HHS Public Access

Author manuscript

*J Law Med Ethics*. Author manuscript; available in PMC 2016 April 01.

Published in final edited form as:

*J Law Med Ethics*. 2015 ; 43(0 1): 48–51. doi:10.1111/jlme.12215.

# The Role of Law in Supporting Secondary Uses of Electronic Health Information

**Tara Ramanathan, J.D., M.P.H.**,

Serves as a public health analyst with the Public Health Law Program (PHLP) at the Centers for Disease Control and Prevention (CDC), where she specializes in state and local government law related to emerging public health issues. She leads PHLP's efforts to promote legal epidemiology and oversees research projects on health care quality and financing and health information technology

**Cason Schmit, J.D.**,

Serves as a legal fellow in PHLP and works with CDC centers and offices and state, tribal, local, and territorial partners to promote the use of law as a tool to improve the public's health. He is actively researching the national legal landscape of the use and exchange of electronic health information

**Akshara Menon, J.D., M.P.H.**, and

Serves as a senior legal fellow in CDC's PHLP, where she collaborates with public health professionals to explore the relationship between public health and the law. She leads legal research projects on health system transformation, prescription drug overdose prevention, and emergency antiviral distribution

**Chanelle Fox**

Juris Doctorate candidate at Indiana University Maurer School of Law and a Masters of Public Health candidate at Indiana University

## Introduction

For decades, health information has been collected and shared for health care delivery and public health purposes. While the "primary use" of patient data for providing direct health care services is the cornerstone of health care practice, health departments rely on data sharing for research and analysis to support disease prevention and health promotion in the population.[1] As the U.S. health system undergoes a digital revolution, health information that was previously captured in paper form now can be captured electronically. Electronic health information (EHI) has transformed the efficiency, capacity, and functions of the U.S. health system.[2] For this reason, there is increased attention to the "secondary use" of electronic patient data for public health uses,[3] including disease reporting and investigation, syndromic surveillance, and patient-specific or population-level communications about health conditions and their associated risk factors. Secondary uses may also encompass clinical research, licensure, and payment for services.

Laws play an instrumental role in facilitating the recording and sharing of health information and granting protections to patients and providers. However, the transition from paper to electronic health information systems pose challenges to the legal environment surrounding

health data.[4] Laws governing access to and disclosure of EHI for secondary uses describe the type of information that can be shared and whether it identifies individual patients, the types of entities sharing the information, and the reasons for which the information is shared.[5] As the implications and challenges of EHI are understood, states are updating laws that once supported paper health records to include electronic health records (EHRs) and the secondary use of data. This article provides an overview of laws supporting secondary use of EHI data for public health purposes, the state law landscape surrounding the transition from paper to EHI systems, and legal tools available for public health uses of EHI.

## Federal Law Supporting the Implementation of EHI for Secondary Uses

Federal law establishes the foundation for secondary uses of EHI. Privacy and security provisions control the access, use, and disclosure of individually identifiable health information, and meaningful use provisions promote the use of health information technology (HIT) and EHRs among health care providers and patients.

The purpose for disclosure is central to existing and future secondary uses of EHI. The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule[6] defines protections for health data acquired for primary uses, while also permitting certain secondary uses for public health purposes. Providers may disclose protected health information (PHI) identifying patients without their authorization to a public health authority for purposes of preventing or controlling disease, injury, or disability under the public health exemption, or if required by law.[7] For other public health uses, providers may share a "limited data set" with treatment dates and zip codes, though providers may re-identify patients for public health alerts or case reports.[8] HIPAA also permits health care entities to use PHI for other potential secondary uses like quality assessment and improvement.[9]

As the implications and challenges of EHI are understood, states are updating laws that once supported paper health records to include electronic health records (EHRs) and the secondary use of data. This article provides an overview of laws supporting secondary use of EHI data for public health purposes, the state law landscape surrounding the transition from paper to EHI systems, and legal tools available for public health uses of EHI.

