HIPAA Transaction and Security Standards: How Community Cancer Centers and Oncology Practices Should Prepare to Comply

by Andrea M. Kahn-Kothmann, J.D., and Celia M. Santander, J.D.

"Conflicts will no doubt continue between the wish to keep personal health information private and the need to use health care data for social good...The ongoing, and divisive, political debate will focus on a number of contentious areas: Should health care professionals be permitted to freely use, and share, full medical information with the health care team and specialists when treating patients?... Do the written consent standards impose undue burdens on the health care industry?... Should the health care industry have to comply with nonuniform standards at the national and state level? But beyond these legitimate concerns lies the important reality that the United States has adopted the first national health information privacy standard in its history. Ensuring health information privacy is vital to respect the dignity of consumers and maintain trust in the health care system."

Lawrence O. Gostin, the Center for Law and the Public's Health, Georgetown University
—from "National Health Information Privacy: Regulations Under the Health Insurance Portability and Accountability Act"
Vol. 285 No. 23 of the Journal of the American Medical Association

While much attention has focused on the Privacy Rule of the Health Insurance Portability and Accountability Act (HIPAA), its two less glamorous "sister" rules—Electronic Transactions and Security—are often overlooked by health care providers dazzled by the glare of the numerous HIPAA privacy requirements and the controversy that surrounds them. In reality, all three rules harmonize to provide a complete picture of Congress's original intent: reducing health care costs by simplifying the administrative structure of the health care system, improving health care quality, and restoring public trust in the health care system as a whole. Moreover, HHS estimates that the 10-year, $17.6 billion projected cost of implementing the Privacy Rule (with the attendant Security Rule provisions) will be more than offset by the expected $29.9 billion in savings that will result from implementing the Transaction Rule.

Andrea M. Kahn-Kothmann, J.D., and Celia M. Santander, J.D., are attorneys with Reed Smith L.L.P. in Philadelphia, Pa. They specialize in health care, including health information issues.

A LITTLE BACKGROUND

In the mid-1990s, the U. S. Congress attempted to reform an increasingly complex and expensive medical system by "encouraging the development of a health information system through the establishment of standards...for the electronic transmission" of certain health care information. Congress enacted HIPAA (Public Law 104-191) in 1996 to supplement the Social Security Act. Part C (Administrative Simplification) of this new law gave the Office of the Secretary of the Department of Health and Human Services (HHS) the power to implement the legislation. Accordingly, HHS wrote various HIPAA-related rules, submitted them for public comment, revised them, and started implementing them into law.

On Oct. 16, 2000, the HIPAA Standards for Electronic Transactions (the Transaction Rule) became effective and require all affected health care providers and other "covered entities" to comply with the standards within two years (by October 16, 2002).

The HIPAA Security and Electronic Signature Standards (the Security Rule) were proposed by HHS in August 1998, but have not yet been finalized. Although the Security Rule was supposed to be finalized before the end of 2000, the Clinton Administration failed to do so before leaving office. Since the Bush administration's regulatory priorities are unclear, no one knows when final regulations for the Security Rule will be published, although there is little doubt that they will eventually be implemented. The Security Rule is an important component of Part C because it supplies the necessary guidance on how to implement the general security measures of the new HIPAA privacy standards (the Privacy Rule).

Both the Transaction Rule and the proposed Security Rule are heavily focused on information technology (IT)—the computer and network systems used to generate, store, and transmit information in electronic form. The Transaction Rule deals almost exclusively with electronic data, although the manu-

al (paper) collection of information, intended ultimately for computer input, will probably be indirectly affected, particularly by the rule's provisions governing direct data entry. The proposed Security Rule addresses issues of physical security (e.g., building access, computer terminal location, and the storage of electronic media), and will probably be expanded to address the security of paper records to accommodate this corresponding expansion of scope in the final, correspondingly expanded, Privacy Rule.

In their present forms, there are inconsistencies between the proposed Security Rule and the final Privacy Rule concerning who is covered by these rules, what information is covered, and other less substantive areas. HHS will probably harmonize the final Security Rule with the final Privacy Rule to eliminate these inconsistencies and achieve the "perfect fit" that was originally envisioned.

