Examining Data Rights in Vendor Contracts: Privacy Obligations Extend to the Terms Negotiated in External Contracts

by Bonnie S. Cassidy, MPA, RHIA, FAHIMA, FHIMSS

Preparing for HIPAA implementation created a new level of excitement and focus on privacy and confidentiality as healthcare organizations developed appropriate compliance programs. New positions and roles for security and privacy officers were created; new enterprise privacy and security education programs, policies, and procedures were developed.

As organizations focused on their internal processes and procedures, not all gave sufficient review to their external agreements with vendors. Organizations unfamiliar with the data rights and data ownership language in their health IT contracts can find that those agreements may compromise the privacy of their patients' personal information.

This has become especially true as technological advances have created new products, services, and entities related to health information not envisioned at the time HIPAA went into effect. At a 2007 meeting of the National Committee on Vital and Health Statistics (NCVHS) Subcommittee on Privacy and Confidentiality, Paul C. Tang, MD, spoke of the many "egregious violations" he has witnessed. "It is a changed world just in the past one year or two years," he said. "There are vendors that are obligating covered entities to do things that they are not allowed to do."[1]

Congress enacted HIPAA to cover the electronic transmission of certain health information, but the US lacks a national privacy policy. Significant movement for HIPAA compliance and enforcement has been lacking. The Office for Civil Rights was given responsibility for enforcing HIPAA, but it does not have authority over all entities that handle personal health information. Vendors, or the business associates of those healthcare entities covered by the privacy rule, are a notable example.

Business associates work on an organization's behalf, such as transcription services and consultants who review medical records and clinical documentation. An organization cannot assume that a signed business associate agreement guarantees HIPAA compliance. Compliance programs should include an evaluation of business associate agreements as well as an ongoing review of contracts.

PHRs a Special Concern

Danger spots in contracts often revolve around the vendor's rights to the health data it handles. Ownership of data is not consistently applied in the healthcare industry, and all providers must be cautious and make every effort to protect the rights to data use in the contract language. For example, a business associate could request real-time access to an organization's database, exclusive access to the data, and the rights to resell the information.

Such deficiencies appear in contracts for all types of products and services. Tang, quoted on a different occasion, noted that the risks appear in contracts for both inpatient and outpatient systems as well as in the privacy statements of personal health record systems providers.[2]

PHRs present a special concern because providers may be independent—not associated with a covered entity—and not governed by HIPAA privacy rules, even indirectly.

"There are more and more of these [PHRs], and they are outsourced to a company that is not a covered entity and they believe there is some financial potential of accessing that asset," Tang said. "One of the ways that [PHR] companies get around their responsibilities is put their disclosure in the 'I agree' statement that nobody reads. Is that fair practice? It's a little bit of buyer beware."[3]

Secondary Uses Require Close Study

A lack of national standards has created a gray area for associated uses of data. Entities with access to data can be sources of the secondary uses of that data, creating risk. Contracts must directly establish the acceptable uses of patient data.

Existing and potential sources of data for secondary use include:

- Public use data sets (e.g., Medicare, Medicaid, Centers for Disease Control surveys, some primary data use such as the National Health and Nutrition Examination Survey)
- Private data sets (e.g., open-source data, commercial use data sets at the patient level, pharmacy benefit and claims manager, provider databases, individual providers, aggregated data from provider consortia)
- Consortium databases such as university health systems consortium
- Aggregated clinical repositories hosted by health IT vendors
- Personal health records, including patient-entered data
- Health information exchanges[4]

Broader Privacy Coverage Recommended

Are there recommendations on the table that HIM professionals should be aware of? Most definitely. At least one current proposal would extend privacy regulations to cover any organization or individual that handles personal health information in any form.

In June 2006 the NCVHS privacy subcommittee submitted 26 policy recommendations to the secretary of Health and Human Services. In particular, one states:

> 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.[5]

In effect, privacy protections would follow the data and not be limited to a group of defined users as it is now under HIPAA. Such a provision would require that a vendor follow the same regulations that the provider operates under.

