Law and the Public's Health

The health-care system has been transformed by the introduction of health information technology. This transformation, in turn, has led to the emergence of one of the most complex areas of health law: how to balance the privacy and security of individuals' health information against the need for access to health information to measure population health and better understand fundamental issues in health-care access, cost, and quality. This installment of *Law and the Public's Health* examines the 2013 HIPAA Privacy Rule and considers its implications for this balancing act.

Sara Rosenbaum, JD
George Washington University School of Public Health and Health Services
Department of Health Policy, Washington, DC

THE HIPAA OMNIBUS RULE: IMPLICATIONS FOR PUBLIC HEALTH POLICY AND PRACTICE

Melissa M. Goldstein, JD
William F. Pewen, PhD, MPH

It has now been more than a decade since the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule became effective, following years of conflicts that pitted multiple interests against one another: individual privacy rights, access to personal health information in public health and research endeavors, the economic interests of the health-care sector, and an expanding government role in health care. These influences combined to produce a convoluted and leaky regulatory system that, paradoxically perhaps, has been criticized since its inception as both burdensome to providers and inadequate to assure health information privacy and security for individual patients.[1]

Four years after the enactment of major HIPAA reforms in the Health Information Technology for Economic and Clinical Health (HITECH) Act,[2] the U.S. Department of Health and Human Services (HHS) has issued an Omnibus Rule that reflects movement to strengthen individual rights while continuing to facilitate the other competing interests, including those of public health, in greater access to health information.

This installment of *Law and the Public's Health* explores the evolution of HIPAA's privacy protections. After a brief description of the history and structure of HIPAA, we highlight key provisions of the recently released final rules and explore their implications for public health policy and practice.

BACKGROUND

Ensuring the privacy and confidentiality of health information has always been a critical aspect of health care, but until the enactment of HIPAA, no comprehensive piece of federal legislation protected health information privacy. Pursuant to the law, Congress gave itself two years to enact federal privacy protections, but in the end tasked HHS with the job of promulgating privacy and security regulations.[3] Following years of negotiations, federal regulations implementing HIPAA's privacy provisions were issued in 2000,[4] revised in 2002,[5] and became effective for most entities in 2003.[6]

The HIPAA Privacy Rule regulates the use and disclosure of protected health information (PHI) by "covered entities," defined as health plans, health care clearinghouses, and health care providers who transmit health information in electronic form. PHI is "individually identifiable health information" that is held or transmitted by a covered entity in any form, paper or electronic.[7] Under the Privacy Rule, covered entities may not use or disclose PHI except as permitted or required. Only two types of disclosures are required: when a patient requests his/her own PHI and when the Secretary of HHS requests PHI for audit or other enforcement purposes.[8] All other disclosures, including those that may be required by other federal or state laws (e.g., public health reporting statutes), are considered "permitted," or allowed by the Privacy Rule.[9] For example, covered entities are permitted to access, use, and disclose PHI for the purposes of treatment, payment, and health care operations.[10] Written "authorizations" by patients are required for uses and disclosures of PHI that are not otherwise permitted or required; as a result, many disclosures, including those related to treatment, payment, and health care operations, require no authorization.[11]

Public health operations have been largely exempted from HIPAA's restrictions. That is, HIPAA permits, but does not require, covered entities to disclose PHI without authorization to public health authorities for activities including, among others, reporting; surveillance, investigations, and interventions; and notifying people at risk of communicable disease.[12] The Privacy Rule, therefore, allows public health authorities to engage in the full range of activities authorized by state law, assuming successful collection of necessary data from covered entities (as either PHI or in less identifiable forms[13,14] allowed by the regulations).[15]

Although establishment of HIPAA's privacy provisions was a watershed in federal health information privacy law, gaps in the Privacy Rule's protections existed. These gaps have been amplified with the increased use of health information technology, which promises not only the possibility of comprehensive health records that can move with individuals over a lifetime, but also more efficient gathering of data that could lead to improved population health. For example, because HIPAA applies only to covered entities as defined in the statute, many of the new entities that store and/or manage PHI electronically have not been covered by the Privacy Rule. Other perceived deficiencies in the Privacy Rule have included its lack of a breach notification standard, concerns about the de-identification and limited data set provisions, objections to the use of consumers' PHI for marketing purposes, and complaints about oversight and enforcement activities.[3]