Federal monetary incentives encourage the "meaningful use" of HIT by providers and facilities and support state-based health information exchange for secondary uses.[10] The Health Information Technology for Economic and Clinical Health Act of 2009 specifies that meaningful use should embrace the goal of improving population health outcomes.[11] Centers for Medicare and Medicaid Services rules set up graduated requirements for receiving incentives, including the adoption of certified, interoperable EHR technologies and data sharing for specific secondary uses, such as syndromic surveillance, health information exchange, or population health.[12] To enable providers and facilities to attain these goals and advance secondary use of data, states are revising laws governing collection and sharing of health data.

## State Law Landscape Surrounding the Transition to EHI

State laws are transitioning to support the use of EHI for primary and secondary uses, particularly by health departments. State EHI laws provide authorizations for public and private entities to share data, impose requirements for the collection and storage of data, and outline consequences for non-compliance. Variations in state EHI laws will affect how health departments in many jurisdictions fulfill their essential public health functions, as well as the extent and impact of cross-jurisdictional or national use of EHI. CDC's Public Health Law Program (PHLP) leads research on EHI uses that are important to essential health department functions, and seeks to describe the landscape of state EHI laws through a 50-state assessment on primary and secondary use.[13] PHLP's research describes broad categories of primary use of data by health care providers, schools, and correctional facilities. Provisions related to secondary uses capture reporting requirements, registries, reimbursement policies, and mechanisms external to the health department.

Data collected from a recent assessment of state laws illustrate important variations in permissible EHI usage. The assessment examined 12 geographically-dispersed states and categorized the relevant legal provisions into three primary uses and 25 secondary uses. No single state's laws included every use category identified. Among the 12 states, all provided for primary use of EHI by providers or facilities. Laws enabling secondary uses were not as uniform. EHI provisions linked to vital statistics in 11 states, immunization information systems in 8 states, and cancer registries in 5 states. Nine states had health information organizations or exchanges, and 11 referenced the use of EHI by payers.[14]

The laws assessed reflect that states are using EHI differently and increasingly across government functions. For example, states are using laws to authorize the combination of discrete data sets, as when integrating vital statistics and immunization data in electronic registries and health information exchanges. States permit the use of EHI to better understand the quality of health care delivered regionally and at specific facilities and establish the authority and operation of health information organizations specializing in health information exchange. These provisions reflect marked differences from the laws governing paper records.[15]

Early evidence suggests that state laws vary widely in addressing health information generally, in addition to specific HIT and secondary uses of EHI. Reflecting these differences, state health departments may rely on legal tools to supplement existing legal authorities and support data sharing for public health.

## Legal Tools for Secondary Uses of EHI to Support Public Health

Legal tools, such as institutional policies and contracts, can sustain secondary uses by aligning data exchange and technological or functional capabilities between certain parties. Data use agreements (DUAs), business associate agreements (BAAs), the federal Data Use and Reciprocal Support Agreement (DURSA), computer matching agreements, and interservice and intra-governmental memoranda of understanding (MOUs) are options for governing access, use, and disclosure of EHI between organizations and jurisdictions. As

with any policies and contracts, the application of these legal tools must be consistent with the applicable statutes and regulations governing primary and secondary uses of EHI.

Some laws or systems established by laws may require formal agreements between institutions. Laws may require providers and facilities to maintain DUAs for activities like syndromic surveillance that permit sharing information from a limited data set without patient authorization.[16] DUAs can be used to facilitate both primary and secondary uses of PHI and deidentified information.[17] Entities must agree on who will share data and who will receive it, promise that the data will not be disclosed further, and ensure that the recipient will not re-identify patients from the data. These data may be used for voluntary public health surveillance and patient notification if a health department receiving data supplies a re-identification code to the contracting provider, who then re-identifies the patient and takes action.[18] DUAs may allow data to be further disclosed for research and healthcare operations.

Laws may also require providers and facilities to contract with business associates to create safeguards that protect PHI.[19] A business associate is an entity contracted to perform services using PHI on behalf of a HIPAA-covered entity, such as data analysis, utilization review, and billing.[20] Business associate agreements can facilitate the sharing of discharge data, clinical quality data such as adverse events, and claims data with public and private payors, and hybrid public health entities that use that data for health care quality review.