Another way of looking at how all of these HIPAA pieces work together is to think of the Transaction Rule as the technical "how to" instructions for working with electronic health information, the Privacy Rule as the policy guiding just what health care entities can and cannot do with health information, and the Security Rule as the guide on how to enforce the Privacy Rule by keeping information safe from unintended uses or disclosures. Since plenty of energy is already focused on the policy portion of the Privacy Rule, this article will focus instead on the Transaction and Security Rules and how to comply with their requirements.

IS MY ORGANIZATION SUBJECT TO THESE RULES?

Many of the rules under HIPAA have their own definition of covered entities, so there is no simple answer. In the Transaction Rule, covered entities consist of health plans, health care clearinghouses, and health care providers who transmit health information electronically in connection with a transaction named in the rule. In the proposed Security Rule, the definition of health care provider is broadened to include providers who process or maintain electronic health information used in any electronic transmissions, not just those named in the Transaction Rule.

"Health care" and "health care provider," however, have definitions under the rules that do not necessarily reflect the common understanding of those terms. How will you know if you are truly a covered entity subject to compliance with the rule? Start by determining whether you provide health care services or products by prescription, and whether you conduct (or pay a service provider to conduct) any of the listed transactions electronically. If you answered yes to both questions, you are most likely a covered entity and subject to the HIPAA rules.

Community oncology programs and oncology private practices that provide treatment services directly to patients, whether other physicians or providers are involved or not, are covered entities under the Transaction Rule if they electronically conduct at least one of the transactions named in the rule. They constitute a covered entity under the Security Rule if they maintain any protected information in electronic form.

COMPLYING WITH THE TRANSACTION RULE

A health care provider is a covered entity (for purposes of the Transaction Rule) only if it engages in one of the following transactions:

- Health care claims or equivalent encounter information
- Health care payment and remittance advice
- Coordination of benefits
- Health care claim status
- Enrollment and disenrollment in a health plan
- Eligibility for a health plan
- Health plan premium payments
- Referral certification and authorization
- First report of injury
- Health claims attachments
- Others as prescribed by regulation by the Secretary of HHS.

Compliance with the Transaction Rule requires that the covered entity conduct the named transactions using the standards for transmissions and the code sets that HHS has named in the rule. HHS has delegated the responsibility for setting and maintaining such standards to independent private organizations called DSMOs (Designated Standards Maintenance Organizations).

The DSMOs publish and maintain Implementation Guides that are incorporated by reference into the HIPAA Transaction Rule. In general, a covered institution's or practice's IT department must follow the Implementation Guides published by the various DSMOs exactly as they are written if and when a covered institution or practice conducts any of the named transactions electronically. If your organization does not conduct a given transaction electronically, you do not need to comply.

If data are being directly entered into a health plan's system (instead of being electronically transmitted), the covered institution or practice does not have to comply with standard format requirements, but data content must conform to the rule's requirements.

For example, an oncology center that collects coordination of benefits information from a patient using a form on its web site does not have to design the form to follow the Transaction Rule format. However, the form must have fields for the same data required by the Transaction Rule, and must adhere to the same data conditions required by the rule if the online form will feed data directly into the payer's system. This means that if a certain data element is mandatory in the transaction standard, it must also be mandatory in the online form. Similarly, if the data element is mandatory only under certain circumstances, it is mandatory under those same circumstances in the online form. Even if the form does not directly feed data into the payer's system and compliance with the rule's standards is not mandatory, the center may want to include standard data elements and conditions of use simply to avoid costly duplicative efforts if the data are transmitted to another entity who conducts the transaction electronically.

Table 1 shows transmission standards for (among others) pharmacy and health care claims and other types of transactions identified by HHS. The standard code sets identified by HHS for use in the named transactions are the International Classification of Diseases 9th Edition, Clinical

Modification (ICD-9-CM)(Vols. I-III), National Drug Codes (NDC), Code on Dental Procedures and Nomenclature, and the Health Care Financing Administration Common Procedure Coding System (HCPCS) (CPT-4) (for services, products and supplies including medical supplies, orthotic and prosthetic devices, and durable medical equipment).