Testifying before the Confidentiality, Privacy and Security Workgroup of the American Health Information Community, Cassi Birnbaum, RHIA, CPHQ, reported on similar recommendations put forth by the California health information exchange collaborative CalRHIO:

> There was definitely consensus among the stakeholders that privacy and security protections should be applied to healthcare information, not the entities handling the data. If this were the case, providers, other covered entities, and consumer concerns would be addressed and the risks of improper disclosure would be greatly mitigated. As it relates to national health information exchange and the hosting of personal health records, the HIPAA privacy and security regulations should be the floor, with additional protections layered on if deemed necessary.[6]

Protecting health information is of the utmost importance, and it is essential to the success of interoperable electronic health information exchange. Proper policies that ensure trust in emerging systems must evolve in step with technology advancements. HHS has invested in multiple coordinated initiatives to ensure health information will be protected as we enter this new era of healthcare.[7]

HIM professionals can respond to these compliance risks by performing a HIPAA compliance audit of their organizations' vendor contracts. They can seek industry solutions by promoting the creation of laws that govern the use and disclosure of all healthcare data and hold accountable everyone who has access to that data.

Notes

1. "Transcript of the January 23, 2007, NCVHS Subcommittee on Privacy and Confidentiality Hearing." Available online at www.ncvhs.hhs.gov/070123tr.htm#introduction.
2. Conn, Joseph. "IT Guru Says Some E-Vendor Contracts Violate Privacy." *Modern Healthcare*, July 19, 2007.
3. Ibid.
4. American Medical Informatics Association. "Secondary Uses and Re-Uses of Healthcare Data: Taxonomy for Policy Formulation and Planning." September 2007. Available online at www.hhs.gov/healthit/documents/m20071113/07b-amia.pdf.
5. National Committee on Vital and Health Statistics. "Privacy and Confidentiality in the Nationwide Health Information Network." June 2006. Available online at www.ncvhs.hhs.gov/060622lt.htm.
6. Birnbaum, Cassi. "Testimony to AHIC CPS Work Group." June 2007. Available online at www.hhs.gov/healthit/ahic/materials/06_07/cps/calrhio.html.
7. "Protecting Patient Privacy in Healthcare Information Systems." Testimony of Robert M. Kolodner, MD. June 19, 2007. Available online at www.hhs.gov/asl/testify/2007/06/t20070619b.html.

References

American Health Information Community, Consumer Empowerment Workgroup. Letter to Michael Leavitt, chair of the American Health Information Community. January 23, 2007. Available online at www.hhs.gov/healthit/documents/m20070123/ce_letter.html.

Cassidy, Bonnie. "Conducting Your Own Internal Assessment." *Journal of AHIMA* 71, no. 5 (May 2000): 16A–D.

Cohen, Michael, and Margret Amatayakul. "Who's Using Your Data?" *Advance for Health Information Executive*. Available online at http://health-care-it.advanceweb.com/Editorial/Content/Editorial.aspx?CC=94753.

Department of Health and Human Services (HHS), Office for Civil Rights. "HIPAA Privacy Rule: Disclosures for Emergency Preparedness—A Decision Tool." Available online at www.hhs.gov/ocr/hipaa/decisiontool/tool/dua.html.

Harris, Steven. "Check for These Essentials in Confidentiality Agreements." October 8, 2007. Available online at www.ama-assn.org/amednews/2007/10/08/bica1008.htm.

HHS, Office for Civil Rights. "Medical Privacy—National Standards to Protect the Privacy of Personal Health Information." Available online at www.hhs.gov/ocr/hipaa/contractprov.html.

HHS, Office for Civil Rights. "National Standards to Protect the Privacy of Personal Health Information." Available online at www.hhs.gov/ocr/hipaa.

HHS, Office of the Assistant Secretary for Planning and Evaluation. "Administrative Simplification in the Healthcare Industry." Available online at www.aspe.hhs.gov/admnsimp.

HIPAA Advisory, www.hipaadvisory.com.

HIPAA Resource Center, www.aishealth.com/Compliance/HIPAAResource.html.

Hjort, Beth. "A HIPAA Privacy Checklist." *Journal of AHIMA* 72, no. 6 (June 2001): 64A–C.

National Electrical Manufacturers Association, www.nema.org/medical.

Otech, Inc., www.otechimg.com.

Bonnie S. Cassidy *(bcassidy@cchit.org) is the strategic project leader for the Certification Commission for Healthcare Information Technology.*

Article citation:
Cassidy, Bonnie S.. "Examining Data Rights in Vendor Contracts: Privacy Obligations Extend to the Terms Negotiated in External Contracts" *Journal of AHIMA* 79, no.4 (April 2008): 56-57.