Because laws may not cover the technical details or infrastructure involved in the exchange of data, agencies and facilities may need other assurances that systems are in place and mutually understood. DURSA is a multi-party legal agreement that governs the standards, services, and policies related to web-based EHI shared between providers and facilities and the federal government through the Nationwide Health Information Network Exchange. All entities, organizations, and federal agencies that sign DURSA voluntarily agree to the framework of responsibilities, obligations, and expectations to promote safe and secure electronic health information exchange.[21] Providers and facilities that sign DURSA can exchange summary patient records for care coordination and disability determination with the Social Security Administration and submit state public health reporting information to CDC.

Laws can support agency or institutional policies that hold facilities or agencies responsible for certain activities through independent agreements. The Computer Matching and Privacy Protection Act of 1988 requires written agreements to establish safeguards to protect PHI matched by computerized matching programs.[22] Computer matching agreements permit federal agencies to verify that reimbursements from government benefit programs are accurate. State agencies also use computer matching for many data sharing functions, such as managing payroll records or verifying eligibility for federal benefit programs.

Differing laws between jurisdictions may necessitate extralegal agreements, especially for interstate EHI sharing. MOUs between governments and organizations for data and services can help increase the capacity of health departments to use EHI for emergency response activities, including responses to pandemic influenza, terrorism, and natural disasters.[23]

MOUs allow public health agencies to collaborate with law enforcement agencies, corrections systems, the judiciary, and other sectors to share PHI and de-identified data for public health emergency response and preparedness. Through these various legal tools, the legal environment surrounding the sharing and analysis of EHI for public health purposes can be strengthened to support the latest HIT policies and architectures.

## Conclusion

Effective sharing of EHI for secondary uses can support public health activities and cross-jurisdictional collaboration. While this article presents ongoing legal efforts to address the sharing of EHI for secondary uses, it remains to be seen whether the law will evolve at a pace commensurate to that of HIT. Topics for future research may address how law (1) incorporates where information is stored, including in facilities, regional health information organizations, or the cloud; (2) standardizes how information is stored and presented; and (3) impacts the sharing and analysis of EHI with public health agencies to better serve both providers and patients.

## Acknowledgement

This document was written by researchers in the Public Health Law Program (PHLP) in the Office for State, Tribal, Local and Territorial Support at the U.S. Centers for Disease Control and Prevention (CDC). The findings and conclusions in this summary are those of the authors and do not necessarily represent the official views of CDC. For further information related to state EHI laws, please contact PHLP at phlawprogram@cdc.gov or at (404) 498-0470.

## References

1. Safran C, Bloomrosen M, Hammond WE, et al. Toward a National Framework for the Secondary Use of Health Data: An American Medical Informatics Association White Paper. Journal of the American Medical Informatics Association. 2007; 14(1):1–9. [PubMed: 17077452]
2. Centers for Disease Control and Prevention (CDC). Status of State Electronic Disease Surveillance Systems – United States, 2007. Morbidity & Mortality Weekly Report. 2009; 58(29):804–807. [PubMed: 19644441]
3. Blumenthal D, Tavenner M. The ‘Meaningful Use’ Regulation for Electronic Health Records. New England Journal of Medicine. 2010; 363(6):501–504. [PubMed: 20647183] Hoffman S, Podgurski A. Big Bad Data: Law, Public Health, and Biomedical Databases. Journal of Law, Medicine & Ethics. 2013; 41(1, Supp.):56–60.
4. Petersen C, DeMuro P, Goodman KW, et al. Sorrell v. IMS Health: Issues and Opportunities for Informaticians. Journal of the American Medical Informatics Association. 2013; 20(1):35–37. See, e.g. [PubMed: 23104048]
5. Sengupta S, Calman NS, Hripcsak G. A Model for Expanded Public Health Reporting in the Context of HIPAA. Journal of the American Medical Informatics Association. 2008; 15(5):569–570. See, e.g. [PubMed: 18579843]
6. Pub. L. No. 104-191, 110 Stat. 1936 (allowing stricter state privacy restrictions)
7. CDC. HIPAA Privacy Rule and Public Health: Guidance from CDC and the U.S. Department of Health and Human Services. Morbidity & Mortality Weekly Report. Apr 11; 2003 52(1):1–12. 45 C.F.R. § 164.512(a), (b), (i) (2013) (stipulating that the provider must account for these disclosures to the patient when requested). *available at* <http://www.cdc.gov/mmwr/preview/mmwrhtml/m2e411a1.htm= (last visited February 4, 2015).
8. See, e.g., 45 C.F.R. § 164.514(e) (2013); see also Sengupta, *supra* note 6
9. U.S. Department of Health & Human Services. OCR Privacy Brief: Summary of the HIPAA Privacy Rule. 2003; 4–10 45 C.F.R. § 164.501 (2013) (defining health-care uses of PHI).

