Confusion Continues over HIPAA's Minimum Necessary Standards

by Sheri Hutchins, MA, RHIA, CCS

Nearly five years after its implementation, HIPAA's minimum necessary standards continue to be problematic for many organizations. A recent report released by the Agency for Healthcare Research and Quality confirms the ongoing confusion over interpretation of the requirement.[1]

The report, based on state-level research from the Health Information Security and Privacy Collaboration (HISPC) project, recommends communication and collaboration from the state to the national level to resolve the confusion. HIM professionals must ensure that release of information processes both facilitate quality care and comply with federal and state regulations.

Minimum Necessary Confusion

The HIPAA privacy rule allows covered entities considerable flexibility in their adoption of policies, procedures, and business practices. Other state and federal privacy laws and regulations also tend to be written broadly to facilitate flexibility in implementation.

While such broad generalization is desirable given the diversity of healthcare organization size, structure, and operation, it has had the unintended effect of generating significant variation in the application of the privacy rule and state law.

The state teams in the HISPC project sought to identify the variations in privacy rules and practices that create barriers to exchange of patient data. The most common source of variation they identified was the interpretation and application of the minimum necessary standard. The teams reported widespread variation in how the standard was understood and applied.

Organizations struggle in determining the appropriate level of information that should be provided to satisfy this standard. Furthermore, organizations found it difficult to apply the standard regardless of whether the release of information was between organizations or within the same organization.

HIPAA Minimum Necessary Requirements

HIPAA regulations mandate that a covered entity must make "reasonable efforts" to limit use and release of protected health information to the "minimum necessary to accomplish the intended purpose of the use, disclosure, or request." Therefore a request for information must be validated and the accurate data specified before a patient's information can be released.

There are three types of release of information:

- **Internal disclosures,** in which providers identify levels of information to be disclosed based upon job description and need-to-know basis (e.g., nurse versus custodial personnel request)
- **Routine disclosures,** in which providers release protected health information based upon policy that limits the amount of information disclosed in order to meet the purpose of the disclosure (e.g., health provider request).
- **Nonroutine disclosures,** in which providers assess requests based on detailed request information. Requests must be reviewed on an individual basis (e.g., medical licensing review board request).[2]

The table [below] outlines the different release of information requirements under HIPAA. Organizations should develop policies regarding these regulations that they use consistently to promote HIPAA compliance. Federal regulations and Office for Civil Rights guidelines serve as definitive sources for HIPAA information.

HIPAA Release of Information Requirements

Healthcare organizations are still struggling with the minimum necessary standard. A review of the regulations helps clarify the requirements surrounding release of information.

Summary of Requirement	Significance and Implications	
Minimum necessary 164.502 (b)	A covered entity must make "reasonable efforts" to limit use and disclosure of PHI to "the minimum necessary to accomplish the intended purpose of the use, disclosure, or request." This standard will not apply to disclosures between providers in the context of treatment, nor to disclosures to plan sponsors by health plans if the plan documents contain new language required by the rules.	The minimum necessary standard is one of the more burdensome elements of the regulations, but has become somewhat more reasonable in the final rule. The draft rules would have required case-specific examination of each element of each disclosure. The final rules permit policies to apply across staff classes in accordance with staff needs for the information, and disclosures that are made "on a routine and recurring basis" to be governed by protocols for determining the minimum information necessary. The standard would have been difficult if not impossible to apply among treating providers, as the draft rules would have required holding providers to a standard of complete knowledge of the outcome of a referral before they make the referral. The exemption of disclosures to plan sponsors reflects current practice in connection with disclosures by administrators to self-funded plans, but imposes a new "firewall" between the employer as plan sponsor and as employer.
Minimum necessary requirements 164.514 (d)	The final regulations retained the "minimum necessary" concept included in the proposed regulations. This requires disclosures of protected health information, even where authorized by the regulations, to be limited to the "minimum necessary" required to accomplish the purpose for which the disclosure is made. However, the final rule has considerably limited its applicability. The intent is to allow clinical processes to take place with free information flow, applying the minimum necessary standard primarily to business and financial processes. Thus the minimum necessary standard does not apply to requests by a provider for information relating to treatment, and the proposed rule requiring that each use and disclosure be individually reviewed has been broadened to allow role-based access according to protocols developed by the covered entity. In addition, the final regulations do not require this determination to be made when responding to a request from another covered entity. Instead, the covered entity requesting the information must limit its request to the information reasonably necessary to accomplish the purpose of the request, significantly lessening the operational impact of the minimum necessary requirement on the disclosing entity.	A covered entity must identify persons or classes of persons in its work force who need access to protected health information to carry out their duties and identify the categories of information to which they need access. Disclosures made on a routine and recurring basis may be based on standard protocols or policies and procedures that limit the amount of information disclosed. Requests between covered entities are streamlined significantly. The final regulations provide for a more workable approach to routine disclosures, whereby covered entities can use policies and procedures, program access levels into system security access modules according to job function, or develop algorithms to administer the requirement, instead of making each "minimum necessary" determination on an individual basis. Non-routine disclosures must still be reviewed individually, but in relation to criteria established beforehand by the covered entity. Determination rules can be made in advance, categorically, with review and comment; this also will have the effect of increasing the consistency of such determinations.

Source: Price Waterhouse Coopers. "Guide to the HIPAA Privacy Regulation." Available online at www.pwc.com/extweb/pwcpublications.nsf/docid/56B94EC68B95B755852572C1006C7C31.

Next Steps

Dealing with the existing knowledge gap over minimum necessary requires education and collaboration between states and national privacy and security efforts. Organizations throughout healthcare require clear direction in the application of the minimum necessary standard through consistent, regular, formal, and accurate education and communication.

HIPAA regulations that support privacy, security, and confidentiality procedures have changed public perception and accountability of how organizations manage protected health information. It is up to HIM professionals to ensure that release of information processes comply with regulations, facilitate effective patient care, and are provided in an efficient and cost-effective manner.

HIM professionals must embrace the challenge of promoting a continuum of patient care while remaining compliant with regulations and the needs of healthcare consumers. Complying with minimum necessary regulations provides a great foundation to achieve that goal.

Oklahoma's HISPC Activities

Oklahoma was one of the states that received a six-month extension to continue HISPC's efforts to implement solutions to certain privacy and security issues. The Oklahoma HISPC is focusing on three aspects of the proposed solutions:

- Establishing an interjurisdictional office of health information technology for the state of Oklahoma
- Developing a universal authorization to release form to apply across jurisdictional lines within the state of Oklahoma
- Participating in an interstate collaboration to research and develop processes to share healthcare consumer data

Defining and understanding minimum necessary guidelines will facilitate the universal authorization for release form process throughout the state.

Notes

1. Agency for Healthcare Research and Quality. "Privacy and Security Solutions for Interoperable Health Information Exchange." July 2007. Available online at http://healthit.ahrq.gov.
2. Office for Civil Rights. "Standards for Privacy of Individually Identifiable Health Information." April 2003. Available online at www.hhs.gov/ocr/hipaa/guidelines/guidanceallsections.pdf.

Acknowledgment

Harry B. Rhodes, MBA, RHIA, CHPS, CPHIMS, FAHIMA

Sheri Hutchins *(sherih@cableone.net) is an independent consultant from Marietta, OK.*

Article citation:
Hutchins, Sheri. "Confusion Continues over HIPAA's Minimum Necessary Standards" *Journal of AHIMA* 78, no.10 (November 2007): 66-67.