HITECH addressed many of these perceived deficiencies by (*1*) strengthening individual control over, and access to, data; (*2*) broadening the definition of who is considered a business associate of a covered entity (and thereby expanding the universe of entities covered by HIPAA) and increasing business associate duties; (*3*) creating a federal breach notification standard; (*4*) placing new restrictions on the marketing and sale of PHI; (*5*) requiring guidance on the use of de-identified data and limited data sets; and (*6*) adding new enforcement provisions and increasing penalties for violations. At the same time, HITECH retained HIPAA's basic legal structure to preserve the ability of public health agencies to establish standards for the reporting of important public health data and to use those data to monitor population health, incidence of disease, and effectiveness of treatment and care.[15] HHS released the Omnibus Rule implementing HITECH's provisions on January 17, 2013.[16] The Rule combines and replaces four previously issued proposed and interim final rules and became effective on March 26, 2013.[17–20]

THE OMNIBUS RULE

Patient access and control

The Omnibus Rule expands an individual's right to receive an electronic copy of his/her PHI.[21] In addition, the Omnibus Rule implements HITECH's requirement that providers follow patient requests that their PHI not be disclosed to a health plan for payment or health care operations purposes if the disclosure is not required by law and relates solely to items or services for which the patient paid out of pocket in full.[22]

Accountability

The Omnibus Rule expands the definition of a "business associate" to include all entities that create, receive, maintain, or transmit PHI on behalf of a covered entity,[7] making clear that companies that store PHI on behalf of health care providers and health plans are business associates.[23] This change extends HIPAA's requirements to a broader group of businesses that handle and have the capability to access identifiable health data, including health information organizations and patient safety organizations.

Further, HITECH made clear that business associates are now directly subject to most provisions of the HIPAA Security Rule as well as certain provisions of the Privacy Rule.[15] The Omnibus Rule clarifies that the definition of a business associate also includes relevant subcontractors, ensuring that a covered entity's or business associate's security requirements encompass outsourced operations.[7]

Marketing restrictions

The Privacy Rule generally prohibited the use or disclosure of PHI for marketing purposes without an individual's authorization, but traditionally allowed a number of exceptions. The Omnibus Rule tightened this approach, so that PHI may no longer be used in most marketing activities without patient authorization if the covered entity is compensated for making the communication by a third party (e.g., a pharmaceutical company) that is promoting its own product. In-kind benefits received by the covered entity (e.g., brochures, even if supplied by the third party) are not considered prohibited remuneration. HITECH also included a provision permitting third-party-sponsored communications to patients regarding drugs or biologics that they already have been prescribed (or generic substitutes). The Omnibus Rule permits payments for such communications (e.g., by a pharmaceutical company to a pharmacy for refill reminders) as long as the payment reasonably relates to the cost of the communication.[24]

Reasonable disclosures
Of particular note to public health practitioners, the Omnibus Rule makes the release of student immunization information to schools less cumbersome by allowing covered entities to disclose the immunization records of students or prospective students to a school if state law requires the school to have proof of immunization and the covered entity obtains and documents the agreement of the parent or guardian.[12]

Genetic information
As required by the Genetic Information Nondiscrimination Act of 2008, the Omnibus Rule incorporates genetic information into the definition of PHI, thereby explicitly applying HIPAA's privacy protections to individual genetic information.[7]

Sale of PHI
In accordance with HITECH's requirements, the Omnibus Rule generally prohibits the sale of PHI, defined as remuneration (financial or otherwise) in exchange for PHI, without individual authorization. Certain exceptions are allowed, including the sale of PHI for certain public health purposes (without restriction as to price) and sales for use in research if the remuneration is limited to a reasonable cost-based fee to cover the cost to prepare and transmit the PHI.[9]

Research
The Omnibus Rule has simplified HIPAA's consent requirements for research participation so that some studies involving PHI that have been required to use multiple consent forms will now be permitted to use a single form, which may prove less confusing to participants.[25] In addition, the Omnibus Rule offers a means for researchers to obtain "prospective consent" for future studies, a change from previous HHS interpretation of the Privacy Rule as requiring study-specific research authorizations.[26] This change facilitates the use of authorizations that are broad enough to encompass a range of future research projects; for example, the need for analysis of a biomarker, a genetic association, or a behavioral link might not be apparent when a study is begun, but could be critical at a future date. The Omnibus Rule now allows the use of prospective consent in such cases, as long as an individual receives an adequate description of the scope of potential future research so that individuals can reasonably anticipate how their PHI might be used.[27]