The adoption of these transaction standards and standard code sets will result in the elimination of about 400 format and content requirements for submitting claims to insurers. The non-standard and "local" codes assigned by insurers, the UB-92 and HCFA 1500 claims forms, and the HCFA-assigned "J" drug codes will also be eliminated. These are specific examples of the way HIPAA plans to simplify the administration of health care, and indicates how costs will be saved by implementing the HIPAA rules.

Table 1: Transaction Standards Identified by HHS

Transaction	Standard
Health care claims or equivalent encounter information[1]	ASC X12N 837
Health care payment and remittance advice[1]	ASC X12N 835
Coordination of benefits[1]	ASC X12N 837
Health care claim status	ASC X12N 276/277
Enrollment and disenrollment in a health plan	ASC X12N 834
Eligibility for a health plan[2]	ASC X12N 270/271
Health plan premium payments	ASC X12N 820
Referral certification and authorization	ASC X12N 278
First report of injury	To Be Determined
Health claims attachments	To Be Determined
Others as prescribed by the Secretary via regulation	To Be Determined

[1]Pharmacy drug claims, NCPDP Telecommunication Standard Implementation Guide 5.1; and Batch Standard Implementation Guide 1.1

[2]Pharmacy drug claims, NCPDP Telecommunication Standard Implementation Guide 5.1; and Batch Standard Implementation Guide 1.0

COMPLYING WITH THE SECURITY RULE

The proposed Security Rule would apply to any health information "pertaining to an individual that is electronically maintained or electronically transmitted." Health information is defined as any information created or received by a covered entity that relates to the past, present, or future physical or mental health or condition of an individual; provision of health care for an individual; or the past, present, or future payment for health care for an individual.

Oncology centers that maintain any of this information electronically would be subject to the Security Rule's provisions for safeguarding such information.

It is important to remember that the Security Rule, as presently proposed, will apply to providers if they conduct any electronic transactions or transmissions that involve protected information, not only those conducted in standard format. The definition of "electronic" is very broad and includes voice recordings and data transmitted over phone lines, including the Internet and faxes.

The proposed Security Rule is intentionally "technology-neutral." HHS recognizes that the information technology industry is constantly evolving, and knowingly refrained from naming any specific IT security methodologies or tools to permit the use of new security technologies as they emerge.

The proposed Security Rule requires a covered entity to assess its own security needs and risks and to devise, implement, and maintain appropriate security measures consistent with its business functions in four major categories: 1) administration, 2) the physical, 3) technical services, and 4) technical mechanisms.

Administration. To meet the HIPAA Security Rule's administrative requirements a program must:

- Obtain a certification that the entity's computer systems/networks are in compliance with a pre-specified set of security requirements before the entity can be accredited
- Put chain-of-trust partner agreements in place to protect the integrity and confidentiality of individually identifiable health information exchanged between entities
- Have a contingency plan that secures and recovers protected information if the computer system/network fails or there is some other catastrophic loss of data
- Document policies for the processing, storage, and handling of protected information
- Provide information access controls with several levels of authorization to accommodate the different types of personnel who need to use protected information
- Have internal audits to spot and correct potential security risks
- Put in place personnel security measures (such as background checks and security clearances) and related policies/procedures
- Take measures to manage the system's security configuration such as documentation, hardware/software implementation and testing, asset management, and virus checking
- Have security incident procedures that include tracing the source of the incident, correcting the problem, appropriate responses, and accurate incident tracking
- Have security management (including risk analysis) decision-making, rules, and policies
- Develop personnel termination procedures that ensure that former employees no longer have access to protected information
- Have personnel training programs on all security policies and procedures.

