Law and the Public's Health

HIPAA'S IMPLICATIONS FOR PUBLIC HEALTH POLICY AND PRACTICE: GUIDANCE FROM THE CDC

Brian Kamoie, JD, MPH
James G. Hodge, Jr., JD, LLM

This installment of *Law and the Public's Health* addresses the Guidance issued in April 2003 by the U.S. Centers for Disease Control and Prevention (CDC) regarding the Privacy Rule under the Health Insurance Portability and Accountability Act (HIPAA)[1] and public health. Following a review of this Guidance and the Privacy Rule to which it pertains, this column assesses the implications for public health policy and practice.

THE HIPAA PRIVACY RULE

The HIPAA Privacy Rule became effective on April 14, 2003.[2] The broad purpose of this regulation is to protect certain types of individually identifiable health information, known as *protected health information* (PHI), from unauthorized access, use, or disclosure. Public health activities rely heavily on the acquisition, use, and exchange of identifiable health information, so it is vital that the public health community understand how the Privacy Rule affects public health practice (e.g., disease reporting and surveillance, direct treatment, and public health research). The CDC's Guidance is intended to clarify the roles and responsibilities of public health agencies, their partners, and others under the Privacy Rule.

The Privacy Rule's permissible disclosure

A principal objective of the Privacy Rule is to bar "covered entities" (such as health care providers) from using or disclosing PHI except as authorized by the individual who is the subject of the information, or as explicitly required or permitted by regulation.[3] The Rule contains a host of disclosure exceptions to the requirement for individual authorization, including disclosures related to law enforcement, judicial proceedings, national security, familial contact, minors, health research, and, notably, public health. Even when the use or disclosure of PHI is permitted, entities may generally provide only the "minimum necessary" amount of information to accomplish the intended purpose of the use, disclosure, or request.[4]

The Rule defines *covered entities* broadly. The term encompasses health care providers, health plans (including Medicaid and Medicare), and health care clearinghouses (public or private entities that process health information).[5] By definition, covered entities do not include public health agencies; however, public health agencies (or any other entity for that matter) may be considered covered under the Rule when they perform certain functions that assimilate functions of covered entities (such as the provision of health care services).

Protected health information is defined as individually identifiable health information that is transmitted or maintained either by electronic media or in any other form or medium.[6] *Health information* is information that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.[7]

Beyond specifying the requirements of covered entities for the use and disclosure of PHI, the Privacy Rule grants individuals certain rights, including the right to access their own PHI, request amendments to that information, receive adequate notice of the uses and disclosures a covered entity makes of their PHI, and receive an accounting of disclosures.[8]

Compulsory disclosure under the Privacy Rule

Although most of the Rule addresses "permissible disclosures" of PHI, disclosures are compelled when individuals request a copy of their PHI, or the U.S. Department of Health and Human Services (DHHS) needs PHI to determine an entity's compliance with the Privacy Rule. As well, the Rule does not preempt other federal, state, tribal, or local laws that may compel disclosure of PHI.

CDC'S PRIVACY RULE GUIDANCE

The CDC's extensive Guidance analyzes and accommodates public health needs for PHI with the provisions and purposes of the Privacy Rule. The following summary of this Guidance provides a capsule of some of its key analyses.

Public health disclosures permitted without authorization

The Privacy Rule permits a covered entity to use and disclose PHI without individual written authorization in certain circumstances. Of central relevance here is that covered entities can disclose PHI without authorization to a public health authority (or its authorized partners or agents) provided the agency is legally authorized to collect and receive the disclosed information and the disclosure is for "public health purposes." Public health purposes include, but are not limited to, public health surveillance, investigations, and interventions.[8] An example of such a disclosure would be the provision of childhood immunization information to an immunization registry.

Covered entities may also disclose information without authorization when required by state and local public health or other laws, regardless of whether the receiving entity is a public health authority. For example, disclosure of an individual's PHI to a state court is permitted under the Rule provided state law required the disclosure (even absent individual authorization). Covered entities can and should include these types of contemplated disclosures in the notice of privacy practices they are required to provide to individuals under the Privacy Rule.

