Unlocking Public Health Data: Navigating New Legal Guardrails and Emerging AI Challenges

Fallon J. Cochlin, Charles D. Curran, and Cason D. Schmit

Keywords: Artificial Intelligence, Privacy, Confidentiality, Public Health Surveillance, Public Health Practice

Abstract: Here, we analyze the public health implications of recent legal developments — including privacy legislation, intergovernmental data exchange, and artificial intelligence governance — with a view toward the future of public health informatics and the potential of diverse data to inform public health actions and drive population health outcomes.

Introduction

Recent legislative initiatives to establish general privacy laws seek to provide more comprehensive protection for consumer data, but these new laws may also impact access to novel data sources for public health. Separately, the COVID-19 response has exposed weaknesses in data federalism and revealed important lessons on how to improve intergovernmental data exchange. Despite their significance, these challenges are eclipsed by seismic developments in artificial intelligence (AI) capabilities and adoption, which will pose profound regulatory and ethical challenges for public health. Public health perspectives are crucial but underrepresented in AI governance efforts.

Fallon Cochlin, J.D., *is a Postdoctoral Research Associate at Texas A&M School of Public Health.* **Charles Curran, J.D.** *is the Principal at Charles D. Curran Consulting, L.L.C.* **Cason D. Schmit, J.D.,** *is an Assistant Professor at Texas A&M School of Public Health.*

Here, we analyze the public health implications of recent data governance developments, with a view toward the future of public health informatics and the potential of diverse data to inform public health actions and drive population health outcomes.

Emerging General Data Privacy Laws

Responding to ever-expanding private sector data collection, federal and state legislators have increasingly introduced and adopted general privacy laws to establish baseline consumer data rights. These laws impose more significant consent requirements for the collection and transfer of sensitive health data. However, they generally exempt data collection by governments and entities already regulated by privacy laws like the Health Insurance Portability and Accountability Act (HIPAA). Such laws should not directly impact traditional public health data collection, such as case reporting. Nonetheless, some new state privacy laws pose potential obstacles to public health's collection and use of novel data sources that may provide valuable insights on the non-biological determinants of health.

At the federal level, Congress has advanced the American Data Privacy & Protection Act (ADPPA), which proposes comprehensive consumer privacy protections.[1] It would establish duties of data minimization for collectors and require affirmative consent for use and transfer of sensitive data. The ADPPA's definitions of sensitive data are expansive, including health information and data relating to minors, race, and ethnicity. However, the ADPPA exempts from its coverage government authorities and entities already regulated under HIPAA, leaving intact many existing channels of public health data transmission. Although

The Journal of Law, Medicine & Ethics, 52 S1 (2024): 70-74.
DOI: 10.1017/jme.2024.40

the ADPPA secured House committee approval in 2022, it failed to advance to a full floor vote.[2] Its prospects remain uncertain in the face of continued debate over the scope of state law preemption and individual enforcement rights.

In the absence of Congressional action, states have increasingly passed their own laws. Since 2020, thirteen states have adopted general consumer privacy statutes, and two states have passed health-data specific privacy measures.[3] Like the ADPPA, these state laws establish consumer data rights of transparency, access and control, and also broadly define sensitive information to include not just health and children's data, but also race and ethnicity, biometric and precise geolocation data. However, these laws also exempt government agencies, HIPAA-regulated entities or data, non-profits (in most cases), and most importantly, data used only for public health purposes.[4]

Given these overlapping exemptions, the new wave of state privacy laws should not directly impact established mechanisms for public health data reporting, such as for reportable conditions and laboratory reporting. Nonetheless, subtle exemption variations in each state's privacy law may still impact the legal basis for public health access to significant data categories collected outside of the clinical care context (e.g., provisions for stringent restrictions on race/ethnicity data or geo-location data). Non-HIPAA individually identifiable data originating from commercial entities — including from mobile apps, wearables or Internet of Things devices — may now require scrutiny to ensure compliance with state law requirements when such data is repurposed for public health use. In states that have adopted very broadly defined privacy laws, businesses and some nonprofits collecting and transferring data with public health relevance — including health-adjacent data and social determinants of health data relating to individuals — could face additional restrictions to share those data with public health partners.[5]

For instance, Washington's "My Health My Data Act" broadly applies to data that relates to "individual health conditions or status, diseases, or diagnoses ... [and] social, psychological, behavioral and medical interventions" and also "any information that a regulated entity processes to associate [such data] that is derived or extrapolated from non-health information." This means that businesses and non-profit organizations that are subject to Washington's law and have data from social interventions (e.g., homelessness or food insecurity) may need to ensure that any transfer of those data to public health partners falls squarely within an existing exemption.[6]

In states that have adopted very broadly defined privacy laws, businesses and some nonprofits collecting and transferring data with public health relevance — including health-adjacent data and social determinants of health data relating to individuals — could face additional restrictions to share those data with public health partners.