Physical Measures. The Security Rule's requirements for physical measures include:

- Assigning one individual to manage and supervise the use of security measures and the conduct of personnel
- Controls to govern the use,

handling, and storage of protected information stored on any tangible media (i.e., locked storage cabinets for data stored on tapes or CDs)
- Controls for physical access to the entity's facilities and systems such as electronic ID badges, biometric security locks, and keypad access controls
- Policies and guidelines on workstation use such as guidance on PC placement to restrict unauthorized individuals' visual access to the PC screen, and time-out mechanisms to ensure that information is not displayed for extended periods of time if an employee walks away from a PC
- Secure workstation locations to prevent physical access by unauthorized people
- Training to enforce all of these policies and procedures.

Technical Services. Technical services include the following requirements to guard against unauthorized access to stored data:
- Access controls in which context-, user-, or role-based rules are embedded in computer system software to tell the computer system who can access what information
- Audit controls that include computer software tools that track who is accessing what information at any given time and keep a record of that access
- Authorization controls which prevent inappropriate authorizations to access-protected information from being issued
- Data authentication that allows software tools to verify the integrity of protected data and ensure that such data have not been modified by any unauthorized person
- Entity authentication that allows software tools to verify the identity of the person using the computer system.

Technical Mechanisms. The Security Rule has flexible guidelines for the protection of transmitted data, referred to as technical mechanisms. If a covered institution uses communications or network controls, the Security Rule requires that it use transmission integrity or message authentication plus access controls or encryption to guard against unauthorized access to data transmitted via a communications network. If the institution uses open network controls (to control transmissions over the Internet, for example), it must use the following software tools: alarms, audit trails, entity authentication, and event reporting.

Again, it must be emphasized that the Security Rule has not been finalized. Although no major changes were anticipated under the Clinton administration, it is impossible to foresee at this point whether the Bush administration will make major or minor modifications in the final rule. Although the Security Rule is not final, it may still be beneficial to assess how close or far your organization would need to go to come into compliance.

Patients to Share Billion Dollar Bill for HIPAA Compliance

Compliance with the new Health Insurance Portability and Accountability Act (HIPAA) will probably cost every American receiving health care as much as $200 over the next three years, according to some estimates. Since HIPAA mandates uniform electronic patient information and higher patient information privacy standards, the cost of meeting these standards will most likely be passed along to health care recipients.

Blue Cross estimates $42 billion as the cost for it to comply with HIPAA regulations. The American Hospital Association believes it will take $22 billion for hospitals to satisfy the law, while the U.S. Department of Health and Human Services estimates a more modest tab of $6 billion.

TAKING THE FIRST STEPS

You must assess your organization to determine how its current practices, policies, and systems measure up to requirements of the Transaction and Security Rules. First, determine which of the transactions named in the Transaction Rule your organization is currently conducting. Next, identify health information protected by the Security Rule within your system. A helpful exercise is to diagram the flow of individual health information 1) within your organization, 2) entering your organization from third parties, and 3) exiting your organization to third parties. Identify everything that comes in contact with protected health information on the diagram: computers, computer networks, network devices, databases, storage media, physical facilities, third parties, and internal departments (including the type of departmental staff). You should also collect existing policies and procedures that cover the security of your facilities, your computer systems, and stored health information. You may also want to confer with payers and others with whom you exchange protected information and/or conduct protected transactions.

Once this information has been gathered, you are ready to prepare a preliminary assessment of how your current practices measure up to HIPAA requirements. Where are the gaps between your current policies and practices and what the rules require? There are many professional advisors, including lawyers and technical consultants, who can help you with this analysis.

Once these gaps have been identified, you must develop and implement solutions to fill them and bring you into compliance with HIPAA standards. Developing a compliance plan will be much like developing any other project plan for your business. In particular, anything that is required by the Transaction Rule can be managed much like other IT implementations, although the solutions must be legally compliant as well as technically functional.

Effectively implementing the HIPAA rules will require more than technical solutions, however. It will require shifts in the culture of your office. Your staff must learn to think of protected information in a different way. Adhering to HIPAA standards must become automatic and be fully integrated into all the daily activities of your practice.