What's Next for the Privacy Rule? HIPAA for All, or Something Quite Like It

by Jill Callahan Dennis, JD, RHIA

The privacy rule is just six, but gaps in its coverage have already widened. Now some organizations are recommending that the rule—or something like it—expand to cover any organization that handles personal health information in any form.

Six years ago this month, the HIPAA privacy rule became effective for most of the US healthcare industry, and by April 14, 2003, compliance with the rule was expected. After much preparation, education, and more than a little consternation over uncertainties in the rule, newly minted privacy officers began administering covered entities' privacy programs, putting in place a variety of new systems to execute the intricacies of the rule's provisions.

There was much to celebrate in the privacy rule. It promoted greater patient access to their health information and codified a number of individual patient rights. It focused newfound attention on confidentiality and security issues within organizations and instituted training and awareness programs that built greater sensitivity.

There also were doubts about the value of some of the rule's provisions from the first day. Many people doubted the value of the accounting of disclosures, given that the kinds of disclosures most likely to be of interest to patients were the very kind that were not required to be documented in the accounting. HIM professionals, in particular, wondered whether patients would want to see the information the rule specified or if they were establishing complex tracking systems that provided little benefit to patients.

Many people also worried about the rule's approach to pre-emption, which defers to state law wherever it is more protective of the patient's rights or more restrictive in its privacy protections. They feared this would perpetuate the administrative complexity of a "patchwork quilt" of privacy protections, where the extent of one's privacy rights is an accident of geography rather than a uniform national standard.

Misinterpretations and a Lack of Integration

Several years later, the industry has seen some of its expected gains—and its fears—realized. Patients do seem more aware, generally, of their rights to access their health information. They know about HIPAA and what it seeks to accomplish.[1] They are asking more questions about privacy.[2] And they are exercising some of the rights HIPAA provides.

However, denial of patient access to their own health information is still a common complaint reported to the Office for Civil Rights. And, as expected by many HIM professionals, very few patients request an accounting of disclosures.[3] The industry still struggles with the ongoing need for pre-emption analyses as new state laws affecting health information are written.

On top of this, the industry has suffered from numerous variations in interpretation of the privacy rule's provisions and its relation to various state laws. Research by RTI International noted problems in the application of the privacy rule's provisions for authorizations and consents as well as confusion over the minimum necessary rule.[4] The report also documented widespread difficulties in understanding the interplay between 42 CFR Part 2 (regulations on confidentiality of alcohol and drug abuse information) and the privacy rule.

Even when considering just a single state's privacy laws, one can find health information privacy issues scattered throughout multiple chapters of laws, and when those laws are analyzed, they often conflict. To further complicate matters, the laws were most often written for a paper-based system and apply imperfectly to electronic health information.[5]

In February 2007 the Government Accountability Office (GAO) issued a report calling on the Department of Health and Human Services (HHS) to improve its efforts to protect the privacy and security of health information, particularly information in electronic form.[6]

The report cited several ongoing challenges: complications in sharing information between entities with different levels of privacy protection, problems in adherence to the "minimum necessary" requirement of the privacy rule (which attempts to limit certain uses and disclosures to only that information necessary to accomplish the purpose of the disclosure), and ongoing problems in patient understanding of their rights to access and amend their records.

GAO was asked by Congress to describe HHS's efforts to ensure privacy as part of its national strategy to build a nationwide network for the exchange of health information. GAO noted that, while progress has been made in HHS's strategy to protect health information, the efforts are not fully integrated or comprehensive.