The Governance of Intergovernmental Data Exchange

Data Federalism

Public health threats transcend jurisdictional boundaries. As such, data sharing between governmental public health partners is vital to inform action and allocate resources effectively. But without a Congressional framework, intergovernmental data use agreements (DUAs) comprise the *de facto* governance mechanism for intergovernmental data exchange.[7] As the product of intergovernmental negotiations, DUAs add complexity and resist standardization that is needed to effectively manage data across thousands of jurisdictions.

Syndromic Surveillance DUAs and the COVID-19 Response

The DUAs that govern syndromic surveillance data presented a significant barrier to a national real-time view of the initial spread of COVID-19.[8] The DUAs — which restricted federal views of state and local syndromic surveillance data below the HHS region level — were the product of public health professionals carefully balancing individual privacy interests with broader social interests while navigating a complex history of intergovernmental relationships.

These DUA restrictions likely conflicted with WHO ethical guidelines, which impose a broad obligation to share surveillance data with other public health agencies.[9] When asked what policy guardrails are needed to permit greater federal access to state and

The Journal of Law, Medicine & Ethics, 52 S1 (2024): 70-74.

local data, a workgroup of state and local epidemiologists identified many protections that were at least partially addressed in the existing DUAs. While this suggests that greater intergovernmental data sharing is close, the COVID-19 response (and its politicization) strained many interjurisdictional relationships, challenging efforts to align data sharing practices with public health ethical norms.[10]

Immunization DUAs and the COVID-19 Response

Similar obstacles to exchange arose with DUAs governing the transfer of vaccination information from state immunization information systems (IIS) to the federal government. Prior to COVID-19, IIS were managed through a cooperative federalism in which states operated registries with federal funding assistance and policy guidance, but did not transfer individually identifiable recipient information to federal public health agencies.[11] However, the Operation Warp Speed response plan called for centralized federal data collection of such individual information for the purposes of monitoring second dose administration and vaccine safety.[12] Several states objected to the provisions of the Centers for Disease Control & Prevention's proposed DUA, raising concerns that (1) the transfer of individual information might violate state law; (2) the transferred information might be repurposed for federal immigration enforcement efforts; and (3) federal data collection of individual and demographic data might also conflict with state de-identification standards.[13] These concerns were eventually addressed pragmatically following the transition between administrations in the early phase of the vaccination campaign, including through amendments by some states to the CDC DUA, issuance of clarifying federal guidance, and public commitments to preclude immigration enforcement use.[14] Notably, these commitments to preclude immigration enforcement data uses align with WHO ethical guidelines.[15]

The lessons of COVID-19 point to opportunities to streamline key terms for data transfers between the federal government and state, territorial or tribal partners, notwithstanding the heterogeneity of public health data sources.[16] These could include standardized provisions defining the scope of federal access to identifiable information, both in the ordinary course and during public health emergencies; appropriately defined legal and technical standards for data de-identification; limits on secondary transfer and use, including access for law-enforcement purposes; data rights; controlling cybersecurity standards; and governance mechanisms. Encouragingly, the CDC's Data Modernization Initiative has now established objectives to adopt such standardized agreements for core data sources by 2024.[17]

Regulating Data Processing: AI and Public Health

AI presents several opportunities to improve public health operations. There are numerous potential public health AI applications. For instance, AI could be used to enhance existing surveillance systems to help identify timely patterns and trends and could be extremely helpful for systems with complex data, like syndromic surveillance and wastewater surveillance. AI could be used to support precision public health, where complex data on health risk factors enable targeted and individualized personalized interventions. AI will inevitably support Learning Health Systems, which continually and systematically incorporate new discoveries and clinical observations into sophisticated clinical decision support tools. AI also could be immensely valuable for supporting efficient resource allocation decisions, potentially game-changing to chronically underfunded public health agencies.[18]

However, managing data is a primary concern with introducing AI into public health systems. The accuracy of AI models relies on thorough training and testing, requiring copious data. Yet, the existing public health IT infrastructure is likely insufficient for many jurisdictions that still struggle with interoperability and outdated systems. In many ways, the future of AI in public health depends on the success of the Data Modernization Initiative.

