Managing HIPAA as Gatekeeper

Save to myBoK

by Margret Amatayakul, MBA, RHIA, CHPS, FHIMSS

An unfortunate result of the HIPAA privacy rule is the emerging use of HIPAA as a gatekeeper, restricting the appropriate fl ow of protected health information (PHI). HIPAA is being cited as a reason not to disclose information without patient permission when needed for treatment, payment, or healthcare operations (TPO). This situation could have untoward results for patient care and negative public health implications and could derail efforts to adopt a national health information infrastructure.

Although some providers are beginning to take a more reasonable approach, most have reverted back to requiring an authorization for disclosure, even when a clear treatment relationship exists. While this may seem like the safest approach and may be required in certain states, there are situations where a written authorization is impractical or even unsafe. This article is intended to offer suggestions for avoiding using HIPAA as a gatekeeper.

The HIPAA privacy rule is a massive regulation, often open to interpretation. Significant changes from the proposed to final rule, a modification of the final rule, and then special guidance has not necessarily made it more manageable. In addition, authorizations for release of information and rights to access health information prior to HIPAA were not consistent between hospitals and physician offices or from state to state. In some cases, the state pre-emption analysis performed for HIPAA revealed that providers were not even following state statutes as they were supposed to prior to HIPAA.

Understanding the Terminology

Perhaps part of the confusion surrounds terminology. HIPAA uses terms in very specific ways that may not have always reflected common usage in the past.

Authorization—There is no specific definition of authorization in either the proposed or final rule. However, based on its use in section 164.508, authorization means a written document wherein the subject of the protected health information, or subject's personal representative in accordance with section 164.502, may provide agreement that PHI may be used or disclosed. Authorization is required except as otherwise permitted or required by HIPAA. As many as 16 exceptions are described. In general, this definition is consistent with common usage.

Consent—There is no specific definition of consent in either the proposed or final rule. However, based on its usage in section 164.506, consent means permission for use or disclosure of protected health information. The requirement for consent does not state that it must be in written form, although it requires that it be in plain language. The consent requirement was significantly changed in the final rule, such that consent is *not* required for:

- Section 164.506(c)(1): Use or disclosure of PHI for its own treatment, payment, or healthcare operations
- Section 164.506(c)(2): Disclosure of PHI for treatment activities of a healthcare provider
- Section 164.506(c)(3): Disclosure of PHI to another covered entity or healthcare provider for the payment activities of the entity that receives the information
- Section 164.506(c)(4): Disclosure of PHI to another covered entity for healthcare operations of the entity that receives the information if each entity either has or had a relationship with the individual who is the subject of the PHI being requested; the PHI pertains to such relationship; and the disclosure is for conducting quality assessment and improvement activities (as defined by HIPAA), or reviewing the competence or qualifications of healthcare professionals, health plan performance, conducting training programs, accreditation, certification, licensing, or credentialing activities
- Section 164.506(c)(5): Disclosure of PHI by a covered entity to other covered entities in an organized healthcare arrangement (OHCA) for healthcare operations activities of the OHCA

References: Exceptions to the Rule

Another part of the confusion is that HIPAA's privacy rule often references multiple sections in any given standard. Sometimes these sections are explicit, other times they are general. The rule also often indicates that something may or may not be done, but lists only exceptions rather than permitted actions.

Absent any state requirement for authorization, is an authorization required to use or disclose PHI for TPO or not? The question may seem even less clear when combined with the verification requirements in section 164.514(h)(1)(i) that require a covered entity to verify the identity and authority of a person requesting PHI if the identity or authority of such person is not known to the covered entity. Still, this section references the ability to obtain oral representation of identity and authority.

Implications

While it is important to protect the privacy of patients or health plan members, it is equally critical to have information necessary for patient care, public health, and payment purposes. The following are a few current activities that are being designed to enhance quality of care and patient safety, streamline payment issues, and protect the public health that could be hindered by not having access to PHI when necessary:

- ASTM International is developing the Continuity of Care Record (CCR) standard. This is an outgrowth of the Patient Care Referral Form designed and mandated by the Massachusetts Department of Public Health for use primarily in inpatient settings. The CCR is designed to be used for all clinical care settings to provide a summary of a patient's health status (e.g., problems, medications, allergies) and basic information about insurance, advance directives, care documentation, and care plan recommendations. To ensure interchangeability of electronic CCRs, the standard employs XML coding that permits preparation, transmission, and viewing in a browser, as an element in an HL7 message or CDA compliant document, in a secure e-mail, as a PDF file, as an HTML file, or as a word processing document. In some cases, patients may directly control the flow of their CCR; however, it could also be transmitted among referring physicians, used as a transfer record for long-term care, or be exchanged by pharmacy benefits managers to support a patient's medication history.
- E-prescribing is gaining considerable momentum after standards for transmission of electronic prescriptions were called for in Public Law 108-173 Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (a.k.a. Medicare Modernization Act [MMA]). Specifically, MMA requires that after a date to be specified by the Secretary of the Department of Health and Human Services, prescriptions for drugs covered under MMA part D that are transmitted electronically shall be transmitted only in accordance with standards meeting the government's requirements (to be recommended by the National Committee on Vital and Health Statistics [NCVHS]), including providing for the electronic transmittal to the prescribing healthcare professional and dispensing pharmacy.
- Initiatives by President Bush have included a health and IT subcommittee of the President's Information Technology Advisory Committee (PITAC), which was chartered by Congress under Public Law 102-194, the High-Performance Computing Act of 1991, and Public Law 105-305, the Next Generation Internet Research Act of 1998. On April 13, 2004, this subcommittee outlined recommendations for electronic health records, clinical decision support, electronic order entry for both outpatient care and within the hospital environment, and secure, private, interoperable health information exchange in order to lower cost, reduce errors, and provide higher quality healthcare. On April 26, 2004, Bush announced a 10-year health information technology plan to accelerate broader adoption of health information technology, which included creating a new subcabinet national health information technology coordinator position, adoption of standards for transmitting x-rays, lab results, and prescriptions over the Internet, funding for demonstration projects, and using the federal government to foster adoption of health information technology.
- The concept of a national health information infrastructure (NHII) has been discussed for several years. In November 2001, the NCVHS outlined a vision and process for building the NHII that would use information technology to enhance connectivity and knowledge sharing, foster collaboration, encourage capital investment, give the federal government a leadership role, use evidence of effectiveness to guide the future of the US healthcare system, and provide incentives for collecting data electronically.

All of these initiatives, including local and regional health information infrastructures that are emerging today, require the appropriate exchange of PHI.

Recommendations

In addition to fully understanding the HIPAA requirements and your state statutes, it is important to provide clear guidance on requirements for uses and disclosures, as well as security measures to provide authentication and protection of data confidentiality, integrity, and availability. Even this column could serve as a reminder of the importance of appropriate exchange of PHI.

Margret Amatayakul *(margretcpr@aol.com) is president of Margret\A Consulting, LLC, an independent consulting firm based in Schaumburg, IL.*

Article citation:
Amatayakul, Margret. "Managing HIPAA as Gatekeeper" (HIPAA on the Job Column). *Journal of AHIMA* 75, no.8 (September 2004): 68-69.