[hereinafter cited as OCR Privacy Brief], *available at* <http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf= (last visited February 4, 2015).

10. Burke, T. The Health Information Technology Provisions in the American Recovery and Reinvestment Act of 2009: Implications for Public Health Policy and Practice. 2010. 125 Pub. Health Rep. 141
11. 42 U.S.C.A. § 300jj-31 (2009) (enacted as part of the American Recovery and Reinvestment Act of 2009); 45 C.F.R. 158.151 (2011); 42 C.F.R. 495.6 (2013) (including a variety of health-care quality measures)
12. HealthIT.gov. Meaningful Use Criteria and How to Attain Meaningful Use of EHRs. *available at* <http://www.healthit.gov/providers-professionals/how-attain-meaningful-use= (last visited February 4, 2015)
13. Menon, A.; Ramanathan, T.; Schmit, C., et al. Assessing the Impact of Laws Related to Electronic Health Information. Poster Presentation at the American Public Health Association Annual Meeting; November 18, 2014; These data were collected in January 2014 from WestlawNext® searches using terms such as health, medical, record, database, electronic, digital, computer, internet, web-based, automated, health information exchange, health information technology, and health information organization. Use categories were defined from a PubMed literature review of scholarly articles published since 2009, and provisions were blind-coded with rigorous coding criteria by two or more licensed attorneys according to principal reference or cross-reference for each category
14. *Id.* (from research examining statutes and regulations from Florida, Indiana, Kansas, Maryland, Michigan, Minnesota, New Hampshire, New York, Oregon, Tennessee, Texas, and Virginia)
15. This analysis does not capture the implementation or enforcement of these provisions or agreements that exist outside state law to facilitate EHI access or use. Therefore, this research cannot be used to infer the extent to which a state is leveraging its legal authority to use EHI
16. See, e.g., N.H. Code Admin. R. Ann. He-W 950.06 (2006) (implementing HIPAA rules at 45 C.F.R. § 164.514(e)(1))
17. CDC. BioSense Background. See OCR Privacy Brief, *supra* note 10, at 9*available at* <http://www.cdc.gov/biosense/background.html= (last visited February 4, 2015)
18. 45 C.F.R. § 164.514(e)(2) v (2013); Sengupta, *supra* note 6, at 569-570
19. See, e.g., Or. Admin. R. 943-014-0415 (2014) (implementing the HIPAA Privacy Rule at 45 C.F.R. § 164.502(e))
20. Am. Recovery & Reinvestment Act of 2009. 45 C.F.R. § 160.103 (2014); see also the American Recovery & Reinvestment Act of 2009, which expanded the regulations on privacy of electronic health records and extended privacy protection to EHRs received and retained by business associates of covered entitiesPub. L. No. 111-5, §§ 13401, 13402, 123 Stat. 115
21. Restatement I of the Data Use and Reciprocal Support Agreement. 2014. *available at* <http://healthewayinc.org/images/Content/Documents/Application-Package/restatement_i_of_the_dursa_9.30.14_final.pdf> (last visited February 4, 2015)
22. 5 U.S.C. § 552a (2010) (amending the Privacy Act of 1974); 32 C.F.R. § 310.53 (2007)
23. HealthIT.gov. Inter-Organizational Agreements. *available at* <http://www.healthit.gov/policy-researchers-implementers/inter-organizational-agreements> (last visited February 4, 2015)CDC, Public Health Law Program. Model Memoranda of Understanding. *available at* <http://www.cdc.gov/phlp/publications/type/mmou.html> (last visited February 4, 2015).