
Becoming a Hybrid Entity: A Policy Option for Public Health

Sallie Milam and Melissa Moorehead

1. Introduction

Digital technology has had a mixed impact on the way Americans understand health care and public health. There is an untapped potential to gain a deep and nuanced view of health that takes into account “the conditions in which people are born, grow, live, work and age ... shaped by the distribution of money, power and resources,” often described as “social determinants of health”¹ (SDOH), which is coming into sharp focus as a federal, state, and local priority. Health and other individual-level data combined from various sources help reveal the relationship of SDOH to individual and population health, and to evaluate interventions. However, ease of access to electronic private information, combined with many examples of data breaches and misuse of data, make many people uneasy. Congress enacted the Health Insurance Portability and Accountability Act of 1996 (HIPAA) in large part to improve the health care system’s efficiency and effectiveness by standardizing and regulating elec-

Sallie Milam, J.D., has practiced law for over 25 years primarily in the health, HIPAA, and general privacy areas. Since 2003, she has served as West Virginia’s Chief Privacy Officer and leads the Executive Branch’s Privacy Program. In her spare time, Sallie develops data sharing educational and resource materials. Sallie received her Juris Doctorate from the University of Richmond School of Law in Richmond, Virginia and her Bachelor of Arts from Brigham Young University in Provo, Utah. Melissa Moorehead has over 15 years of experience in the non-profit health care and public health world as a project manager, policy analyst, evaluator, subject matter expert in health care reform, and advocate. They are currently involved in promoting community capacity to collaborate and share data across sectors in the Data Across Sectors for Health national program office of the Robert Wood Johnson Foundation, co-located at the Illinois and Michigan Public Health Institutes. Melissa received a Bachelor of Arts from the University of Michigan in Ann Arbor, Michigan.

tronic personal health information, but also to allay fears about improper use of personal health data.² HIPAA was the first and remains the only national, all-encompassing privacy law seeking to safeguard personal health information and limit its inappropriate use and sharing.

Congress shaped HIPAA so that it applies to health plans, health care clearinghouses, and health care providers that transmit electronic health information in covered transactions.³ If a public health department operates a health plan (e.g., Medicaid or the Children’s Health Insurance Program), serves as a health care provider (e.g., a clinic or laboratory that bills electronically), or acts as a clearinghouse, it is covered by HIPAA. Importantly, however, HIPAA recognizes public health as a matter of national priority and specifically exempts sharing certain data with public health agencies from its reach.⁴

2. The Challenge of Applying HIPAA to Public Health’s Traditional, Non-covered Programs

In April 2016, the US Department of Health and Human Services launched the Public Health 3.0 initiative. Public Health 3.0 envisions public health authorities collaborating with other entities across sectors to develop “timely, locally relevant health information systems” that “address all factors that promote health and well-being.”⁵ This opens new challenges to privacy and ethics as public health authorities seek to gain access to a broader array of personal health information from providers or payers, to link with new partners’ data sets, for new purposes. Additionally, community groups seek timely and relevant data about their constituencies at a more granular level than ever before.

Among its many requirements, HIPAA prohibits the use and sharing of individually identifiable health information, unless the proposed use or disclosure is specifically permitted or required under the HIPAA Privacy Rule (“the Rule”).⁶ The Privacy Rule’s “safe harbor standard” is the most commonly utilized HIPAA compliant de-identification method, as it is straightforward and specifies prohibited data elements that directly identify a person, such as name, Social Security number, and medical record number.⁷ HIPAA also generally requires redaction of dates that are more specific than a year and geographies that are smaller than a state.⁸ The downside to this method is that it yields a dataset that does not include granular, place-based, temporal data that is useful to communities. Consequently, when public health shares data that has been de-identified according to the HIPAA safe harbor standard, it may not be able to fully achieve the Public Health 3.0 vision.

SDOH and the associated inequities that are major drivers of morbidity and mortality must include input from people with lived experience in the populations most affected. This is important in understanding the meaning of the data collected, the development of effective interventions, and evaluating true impact. At the same time, many other community health stakeholders — from hospitals to insurers to community leaders — are beginning to understand the potential for public health data to strengthen their own work, whether it is driven by community benefit regulations, payment reform, or civic engagement. Sadly, lack of understanding of technology and regulation dampens the flow of useful information even as the volume, timeliness, and granularity of health data increases exponentially. While it is difficult to develop empirical evidence of what did not happen (cases where data should have been shared but were not),¹⁰ there is growing alarm that this lack of understanding can

Sadly, lack of understanding of technology and regulation dampens the flow of useful information even as the volume, timeliness, and granularity of health data increases exponentially. While it is difficult to develop empirical evidence of what did not happen (cases where data should have been shared but were not), there is growing alarm that this lack of understanding can lead to missed opportunities for community health improvement when stakeholders believe that HIPAA constrains their ability to share and use data.