For example, the privacy rule mandates that covered entities require their contracted business associate to implement certain privacy protections. However, covered entities are generally not liable for privacy violations of their business associates, and the HHS secretary does not have direct enforcement authority over any persons or organizations that are not covered entities as defined in the rule.[7]

As Times Change, the Gaps Widen

The fact that the privacy rule is only enforceable upon "covered entities" is a weakness that many have noted.[8,9] AHIMA, for one, has called for the establishment of uniform privacy legislation to ensure that all individuals are secure from the misuse of their personal health information wherever it is collected, utilized, transferred, or rests.[10]

The privacy rule defines covered entities as "a health plan, a health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter."[11] And while that definition covers a large number of organizations that use and disclose health information, it has not kept pace with new developments in healthcare.

At the time the privacy rule was written, regulators were not anticipating the development of new kinds of organizations with access to patient information, such as health information exchanges (HIEs) and personal health record (PHR) vendors. Neither an HIE nor a personal health record vendor is a covered entity under the privacy rule's definition (although participants in the exchange could be covered entities, and covered entities could offer personal health record applications).

As a result, the privacy protections mandated by the HIPAA privacy rule do not apply, and the HHS secretary has no authority to enforce the rule's provisions with those organizations that are not otherwise covered entities. In addition, as noted, there is no direct enforcement authority over the business associates of covered entities.

This gap in the privacy rule has the potential to weaken consumer confidence in the industry's ability to safeguard confidential information. Indeed, some consumer privacy groups have spoken specifically to this issue. The 2007 Privacy Principles issued by the Coalition for Patient Privacy call for the right to health privacy to apply to all health information regardless of the source, the form it is in, or who handles it.[12]

Two Recommendations on Broadening Protections

In June 2007 HHS received similar recommendations from two federal advisory groups. Both identified the emergence of new organizations that fell outside of the privacy rule's coverage, and they advised broader application of federal rules—HIPAA or otherwise—to protect personal health information in any format and any setting.

The concept of broadening protection for health information has been mirrored in bills introduced by state legislatures, as well. RTI research, conducted through 33 states and Puerto Rico under the federally funded Health Information Security and Privacy Collaboration, shows substantial interest in updating state laws to better protect patient information being handled and processed by health information exchanges.[13] (For more on this work, see the story "Harmonization Destination" by Chris Dimick.)

The AHIC CPS Workgroup

Recognizing that consumer trust is an essential building block in developing a nationwide health information network, the American Health Information Community (AHIC) of the US Department of Health and Human Services formed the Confidentiality, Privacy and Security (CPS) Workgroup in 2006. The broad charge to the group, which is staffed by the Office of the National Coordinator for Health Information Technology, is to make recommendations to the community regarding the protection of health information in order to secure trust and support appropriate interoperable electronic health information exchange. (Specific charges to the work group and the member list can be found online at www.hhs.gov/healthit/ahic/confidentiality.)

Among other issues, the CPS work group has taken up the issue of gaps in the protection of patient health information, and in June 2007, the group recommended that participants (excluding consumers) in electronic HIE networks should be required to meet enforceable privacy and security criteria at least equivalent to any relevant HIPAA requirements. The group also recommended that persons or entities functioning as business associates that participate in electronic HIE networks should also be required to meet such standards. (The work group's complete recommendations can be read in the sidebar below.)

AHIC CPS Workgroup Recommendation

All persons and entities, excluding consumers, that participate directly in, or comprise, an electronic health information exchange network, through which individually identifiable health information is stored, compiled, transmitted, modified, or accessed should be required to meet enforceable privacy and security criteria at least equivalent to any relevant HIPAA requirements (45 CFR Parts 160 and 164).

Furthermore, any person or entity that functions as a Business Associate (as described in 45 CFR §160.103) and participates directly in, or comprises, an electronic health information exchange network should be required to meet enforceable privacy and security criteria at least equivalent to any relevant HIPAA requirements, independent of those established by contractual arrangements (such as a Business Associate Agreement as provided for in HIPAA).

Source: Letter from Kirk J. Nahra, chair of the American Health Information Community Confidentiality, Privacy and Security Workgroup, to Michael O. Leavitt, chair of the American Health Information Community. June 12, 2007. Available online at www.hhs.gov/healthit/documents/m20070612/cps_letter.html.

