information management (HIM) and information systems (IS) directors are concerned about security and Health Information Portability and Accountability Act (HIPAA) standards. They perceive these standards as obstacles to implementing a remote coding solution, but the fact is that these standards present a clear blueprint of the technology and policies that must be in place to move forward.

**Patty:** Absolutely! The proposed HIPAA security standards do provide a pathway for moving the healthcare industry into the electronic era. These standards make it possible for vendors to develop software and hardware solutions that provide the means to securely access and transfer patient information between providers, payers and business partners. Many health care providers and their vendors are talking to each other today about how to deliver HIPAA-ready solutions. Bottom-line driven provider organizations are looking for ways to maximize the use of the Internet and other technologies to streamline and improve health care delivery and business processes. Competition is driving vendors to be HIPAA-ready today to meet the demands of health care organizations.

From the remote coding standpoint, HIPAA lays the framework for implementing Internet-based coding applications and providing remote access to authorized employees and business partners. In addition, the application service providers model is providing new capabilities for organizations, especially HIM departments, to manage business processes such as coding, dictation, transcription and document storage.

**Leslie:** The proposed HIPAA security requirements are pretty significant, not exactly a quick read. I understand that the requirements are categorized into four general areas: Administrative Procedures, which includes the documentation of policies and security measures; Physical Safeguards, which includes the protection of physical computers and equipment; Technical Security Services, which identifies the processes that control and monitor access and protect information; and Technical Security Mechanisms, which includes the protection of transmitted data. Do these categories provide specific security implementation features that can guide HIM and IS professionals in their evaluation of remote coding applications?

**Patty:** Yes and No. HIPAA consists of a set of requirements that are technologically neutral and do not dictate how health care organizations should implement security requirements. A list of features is provided to assist in the development of security requirements but not all of the features need to be implemented as long as the intent of the security requirement has been met.

The first step in evaluating remote coding vendors requires a provider organization to define its security business requirements. Once business requirements are defined, then HIM and IS professionals can evaluate which technology solution more closely matches their security approach.

For example, some remote coding vendors store images/rec-ords on CD-ROM, local desktop computers, or on servers located at hosting facilities. Other examples include various transmission methods and encryption options, use of firewalls, functionality for managing data integrity and different ways to control access to data such as user-based or role-based access. Depending on the organization's security approach, one solution might be better than another or any one of the solutions might fit into a provider's existing security vision.

**Leslie:** HIM professionals have been so close to confidentiality and privacy issues, I imagine once one starts looking at remote coding applications, the security issues become familiar. What do you think are the key security features that HIM professionals should use in selecting a remote coding solution?

**Patty:** Since there are various ways to meet the intent of the proposed HIPAA security requirements, HIM and IS professionals need to understand the technologies used by remote coding vendors and evaluate them against how their technologies are deployed. At minimum, remote coding vendors should be evaluated on:

- How data is captured, transferred, stored and accessed
- What type of encryption methods are used
- Firewall controls
- Bandwidth requirements
- Authentication methods
- Audit controls and reporting
- Physical security of hardware
- Maintenance of data
- Disaster recovery methods
- Workflow management

The HIPAA security regulations define six security features that can be used to evaluate remote coding vendors. These features include the ten attributes I just mentioned. Let's take a look at the highlights of each feature.

- Authentication—User identification code and password change password on regular intervals, alphanumeric passwords, no reuse of passwords, no password sharing.
- Authorization—Users can only access those applications they are authorized to use. System time outs, security profiles drive what users can access.
- Data Integrity—Management of duplicates, anti-virus protection, prompts for missing information, controls on simultaneous updates, data protected from unauthorized access via the Internet through the use of firewalls, encryption and authentication devices.
- Audit trails—System alarms for predefined events, user activity, management reports on user activity, error logs, file changes.
- Disaster recovery—Backups, mirroring, recovery plan.
- Data storage and transmission—Physical security of servers, workstations and storage media, maintenance of data; encryption methods, firewall controls. Remote access to the provider's information systems (encoder, abstracting, clinical systems etc.) requires secure dial-in or VPN access, unique user IDs and passwords, limited access times, and limited connection duration.

**Leslie:** I have noticed that HIPAA appears so comprehensive that its hard for organizations to figure out where and how to start. This seems especially true of business partners and chain of trust agreements. The good news is that remote coding vendors have designed their systems with HIPAA in mind. Doesn't this enable organizations to work with remote coding vendors today to deploy new technology and solve a nagging business problem?

**Patty:** Yes! Working with HIPAA-ready remote coding vendors should facilitate the implementation of solutions now rather than later. Organizations will need to use formal chain of trust provisions with their remote coding business partners and vendors to ensure accountability and the protection of privacy.

Provider organizations shouldn't use HIPAA as an excuse not to implement technology, but rather as a reason to move forward. The purpose of HIPAA regulations is to improve the efficiency of delivering health care and streamlining business practices. HIPAA implementation requires a step-by-step approach and while I believe it's important to be thoughtful in our implementation activities, we shouldn't let our deliberations cloud decision-making on market ready products that make use of technology, especially the Internet, to solve or improve current business problems.

*Leslie Ann Fox is president and chief executive officer and Patty Thierry is vice president of operations and chief information officer of Care Communications Inc., a Chicago-based HIM services company whose newest service is CAREcoding.com.*

*They invite readers to send their thoughts and opinions on this column to [lfox@care-communications.com](mailto:lfox@care-communications.com) or [pthierry@care-communications.com](mailto:pthierry@care-communications.com).*