Breach notice
HITECH required that covered entities notify individuals whose unsecured PHI has been disclosed as a result of a privacy or security breach.[15] The Omnibus Rule replaces a controversial "risk of harm" breach standard from an earlier version of the rule[23] with an objective requirement that covered entities treat improper disclosures of PHI presumptively as breaches unless certain statutory conditions exist (e.g., demonstration that the data were encrypted) or the covered entity can demonstrate a low probability that PHI has been compromised. The latter requires a four-part risk assessment that includes consideration of whether the data were actually acquired or viewed by an unauthorized person and the extent of mitigation accomplished.[28]

Penalties
The Omnibus Rule clarifies that assessment of violations includes consideration of the number of individuals affected, the length of noncompliance, and the severity of culpability.[29,30] Penalties may reach a cap of $1.5 million per identical violation type per year.[31]

Implementation
In general, covered entities and their business associates had until September 23, 2013, to comply with the provisions of the Omnibus Rule. Under certain circumstances, covered entities are permitted up to one additional year to amend existing business associate contracts.[32]

IMPLICATIONS FOR PUBLIC HEALTH POLICY AND PRACTICE

HITECH addressed some of the gaps in the Privacy Rule's protections and, therefore, may help build public trust in the new environment of increased digitization of health data.[23] As the product of two statutes and a prolonged rulemaking process, the Omnibus Rule has produced a changed landscape for health information.

The Omnibus Rule has significantly tightened HIPAA's requirements for business associates, making it clear that they (and their subcontractors) must comply with its restrictions and can be held directly accountable for failure to do so. Moreover, the universe of entities covered by the law has widened and now encompasses, for example, health information exchange networks and personal health records (PHRs) that are offered through a covered entity's electronic health record.[23] The Omnibus Rule also strengthens individuals' control over their own data, including the right to restrict disclosure of PHI for purposes of carrying out payment or health care operations.

Nevertheless, HIPAA continues to reflect the inherent tension between the interests of public health and

the rights of individuals. While core public health duties have long required access to data for surveillance and response, demands for access to more extensive health information have grown, as some argue that serious public health concerns justify increased intrusion into personal health information. The Omnibus Rule retains HIPAA's basic structure in this regard and ensures the availability of PHI for public health purposes; indeed, the Omnibus Rule not only exempts public health purposes from its general proscription against the sale of PHI,[9] but covered entities are not restricted to selling PHI for such purposes at cost.[33]

The Omnibus Rule also continues to support the use of both limited data sets and de-identified data without individual authorization,[15] although neither type of data may ultimately prove reliable in maintaining confidentiality. HHS itself has noted a level of risk of re-identification of such data,[34] yet a critical aspect of current public health analyses is the integration of such data sets.

Ultimately, the foundation for the collection of public health data is public trust, which requires the formulation of policy that carefully considers both individual rights and collective goods. As the Institute of Medicine has reported that 58% of Americans think laws and practices do not adequately protect their health information[35] and only about one in 10 Americans supports sharing data with researchers without consent,[36] critical questions remain regarding whether the Omnibus Rule has adequately addressed such concerns.

LOOKING AHEAD

HHS has not yet completed its work on HITECH. Rulemaking to ensure greater transparency regarding disclosure of identifiable health data from electronic records is not complete and additional guidance is needed regarding the status of PHRs that are not covered by HIPAA and HIPAA's requirements to use or disclose only the minimum amount of health information necessary to achieve a covered entity's purpose.[23]

As technology rapidly advances and health information is gathered and stored in many environments, a more critical gap in HIPAA's protection of identifiable health data persists: it remains a context-centric approach to health information privacy. Data are protected largely based on when and by whom it was acquired. Most Americans are likely to view such "context" as a distinction without a difference—their health information is personal, valuable, and potentially vulnerable to misuse. It is likely that the tug of war over individual health data has not yet ended.

Melissa Goldstein is an Associate Professor of Health Policy at The George Washington University School of Public Health and Health Services in Washington, D.C. William Pewen is an Assistant Professor in Public Health and Family Medicine at Marshall University in Huntington, West Virginia.

Address correspondence to: Melissa M. Goldstein, JD, The George Washington University School of Public Health and Health Services, 2021 K St. NW, Ste. 800, Washington, DC 20006; tel. 202-994-4235; fax 202-994-3504; e-mail <mgoldste@gwu.edu>.