Regulation is another central issue facing public health AI integration. Governance of AI is a technology-wide challenge faced by industry and government alike. Traditional legislative processes are slow and will inevitably be outpaced by AI. Increasingly, governance deliberations are focusing on "soft law," which describes judicially unenforceable guidelines, standards, and rules intended to guide industry behavior. The most common critique of soft law governance is that it relies excessively on industry self-regulation, which has a mixed history of success. One solution is to bridge soft and hard law through collaborative governance, wherein governments incorporate soft law standards into hard law regulatory frameworks, marrying the enforcement capability of hard laws and the flexibility of soft laws.[19]

Recent international AI governance efforts include the EU AI Act and China's Global AI Governance Initiative. The EU's AI Act has a risk-based framework with more stringent requirements for riskier applications.[20] In the U.S., the Biden Administration's recent Executive Order and OMB guidelines provide a blue-

The Journal of Law, Medicine & Ethics, 52 S1 (2024): 70-74.

print for developing federal AI standards.[21] Within these efforts, however, the public health perspective is nonexistent. AI risks often amount to population-level harms, and public health ethics have evolved to address these unique risks. In an analysis of 638 soft law frameworks, not one had a public health focus.[22] AI governance lacking this perspective could prevent useful applications of AI in public health and impede government regulation of AI as a structural determinant of health.

Conclusion

Since data are essential to public health practice, laws that regulate data are critical dimensions of public health authority. Long ago, the public health paradigm expanded beyond biological determinants of health to include political, environmental, and social determinants of health. Similarly, the scope of public health data governance must expand beyond traditional health privacy laws — like HIPAA — to be inclusive of the data that reflect the political, environmental, and social factors that impact our health. These health-adjacent data are at risk of being locked out of future public health informatics by the current wave of laws regulating data and their processing.

Public health agencies and organizations would be well advised to follow legislative developments, educate policymakers on preserving access to data, and contribute to parallel efforts to standardize DUA terms. The inclusion of legislative exceptions that permit data to be used, transferred, and processed for public health purposes is an effective means to support future public health informatics activities. However, care should be taken to restrict inappropriate data use and ensure established ethical principles serve as a lodestar for public health data governance.

Acknowledgements and Disclaimer

The authors did not receive funding for this work and have no conflicts to disclose. This article discusses general developments and is not intended to provide legal advice.