By including public health activities among the uses and disclosures permitted without individual authorization, the Privacy Rule recognizes "the legitimate need for public health authorities and others responsible for ensuring the public's health and safety to have access to PHI to conduct their missions; and . . . the importance of public health reporting by covered entities to identify threats to the public and individuals."[8]

The Rule's broad definition of *public health authority* includes agencies and authorities at any level of government (federal, tribal, territorial, state, or local), or an individual or entity acting under a grant of authority from such entities and responsible for public health matters as part of an official mandate.[8] Public health authorities thus include DHHS, the CDC, the National Institutes of Health, the Food and Drug Administration, and other divisions at the federal level, as well as state, tribal, territorial, and county/city departments of health or public health. In addition, the definition includes entities with which a public health agency conducts authorized public health activities (through memoranda of understanding/agreement or contracts). Such entities are treated as public health authorities for those activities they conduct under grants of authority from public health agencies. As a result, these contracts should contain duties and safeguards for the use and disclosure of PHI by both sides of the agreement. For example, such agreements should require contractors to use PHI only for the purposes of the public health activity and to have safeguards in place to prevent use and disclosure beyond such purposes. Such agreements should also require contractors to share their policies and procedures regarding PHI with the public health authority, and to notify the public health authority if any unauthorized disclosure occurs. (Although the Privacy Rule does not require the use of these types of safeguards in agreements between public health authorities and their contractors [because such contractors are not treated as "Business Associates" under the Privacy Rule], the inclusion of such provisions is a good business practice and should assist public health authorities and their contractors in ensuring that no unauthorized disclosure of PHI occurs.)

The CDC Guidance provides examples of public health practice situations covered by the public health disclosure provisions of the Privacy Rule. It also offers sample language to be used by public health authorities when communicating with covered entities or relevant agencies about disclosure issues. For example, the Guidance offers the following scenario:

> **State cancer registry.** Under a state law, health-care providers are required to report cancer cases to a state's cancer registry. Names are included to prevent duplicate reporting and counting. State law protects the confidentiality of the data. Can covered entities disclose the information under the Privacy Rule?
>
> **Privacy Rule effect.** Covered entities may disclose PHI to a public health agency, or any other entity, when the disclosure is required by law. However, the covered entities [must be prepared to account for the disclosures if requested by] the persons whose PHI has been shared. The state agency may use and further disclose the PHI consistent with applicable state law.[6]

The Guidance offers similar explanations for state university-maintained cancer registries, early hearing and detection programs, disease registries maintained by private foundations, and standard surveillance projects.[6]

Public health authorities as covered entities

Much of the CDC Guidance relates to public health authorities as receivers of information from covered entities. In this capacity, public health authorities doing public health activities are not covered by the Privacy Rule. When, however, a public health authority acts as a provider of personal health services, either directly or through subcontract (e.g., maternity care,

or HIV testing and treatment), the authority is itself considered a covered entity. The authority is accordingly required to comply with all of the Privacy Rule's provisions (e.g., consent/authorization, providing notice of privacy practices and rights, accounting for disclosures) at least for its covered functions if it performs electronic transactions (e.g., the generation of claims for payment) covered by HIPAA's transactions rule as part of those activities.[5,8]

Other functions performed by some public health authorities may also afford the authorities covered entity status. Public health authorities administering government health care or financing programs (e.g., Medicare, Medicaid, or the Veterans Health Administration) are covered.[5,8] The Centers for Medicare and Medicaid Services (CMS) offer flow charts and interactive tools to help public health authorities determine their covered entity status.[10]

A public health authority that is a covered entity and that has both covered and non-covered functions may designate itself as a hybrid entity under the Rule. By doing so, the authority designates its covered components, which are subject to the Privacy Rule's requirements. The remaining non-covered public health activities are exempt from Privacy Rule requirements. For example, one division of a state department of public health might operate health clinics that are covered health providers, while other divisions conduct public health surveillance and disease reporting (non-covered functions).