Even though HIPAA exempts information sharing for basic public health functions, the complex political and business arrangements that vary by jurisdiction can make determinations of law difficult, and mistakes can be costly⁹ — and chilling. Too often, legal counsel will suggest that the safest route is “locking down” data that should be available, to avoid liability for improperly navigating law or unintended or unforeseen disclosures. While HIPAA is an important safeguard in the health sector, public health entities have a duty to ensure that it does not pose a barrier to working across sectors to fulfill their essential functions for the public good. We propose strategies below.

3. Communities Need Timely and Locally Relevant Health Data

While public health authorities have a host of traditional functions in epidemiology, surveillance, and population-level intervention that are greatly enhanced by technology, a true understanding of

lead to missed opportunities for community health improvement when stakeholders believe that HIPAA constrains their ability to share and use data.¹¹

When the right combination of data literacy, infrastructure, and trust exists, innovative partnerships can lead to real health improvements. When it does not, the results can be disastrous. Lack of access to surveillance data at a geographic or demographically precise level can lead to unrecognized epidemic or endemic situations. In the case of Flint, Michigan’s water crisis, while the levels of system failures and responsibilities continue to be debated — and litigated — the situation might have been resolved sooner had blood lead level test results from public health surveillance been more readily available to local doctors. Dr. Hanna-Attisha, who eventually verified the problem using data from her hospital’s medical records, has said that she believes that the problem need not have gone on so long. “I tried to get that blood lead data both from the state and from the county health departments but had roadblocks at every direction.”¹²

Epidemiology and service utilization information can also be important to communities. Community-based organizations often want better enforcement of housing standards but can have a hard time convincing authorities to act. In some areas, these groups have worked with the public health sector to identify clusters of pediatric asthma in neighborhoods with poor housing. Looking for patterns in hospitalizations can further help to understand what exacerbates housing-related health conditions to even more dangerous levels. Demonstrating that children living in apartments without adequate air conditioning visit the emergency room more often can galvanize action by health systems as well as municipal authorities, but it takes extremely granular data to make the case.

4. HIPAA's Hybrid Entity Policy Option

Applying HIPAA's use, disclosure, and de-identification regulations to traditional public health data sharing prevents communities from accessing needed data from vital statistics, registries, surveillance, interventions, and investigations. HIPAA does not intend this result and does not list traditional public health activities within its scope.¹³ Moreover, the Rule offers a mechanism to carve out non-covered functions, such as traditional public health programs, from the rest of the organization, so that HIPAA only applies to those portions of an organization that the law specifically lists as covered, such as a public health laboratory that bills electronically or a Children's Health Insurance Program. This policy option is known as becoming a hybrid entity.¹⁴

Becoming a hybrid entity requires research and assessment to identify the legal entity within which the public health department sits.¹⁵ It also requires an evaluation of services against HIPAA to determine which parts of the organization provide covered services.¹⁶ The assessment results must be reflected in writing, commonly referred to as a hybrid entity policy, and maintained for six years.¹⁷ HIPAA offers the hybrid entity policy option so that organizations, including public health departments, may strategically and legally limit the application of HIPAA, thereby exempting traditional public health programs from its reach.¹⁸

Vital statistics about overdose deaths reveal the problem generally, but understanding the local environment is essential for action. As an example, Indiana State Department of Health's (ISDH) syndromic surveillance system (Essence) captures drug overdose activity. ISDH launched a pilot project to monitor trends and alert local health partners regarding increases in overdoses.¹⁹ Examples of available data fields include: patient zip code and county of resi-

dence, hospital name, county and zip code, date and time of patient arrival, and chief complaints.²⁰ ISDH safeguards individual privacy by only releasing de-identified data to authorized individuals who have signed their agreement.²¹

Because ISDH chose to be a hybrid entity under HIPAA, it removed its syndromic surveillance program from HIPAA's reach and is legally able to share granular and timely overdose syndromic surveillance data with local health departments and other partners. If ISDH had not become a hybrid entity, its syndromic surveillance program would be covered by HIPAA because of its other HIPAA-covered programs - Breast and Cervical Cancer Program, Children's Special Health Care Services Program, Genomics/Newborn Screening Program, Hemophilia Program and HIV Medical Services Program.²² In the absence of meeting a HIPAA exception and without access to a statistical expert, if ISDH's overdose syndromic surveillance system were HIPAA covered, it would generally not be able to share the detailed dates and time (anything less than a year) and geographic data (generally any subdivision smaller than a state) with partners beyond the local health departments.²³ The power of ISDH's overdose syndromic surveillance would not be maximized.