REFERENCES

1. Institute of Medicine. Beyond the HIPAA Privacy Rule: enhancing privacy, improving health through research. National Academies Press: Washington; 2009.
2. Pub. L. No. 111-5, 123 Stat. 115, 226-79 (2009), codified at 42 U.S.C. §§ 300jj *et seq.*; §§ 17901 *et seq.*
3. McGraw D. Privacy and health information technology. Washington: O'Neill Institute for National and Global Health Law; 2009, at 5-6. Also available from: URL: http://www.law.georgetown.edu/oneillinstitute/national-health-law/legal-solutions-in-health-reform/Privacy.html [cited 2013 Jun 30].
4. Department of Health and Human Services (US). Standards for privacy of individually identifiable health information: final rule. Fed Reg 2000;65:82462-829.
5. Department of Health and Human Services (US). Standards for privacy of individually identifiable health information: final rule. Fed Reg 2002;67:53182-3273.
6. Department of Health and Human Services (US). The Privacy Rule [cited 2013 Jun 30]. Available from: URL: http://www.hhs.gov/ocr/privacy/hipaa/administrative
7. 45 C.F.R. §160.103.
8. 45 C.F.R. §164.502(a)(2).
9. 45 C.F.R. §164.502(a).
10. 45 C.F.R. §164.506(a).
11. 45 C.F.R. §164.508(a).
12. 45 C.F.R. §164.512(b).
13. 45 C.F.R. §164.514(b).
14. 45 C.F.R. §164.514(e).
15. Goldstein MM. The health privacy provisions in The American Recovery and Reinvestment Act of 2009: implications for public health policy and practice. Public Health Rep 2010;125:343-9.
16. Department of Health and Human Services (US). Modifications to the HIPAA privacy, security, enforcement, and breach notification rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; other modifications to the HIPAA Rules: final rule. Fed Reg 2013;78:5566-702.
17. Department of Health and Human Services (US). Modifications to the HIPAA privacy, security, and enforcement rules under the Health Information Technology for Economic and Clinical Health Act: proposed rule. Fed Reg 2010;75:40868-924.
18. Department of Health and Human Services (US). HIPAA administrative simplification: enforcement: interim final rule; request for comments. Fed Reg 2009;74:56123-31.
19. Department of Health and Human Services (US). Breach notification for unsecured protected health information: interim final rule with request for comments. Fed Reg 2009;74:42740-70.
20. Centers for Medicare & Medicaid Services (US). Interim final rules prohibiting discrimination based on genetic information in health insurance coverage and group health plans. Fed Reg 2009;74:51664-797.
21. 45 C.F.R. §164.524(c)(2)(ii).

22. 45 C.F.R. §164.522(a).
23. McGraw D. Final HIPAA rules a major step forward, but there's more work to be done. iHealthBeat 2013 Feb 8. Also available from: URL: http://www.ihealthbeat.org/perspectives/2013/final-hipaa-rules-a-major-step-forward-but-theres-more-work-to-be-done.aspx# [cited 2013 Jun 30].
24. 45 C.F.R. §164.501.
25. 45 C.F.R. §164.508(b)(3)(i).
26. 45 C.F.R. §164.508(c)(1)(iv).
27. Department of Health and Human Services (US). Modifications to the HIPAA privacy, security, enforcement, and breach notification rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; other modifications to the HIPAA Rules: final rule. Fed Reg 2013;78:5566-702, at 5611-3.
28. 45 C.F.R. §164.402.
29. Department of Health and Human Services (US). Modifications to the HIPAA privacy, security, enforcement, and breach notification rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; other modifications to the HIPAA Rules: final rule. Fed Reg 2013;78:5566-702, at 5584-5.
30. 45 C.F.R. §160.408.
31. 45 C.F.R. §160.404(b).
32. 45 C.F.R. §164.532(d).
33. Department of Health and Human Services (US). Modifications to the HIPAA privacy, security, enforcement, and breach notification rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; other modifications to the HIPAA Rules: final rule. Fed Reg 2013;78:5566-702, at 5607.
34. Department of Health and Human Services (US). Guidance regarding methods for de-identification of protected health information in accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. 2012 Nov 26 [cited 2013 Jun 30]. Available from: URL: http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/hhs_deid_guidance.pdf
35. Westin AF. IOM project survey findings on health research and privacy. Presented at the Institute of Medicine Committee Meeting; 2007 Oct 2; Washington. Also available from: URL: http://www.iom.edu/~/media/Files/Activity%20Files/Research/HIPAAandResearch/AlanWestinIOMsrvyRept.ashx [cited 2013 Jun 30].
36. Caine K, Hanania R. Patients want granular privacy control over health information in electronic medical records. J Am Med Inform Assoc 2013;20:7-15.