Holland & Hart

John Husband

Senior Partner
303.295.8228
Denver
jhusband@hollandhart.com

Navigating the HIPAA Privacy Standard Consent and Business Associate Provisions

Navigating the HIPAA Privacy Standard Consent and Business Associate Provisions

Insight — 11/25/2001 12:00:00 AM

Introduction
The final health care privacy standards, released by the Department of Health and Human Services (DHHS) in late December 2000, are confusing to say the least. The premise of the rule is simple -- a patient's medical record should remain private. Maintaining that privacy while allowing a provider to furnish quality care is not simple. Consequently, preparing to implement these standards will take a great deal of time. The April 2003 deadline is not as far off as it seems. Providers who do not act well before this deadline will not be ready.

While many states have their own medical record confidentiality statutes, Congress mandated additional protection as part of the Administrative Simplification provisions of the 1996 Health Insurance Portability and Accountability Act (HIPAA). The basic premise of Administrative Simplification was to create standardized electronic formats for healthcare functions such as including billing and claims submission. This would necessitate electronic submission of medical information about a given patient. The perceived vulnerabilities of electronic submissions led Congress to require the development of federal privacy standards.

The federal standards were designed to protect an individual's medical record, called "private health information" (PHI). They apply to any "health care provider who transmits any health information in electronic form in connection with a transaction," such as payment for healthcare services, healthcare claims, etc. If a provider does not have electronic capability, but employs an outside entity to make the electronic transmission, by extension, the rule applies to that provider.

Consent to Use and Disclose PHI
When a provider sees an individual for the first time, unless that individual is mentally or physically incapacitated, the provider must obtain a signed consent. The consent enables the provider to use and disclose the individual's PHI for treatment, payment and health care operations purposes. It also indicates the individual's awareness of the provider's privacy practices. These practices must be outlined in a separate notice that must be furnished to the individual. A provider may refuse to treat an individual who refuses to sign a consent.

Consent for Treatment Purposes
Once signed, the patient's PHI may be shared with the provider's employees and others who are involved in the patient's treatment. These uses and disclosures should be listed in the provider's privacy notice.

Consent for Payment Purposes
The consent also allows the provider the seek reimbursement from the patient's

insurer or other third party payer. Without this consent, the provider cannot transmit the necessary information to substantiate and receive payment.

Consent for Health Care Operations
The ability to use PHI for health care operations is vital to the provider's business viability. It includes many administrative activities such as 1) quality assessment and improvement; 2) training programs; 3) compliance and other legal or audit reviews; and 4) business development.

The Business Associate
The patient's consent allows the provider to share PHI with others who, while not having a treatment relationship with the patient per se, may need the information to support the provider's healthcare operations. These entities, called "business associates," furnish legal, actuarial, accounting, consulting, management, administrative accreditation, data aggregation, and financial services to the provider. Because business associates are not employees of the provider and, thus, are not under the provider's direct control, the provider must ensure that the business associate also maintains the patient's privacy. To that end, the provider and business associate must enter into a "business associate contract" before the PHI can be disclosed. The federal standards list the requisite elements of the contract.

A Provider's Liability for Breaches by a Business Associate
A provider is not required to actively monitor its business associates; however, it must investigate any complaints or other credible information inferring a violation by the business associate. "Reasonable" steps must be taken to correct any actions taken by the business associate that may breach a patient's privacy. This may include terminating the contract if feasible. If terminating the contract is not feasible, the provider must report the problem to the DHHS Secretary.

When a Business Associate Contract is NOT needed
If a nursing home patient needs hospital care, the nursing home can disclose the patient's PHI to the hospital because the hospital is providing treatment to the patient. A business associate contract between the nursing home and the hospital is not necessary. However, the hospital must obtain a signed consent as soon as practicable for its own treatment, payment, and healthcare operations purposes.

When an inpatient is being discharged to another facility or a home care provider, the hospital or physician may need to disclose PHI to that post-hospital provider. Again, since the post-hospital provider is furnishing care to the patient, a business associate contract between the hospital and the post-hospital provider is not necessary. The post-hospital provider must obtain a consent for its services as soon as practicable.

When a Business Associate Contract MIGHT be Needed
Institutional providers such as nursing homes and hospitals need temporary nursing staff to fill vacancies caused by illnesses, vacations, etc. The provider may employ individuals who hold themselves out as independent contractors or use the services of a nursing staff agency. Since the temporary nurse is providing treatment to the patient, a business associate contract is not necessary. However, if the agency is involved in the temporary nurse's work at any level -- i.e., providing insurance coverage, billing the hospital for the nurse's time -- a contract between the agency and the institution may be appropriate. This is a case-by-case circumstance that must be determined by the provider with input from the provider's legal counsel.

When a Business Associate Contract IS Needed
When conducting a reimbursement audit, a "health care operation," a facility may seek to hire an outside auditor. The facility and auditor must have a business associate contract to ensure patient privacy while the auditor reviews charts.

During a billing compliance audit, errors or fraud may be discovered. Alternatively, a government auditor may initiate an investigation. In either case, a provider's outside legal counsel may need access to medical records to ensure adequate representation. A business associate contract must be in force between the provider and the legal counsel so that the PHI can be disclosed.

If a provider is sued for malpractice, the provider's outside legal counsel will probably need the plaintiff's medical record to prepare a defense. Again, a business associate contract must be in force between the provider and legal counsel so that the PHI can be disclosed.

What's Next - Starting the Implementation Process
Of course, there are many more requirements regarding consent, business associate contracts and patient privacy. Moreover, there are many aspects of these provisions that remain open to individual interpretation. Additional clarifying rules are expected to be published before the standard's April 2003 effective date.

Nevertheless, providers should begin implementing the federal standard now. Implementing all of the requirements of the privacy standards will be a mammoth undertaking if providers attempt to implement everything at once. It is best to break things down. Create an outline of the actions needed before April 2003 with a timeline for completing each action. For example, set a timeline to:

1. Begin to sensitize staff to the overall requirements of the federal privacy standard so that they may become accustomed to the new rules long before the effective date.

2. Review current business relationships.

    a. Is an outside auditor, legal counsel, staffing agency, etc., being used currently?
    b. Can existing contracts be amended to incorporate the required elements of the business associate contract?
    c. Are additional contracts needed?

3. Begin to draft the privacy notice outlining the provider's privacy practices and consent form.

    a. Remember, these must be separate forms.

Breaking down the implementation steps will give providers a clearer picture of any outstanding needs and enable them to establish the next set of implementation steps.