5. Conclusion

Freeing traditional public health data from HIPAA constraints is critical to conquering data lock-down. Traditional public health data privacy remains safeguarded through a combination of state and local law, ethical obligations²⁴ and data use agreements under which the data was obtained.²⁵ Becoming a hybrid entity is an important policy option for public health to consider for engaging communities in improving health and achieving equity.

Note

The authors have nothing to disclose.

References

1. World Health Organization, "About Social Determinants of Health," available at <https://www.who.int/social_determinants/sdh_definition/en/> (last visited March 5, 2019).
2. 42 U.S.C. § 1320d note (1996).
3. 42 U.S.C. § 1320d-1(a) (1996).
4. 5 C.F.R. § 164.512(b); see also *id.* at § 164.512(a).
5. K. B. DeSalvo et al., "Public Health 3.0: Time for an Upgrade," *American Journal of Public Health* 106, no. 4 (2016): 621-622.
6. 45 C.F.R. § 164.502(a) (2013).
7. 45 C.F.R. § 164.514(b)(2) (2013).
8. *Id.* HIPAA also provides an expert determination standard. 45 C.F.R. § 164.514(b)(1) (2013).
9. See, Office of Civil Rights, Health and Human Services, *UMass Settles Potential HIPAA Violations Following Malware Infection*, News Release, November 22, 2016, available at <<http://wayback.archive-it.org/3926/20170128222809/https://www>

- hhs.gov/about/news/2016/11/22/umass-settles-potential-hipaa-violations-following-malware-infection.html> (last visited March 5, 2019).
10. W. G van Panhuis et al., “A Systematic Review of Barriers to Data Sharing in Public Health,” *BioMed Central Public Health* 14 (2014): 1144.
 11. D. Wartenberg and W. D. Thompson, “Privacy Versus Public Health: The Impact of Current Confidentiality Rules,” *American Journal of Public Health* 100, no. 3 (2010): 407-412.
 12. M. Hana-Attisha, interview by Terry Gross, *Fresh Air*, National Public Radio, June 25, 2018.
 13. See 42 U.S.C., *supra* note 3.
 14. 45 C.F.R. § 164.103 (2013).
 15. *Id.*
 16. 45 C.F.R. § 164.105(a)(2)(iii)(D) (2013).
 17. 45 C.F.R. § 164.105(c)(1) and (2) (2013).
 18. The Network for Public Health Law offers a Hybrid Entity Toolkit that includes legal, policy and practical guidance to understand and implement HIPAA’s hybrid entity option. See “Health Information and Data Sharing,” available at <https://www.networkforphl.org/topics__resources/topics__resources/health_information_and_data_sharing/> (last visited March 5, 2019).
 19. M. Billman and K. Dotson, “Using Drug Overdose Syndromic Surveillance Data to Impact Local Public Health Action,” *Online Journal of Public Health Informatics* 10, no. 1 (2018); Indiana State Department of Health, *Overdose Prevention: Overdose Response Project Overview*, 2018, available at <<https://www.in.gov/isdh/27798.htm>> (last visited March 5, 2019).
 20. Indiana State Department of Health, *Epidemiology Resource Center: ESSENCE User Guide*, v. 1.19 (2017): at 6-8, available at <https://www.in.gov/isdh/files/Indiana%20ESSENCE%20User%20Guide_2017.pdf> (last visited March 5, 2019).
 21. *Id.*, at 27.
 22. See, Indiana State Department of Health, “What Is HIPAA,” available at <<https://www.in.gov/isdh/23501.htm>> (last visited March 5, 2019).
 23. This hypothetical utilizes the HIPAA Privacy Rule’s safe harbor method of de-identification. See 45 C.F.R., *supra* note 7.
 24. Public health authorities may adopt a code of ethics as a way to explicitly state values, commitments and standards. The Principles of the Ethical Practice of Public Health address the balance between information sharing and the importance of protecting individual and community confidentiality, which application could result in a public health department’s decision not to make public certain information. Public Health Leadership Society, *Principles of the Ethical Practice of Public Health* (2002): at 4, available at <https://www.apha.org/-/media/files/pdf/membergroups/ethics/ethics_brochure ashx> (last visited March 5, 2019).
 25. J. M. Sharfstein, D. Chrysler, J. Bernstein, L. Armijos, L. Tolosa-Leiva, H. Taylor, and L. Rutkow, “Using Electronic Health Data for Community Health: Example Cases and Legal Analysis,” December 2017, available at <<http://www.debeaumont.org/EHDforCommunityHealth>> (last visited March 5, 2019).