The recommendation thus extends HIPAA or HIPAA-like requirements to a new class of entities—HIE participants—regardless of whether they are considered covered entities under the privacy rule. As the CPS work group notes, this represents an "important step in assessing the obligations that are appropriate for persons and entities participating in such a network that have responsibility for such valuable personal information."[14] The recommendations were accepted by AHIC and referred to the HHS secretary for consideration.

The work group has continued to examine which particular elements of HIPAA (or a HIPAA-like requirement) should apply to HIEs. A currently drafted set of recommendations would not apply all HIPAA requirements to HIEs, because many of those requirements are best applied at the covered entity level. However, the group is currently analyzing what, if any, additional confidentiality, privacy, and security protections should apply to these exchanges—in other words, whether any of the requirements for these exchanges should be "higher" or more stringent than those of the HIPAA privacy rule.

The recommendations would also extend to some noncovered entities offering PHRs. To the extent those records interface with electronic health information exchange networks, they would be subject to the CPS work group's recommendations. Just as they are doing with HIEs, the work group is analyzing what, if any, additional protections should apply to information contained within PHRs, and whether the privacy requirements for PHR data should exceed the present level of protections offered by the privacy rule.

To monitor the ongoing work of the CPS work group, visit its Web site at www.hhs.gov/healthit/ahic/confidentiality.

NCVHS

Joining the AHIC CPS Workgroup in calling for broader application of rules to protect personal health information is the National Committee on Vital and Health Statistics. In June 2006 NCVHS recommended to the HHS secretary that "HHS should work with other federal agencies and the Congress to ensure that privacy and confidentiality rules apply to all individuals and entities that create, compile, store, transmit, or use personal health information in any form and in any setting, including employers, insurers, financial institutions, commercial data providers, application service providers, and schools."[15]

Since issuing that recommendation, NCVHS held a series of hearings to learn more about the kinds of organizations and individuals that handle health information but are not covered entities under HIPAA. Some of these organizations and individuals are noncovered healthcare providers, such as athletic trainers and medical spas that do not submit claims for payment in electronic form.

Even more surprising was the finding that a number of organizations that are essential to the operation of a nationwide health information network fall outside the definition of covered entity, such as HIEs, regional health information organizations, record locator services, system integrators, and medical record banks.

As a result of the finding, NCVHS issued a new recommendation in June 2007 calling on HHS and Congress to pass laws and regulations that would ensure that all entities that create, compile, store, transmit, or use personally identifiable health information are covered by a federal privacy law. The complete recommendation can be found in the sidebar below.

NCVHS Recommendation

Recommendation: HHS and the Congress should move expeditiously to establish laws and regulations that will ensure that all entities that create, compile, store, transmit, or use personally identifiable health information are covered by a federal privacy law. This is necessary to assure the public that the NHIN, and all of its components, are deserving of their trust.

Source: Letter from Simon P. Cohn, chair of the National Committee on Vital and Health Statistics, to Secretary of Health and Human Services Michael O. Leavitt. June 22, 2006. Available online at www.ncvhs.hhs.gov/070621lt2.pdf.

More HIPAA Ahead?

Will we see an expansion of the HIPAA privacy rule? The development of new organizations not anticipated in the original rule and the recognition that consumer trust is a prerequisite to widespread HIE suggest that the privacy gaps must be closed somehow.

At a June 2007 AHIC meeting, Robert Kolodner, MD, national coordinator for health IT, presented a "privacy and security framework" to foster adoption of privacy and security practices that promote trust. The framework is intended to build consensus around principles that would guide the use and disclosure of health information in both the public and private sector. Kolodner described plans to build a harmonized set of principles around the following key themes:

- Accountability and oversight
- Limitations on data collection
- Data integrity and quality
- Enforcement and remedies for misuse
- Individual participation and control, access, and correction rights
- Openness and transparency
- Use limitation and consent and disclosure
- Security, safeguards, and controls

Whether these principles can be harmonized without broadening the reach of the privacy rule or requiring greater consistency of state laws and regulations remains to be seen. There certainly are risks to "opening up" the HIPAA privacy rule to changes. Modifications could introduce uncertainty into areas of the rule that have become successfully embedded in covered entity operations. And there is always a risk that changes could result in even more widespread misinterpretation of certain aspects of the rule.