Public health research

The Guidance notes the existence of separate standards addressing the Privacy Rule's disclosure exceptions related to health research.[5,8,10] The intersection of the health research and public health exceptions under the Rule is complex because of differing standards and unclear distinctions between research and public health practice. In brief, the majority of public health activities (e.g., surveillance, disease prevention/control) likely do not meet the definition of research under the Privacy Rule, nor are they considered research under the Common Rule, which applies to most federally-conducted and sponsored research and addresses human subject safeguards. The Privacy Rule and Common Rule define *research* as systematic investigation—including research development, testing, and evaluation—designed to develop or contribute to generalizable knowledge. Public health activities have as their primary purpose the conduct of essential public health services and functions, rather than contribution to generalizable knowledge (as with research). Because many activities of public health authorities are not considered research, authorities may disclose information generated through their investigation that otherwise would be covered by the Privacy Rule. At the same time, if a public health authority designs and conducts research activities (e.g., a research study to evaluate the efficacy of a drug to treat an illness under surveillance), federal and state laws governing consent, disclosure, and other requirements apply.

CONCLUSION

While the Privacy Rule does not intentionally limit public health authorities in their performance of public health activities, it has had an impact on these activities; assessment of these effects is ongoing. Perhaps the most important aspect of the Privacy Rule in a public health context is that public health authorities may be covered entities depending on their activities; there is no blanket exception for public health, as many initially believed. When a public health authority is a covered entity, Privacy Rule requirements apply. When a public health authority is a hybrid entity, the Rule's requirements apply only to the covered functions. Therefore, public health authorities should review the scope of their activities to determine the extent of coverage and the appropriateness of designation as a hybrid.

Second, the obligations of public health authorities to comply with the Privacy Rule are not removed when authorities contract to conduct activities covered by the Rule through private entities. In essence, the Privacy Act's duties are non-delegable and devolve to the entity acting as the agent of the public health authority. Therefore, public health agencies should ensure that compliance with the Rule is a basic element of all agreements and contracts where applicable.

The CDC Guidance offers practical examples that are relevant and familiar to public health practitioners; however, it certainly will not be the last word. New questions of interpretation and applicability will arise as the impact of national privacy policies on public health practice continues to evolve. Ultimately, what is needed are policy choices that continue to balance health information privacy with public health activities.[11]

Brian Kamoie is an assistant professor in the Department of Health Policy at the George Washington University School of Public Health and Health Services. James G. Hodge, Jr. is on the faculties of the Georgetown University Law Center and the Johns Hopkins Bloomberg School of Public Health; he is also Deputy Director of the Center for Law and the Public's Health at Georgetown and Johns Hopkins Universities in Washington, DC and Baltimore, MD. He assisted in the development of the CDC Guidance.

REFERENCES

1. Health Insurance Portability and Accountability Act, Pub. L. No. 104-191 (Aug. 21, 1996).
2. 65 Fed. Reg. 82461 (Dec. 28, 2000); 67 Fed. Reg. 53181 (Aug. 14, 2002).
3. 45 CFR § 164.502(a); 65 Fed. Reg. 82805 (Dec. 28, 2000).
4. 45 CFR § 164.502(b); 65 Fed. Reg. 82805 (Dec. 28, 2000).
5. 45 CFR § 160.103; 65 Fed. Reg. 82799 (Dec. 28, 2000).
6. 45 CFR § 164.501; Fed. Reg. 82805 (Dec. 28, 2000).
7. 45 CFR § 160.103; 65 Fed. Reg. 82799 (Dec. 28, 2000).
8. 45 CFR §§ 164.520-164.526; Fed. Reg. 82820-26 (Dec. 28, 2000).
9. HIPAA Privacy Rule and public health: guidance from the CDC and the U.S. Department of Health and Human Services. MMWR Morb Mortal Wkly Rep 2003; 52(Early Release):1-19. Also available from: URL: http://www.cdc.gov/privacyrule/Guidance/PRmmwrguidance.pdf
10. Centers for Medicare and Medicaid Services. Covered entity decision tools [cited 2003 Oct 8]. Available from: URL: http://www.cms.hhs.gov/hipaa/hipaa2/support/tools/decisionsupport/default.asp
11. Gostin LO, Hodge Jr JG. Model state public health privacy act [cited 2003 Oct 8]. Available from: URL: http://www.publichealthlaw.net/Resources/ResourcesPDFs/modelprivact.pdf