References

1. American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022).
2. C.F. Kerry, *Will California Be the Death of National Privacy Legislation?* (July 11, 2023), Brookings, *available at* <https://www.brookings.edu/articles/will-california-be-the-death-of-national-privacy-legislation/> (last visited November 20, 2023).
3. A. Folks, *US State Privacy Legislation Tracker* (November 17, 2023), IAPP, *available at* <https://iapp.org/resources/article/us-state-privacy-legislation-tracker/> (last visited November 20, 2023); H.B. Deixler, et al., *Recently Enacted Health Data Privacy Laws in Washington and Nevada Pose Challenges for Businesses* (July 25, 2023), Latham & Watkins: Global Privacy & Security Compliance Law Blog, *available at* <https://www.globalprivacyblog.com/legislative-regulatory-developments/recently-enacted-health-data-privacy-laws-in-washington-and-nevada-pose-challenges-for-businesses/> (last visited October 20, 2023).
4. A.H. Greene, *How State General Privacy Laws Apply to Healthcare Providers* (January 31, 2023), Davis Wright Tremaine LLP, *available at* <https://www.dwt.com/blogs/privacy--security-law-blog/2023/01/privacy-healthcare-providers-hipaa> (last visited November 20, 2023).
5. C.D. Schmit et al., *Public Health Informatics Depends on Engagement with Privacy Legislation* (October 28, 2022), Health Affairs Forefront, *available at* <https://www.healthaffairs.org/content/forefront/public-health-informatics-depends-engagement-privacy-legislation> (last visited November 20, 2023); C. D. Schmit, B. Larson, and H. Kum, "Data Privacy in the Time of Plague," *Yale Journal of Health Policy, Law, and Ethics* 21 no. 1 (2021): 152; See Consumer Data Protection Act, VA. CODE ANN. §§ 59.1-575–59.1-585 (2021).
6. Washington "My Health My Data Act" §3(8) (HB 1155) (2023).
7. B.A. Fahey, "Data Federalism," *Harvard Law Review* 135 no. 4 (2022): 1007.
8. C.D. Schmit, et al., "Views on Increased Federal Access to State and Local National Syndromic Surveillance Program Data: A Nominal Group Technique Study with State and Local Epidemiologists," *BMC Public Health* 23 no. 1 (2023): 431.
9. World Health Organization, *WHO Guidelines on Ethical Issues in Public Health Surveillance*, ISBN: 9789241512657 (June 19, 2017).
10. See Schmit, et al., *supra* note 8.
11. See Congressional Research Service, *Immunization Information Systems: Overview and Current Issues*, R47024 (February 1, 2022), *available at* <https://crsreports.congress.gov/product/pdf/R/R47024> (last visited November 20, 2023).
12. U.S. Department of Health & Human Services, *From the Factory to the Frontlines: The Operation Warp Speed Strategy for Distributing a COVID-19 Vaccine* (September 16, 2020), *available at* <https://media.defense.gov/2020/Sep/16/2002498509/-1/-1/1/OPERATION_WARP_SPEED_STRATEGY_FOR_DISTRIBUTING_COVID19_VACCINE.PDF> (last visited November 20, 2023); Centers for Disease Control and Prevention, *Data Use and Sharing Agreement to Support the United States Government's COVID-19 Emergency Response Jurisdiction Immunization and Vaccine Administration Data Agreement*, *available at* <https://www.cdc.gov/vaccines/covid-19/reporting/downloads/vaccine-administration-data-agreement.pdf> (last visited Dec. 2, 2022).
13. See Governor Andrew M. Cuomo, Press Release, *Governor Cuomo Issues Letter to Secretary of Health and Human Services Urging Support for Underserved Communities and Protection for Undocumented immigrants in Vaccine Distribution Program* (December 1, 2020), *available at* <https://www.governor.ny.gov/news/governor-cuomo-issues-letter-secretary-health-and-human-services-urging-support-underserved> (last visited November 20, 2023); C. Antonios et al., *Why Some States Won't Share Race and Ethnicity Data on Vaccinations with the CDC-and Why That's a Problem* (February 16, 2021), COVID Tracking Project at The Atlantic, *available at* <https://covidtracking.com/analysis-updates/why-some-states-wont-share-race-and-ethnicity-data-on-vaccinations-with-the-cdc-and-why-thats-a-problem> (last visited November 20, 2023).
14. See CDC Data Use Agreement, *supra* note 12 at Appendix G (Q&A); President Joseph R. Biden, Jr., *National Strategy for the COVID-19 Response and Pandemic Preparedness* (January 2021), *available at* <https://www.whitehouse.gov/wp-content/uploads/2021/01/National-Strategy-for-the-COVID-19-Response-and-Pandemic-Preparedness.pdf> (last visited November 20, 2023).
15. See WHO, *supra* note 9.

The Journal of Law, Medicine & Ethics, 52 S1 (2024): 70-74.

16. C. Curran, *Streamlining Public Health Data Use Agreements for the Next Pandemic* (April 19, 2023), Health Affairs Forefront, *available at* <https://www.healthaffairs.org/content/forefront/streamlining-public-health-data-use-agreements-next-pandemic> (last visited November 20, 2023).
17. Centers for Disease Control and Prevention, *Public Health Data Strategy: Goal 4: 2-Year Milestones* (April 6, 2023), *available at* <https://www.cdc.gov/ophdst/public-health-data-strategy/goal-4-milestones.html> (last visited November 20, 2023).
18. T. Panch, et al., "Artificial intelligence: opportunities and risks for public health," *The Lancet Digital Health Correspondence* 1 no. 1 (2019): E13.
19. C.D. Schmit, M.J. Doerr, and J.K. Wagner, "Leveraging IP for AI Governance." Science 379 no. 6633 (2023): 646–48.
20. *EU AI Act: First Regulation on Artificial Intelligence* (June 14, 2023), European Parliament, *available at* <https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence> (last visited November 20, 2023).
21. See The White House, Press Release, *OMB Releases Implementation Guidance Following President Biden's Executive Order on Artificial Intelligence* (November 7, 2023), *available at* <https://www.whitehouse.gov/omb/briefing-room/2023/11/01/omb-releases-implementation-guidance-following-president-bidens-executive-order-on-artificial-intelligence/> (last visited November 20, 2023).
22. C.I. Gutierrez and G.E. Marchant, "A Global Perspective of Soft Law Programs for the Governance of Artificial Intelligence," SSRN Electronic Journal 3855171 (2021).

The Journal of Law, Medicine & Ethics, 52 S1 (2024): 70-74.