But if the industry is to make progress in gaining public confidence in the confidentiality and security of personal health information, it seems clear that some changes, whether in the form of regulatory changes or in new legislation at the state or federal level, are in store.

Notes

1. Williams, Arthur R., et.al. "HIPAA Costs and Patient Perceptions of Privacy Safeguards at Mayo Clinic." *Joint Commission Journal on Quality and Patient Safety* 34, no. 1 (Jan. 2008): 27–35. Mayo Clinic patients surveyed indicated high levels of awareness about HIPAA, and 80 percent were able to answer six or more HIPAA questions correctly on a 10-question quiz.
2. AHIMA. "State of HIPAA Privacy and Security Compliance." 2006. The survey asked respondents "how are patients reacting to HIPAA privacy efforts?" Thirty percent of respondents indicated they are getting "more questions from consumers."
3. AHIMA. "On the Front Lines of Healthcare Privacy: An AHIMA Roundtable." 2007.
4. RTI International. "Privacy and Security Solutions for Interoperable Health Information Exchange: Nationwide Summary." July 2007. Available online at www.rti.org/pubs/nationwide_summary.pdf.
5. Dimitropoulos, Linda. "Privacy & Security Solutions for Interoperable Health Information Exchange." Report to the American Health Information Community. RTI International. March 13, 2007.
6. United States Government Accountability Office. "Health Information Technology: Early Efforts Initiated but Comprehensive Privacy Approach Needed for National Strategy," GAO-07-238, 2007. Available online at www.gao.gov/new.items/d07238.pdf.
7. Ibid.
8. Hoffman, Sharona, and Andy Podgurski. "In Sickness, Health, and Cyberspace: Protecting the Security of Electronic Private Health Information." August 2006. Bepress Legal Series. Working Paper 1522. Available online at http://law.bepress.com/expresso/eps/1522.
9. Fox, Steve, and Rebekah Monson. "HIPAA and Foreign Outsourcing." HIPAA/LAW, February 2004. Available online at www.hipaadvisory.com/action/legalqa/law/Legal44.htm.
10. AHIMA. "Statement on Confidentiality, Privacy and Security of Health Records." December 2007.
11. HIPAA, Public Law 104-191, 45 CFR §160.103.
12. Coalition for Patient Privacy. 2007 Patient Privacy Principles. Available online at www.patientprivacyrights.org/coalition.
13. RTI International. "Privacy and Security Solutions for Interoperable Health Information Exchange: Nationwide Summary."
14. Letter from Kirk J. Nahra, chair of the American Health Information Community Confidentiality, Privacy and Security Workgroup, to Michael O. Leavitt, chair of the American Health Information Community. June 12, 2007. Available online at www.hhs.gov/healthit/documents/m20070612/cps_letter.html.
15. Letter from Simon P. Cohn, chair of the National Committee on Vital and Health Statistics, to Secretary of Health and Human Services Michael O. Leavitt. June 22, 2006. Available online at www.ncvhs.hhs.gov/070621lt2.pdf.

Jill Callahan Dennis *(jill.dennis@ahima.org) is senior vice president of public and industry leadership at AHIMA and a member of the AHIC Confidentiality, Privacy and Security Workgroup.*

Article citation:
Dennis, Jill Callahan. "What's Next for the Privacy Rule? HIPAA for All, or Something Quite Like It" *Journal of AHIMA* 79, no.4 (April 2008): 24-29.