Public Health Law

Office for State, Tribal, Local and Territorial Support
Centers for Disease Control and Prevention

Federal Public Health Laws Supporting Data Use and Sharing

The role of health information technology (HIT) in impacting the efficiency and effectiveness of healthcare delivery is well-documented.[1] As HIT has progressed, the law has changed to allow HIT to serve traditional public health functions. This issue brief summarizes federal laws supporting the use and sharing of health data within the developing public health HIT landscape.

Collecting patient data for providing direct healthcare services (commonly called "primary use") is the cornerstone of healthcare practice. In recent years, sharing of electronic patient data for public health uses has been given increased attention.[2] Health departments and other entities rely on data sharing for research and analysis to support disease prevention and health promotion in the population (commonly called "secondary use" of data).[3]

Law lays the foundation for the recording, storage, and use of electronic health information (EHI). For example, law plays a significant role in enabling health departments to use HIT to improve systems that individual patient information to track population health trends and interface with similar HIT systems used by healthcare providers and facilities. In addition, law supports the sharing of EHI to facilitate

[1] *See* Julia Adler-Milstein, & Ashish K. Jha, *Sharing clinical data electronically: A critical challenge for fixing the health care system*, 307 J. AM. MED. ASS'N 1695 (2012); David Blumenthal & Marilyn Tavenner, *The "Meaningful Use" Regulation for Electronic Health Records*, 363 NEW ENG. J. MED. 6, 501 (2010); Taylor Burke, *The health information technology provisions in the American Recovery and Reinvestment Act of 2009: implications for public health policy and practice*, 125 PUB. HEALTH REPORTS 141 (2010); Neil Calman, et al., *Strengthening public health and primary care collaboration through electronic health records*, 102 AM. J. PUB. HEALTH 13 (2012); Daniel J. Friedman, et al., *Electronic health records and US public health: current realities and future promise,* 103 AM. J. PUB. HEALTH 1560 (2013); Tiina Maenpaa, et al., *The utilization rate of the regional health information exchange: how it impacts on health care delivery outcomes*, 18 J. PUB. HEALTH MGMT. & PRACTICE 215 (2012).

[2] David Blumenthal & Marilyn Tavenner, *The "Meaningful Use" Regulation for Electronic Health Records*, 363 NEW ENG. J. MED. 6, 501 (2010); Sharona Hoffman & Andy Podgurski, *Big Bad Data: Law, Public Health, and Biomedical Databases*, J.L. MED. & ETHICS Suppl. 56 (Spring 2013).

[3] *See, e.g.*, Charles Safran, Meryl Bloomrosen, W. Edward Hammond, et al., *Toward a National Framework for the Secondary Use of Health Data: An American Medical Informatics Association White Paper*, 14 J. AM. MED. INFORMATICS ASS'N 1–9 (2007).

surveillance, emergency and outbreak response, and health communication, among other essential public health functions.

This issue brief summarizes federal laws that have shaped state, tribal, local, and territorial health departments' use of HIT, including

- Laws that promote healthcare providers' HIT implementation and use;
- Laws that address how EHI collected for primary uses can be shared with healthcare providers and others for primary and secondary purposes, including public health activities; and
- Privacy laws that govern the types of EHI that can be disclosed and the permitted uses of EHI.

Promoting Electronic Health Records to Improve Population Health

While health information collected for patient care has been used for public health purposes for decades, the transition from paper to electronic records has revolutionized the efficiency, capacity, and functions of the US health system. The electronic revolution in the healthcare sector spreads into the public health sector by improving the overall value of information and the ease of sharing it.[4] Federal law has been a driving force in HIT's implementation and use.[5]

Enacted as part of the American Recovery and Reinvestment Act of 2009, the Health Information Technology for Economic and Clinical Health (HITECH) Act launched reforms to promote the use of HIT by private providers serving Medicare and Medicaid beneficiaries.[6] HITECH Act provisions

- Established the Office of the National Coordinator for Health Information Technology and committees that provide standards and specifications for HIT quality;[7]
- Required federal agencies to use HIT and provide for its voluntary use by private providers;[8]
- Provided for testing, research, grants, and loans for implementation and demonstrations for HIT education, including financial assistance to states and tribes;[9]
- Applied privacy and security requirements and penalties to HIT and required audits and enforcement;[10] and
- Secured incentive payments through the Centers for Medicare and Medicaid Services (CMS) for professionals and hospitals that are deemed eligible based on their "meaningful use" of certified electronic health record (EHR) technologies.[11]

---

[4] Tara Ramanathan, et al., *The Role of Law in Supporting Secondary Use of Electronic Health Information,* 43 J.L. MED. & ETHICS (forthcoming 2015).
[5] *Id*.
[6] 42 U.S.C. ch. 156, *available at* www.healthit.gov/sites/default/files/hitech_act_excerpt_from_arra_with_index.pdf.
[7] 42 U.S.C. § 300jj-11.
[8] *Id.* § 17901.
[9] *Id.* §§ 17911, 17912, 300jj-31-300jj-38).
[10] 42 U.S.C. §§ 17921-17953.
[11] *Id.* § 300jj-31; 42 C.F.R. §§ 492.6, 492.310; *EHR incentive programs*, CENTERS FOR MEDICARE AND MEDICAID SERVICES, www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/index.html (last accessed Dec. 4,

Regulations set three stages of requirements for professionals and facilities to adopt certified EHR[12] technologies and use them for certain purposes, including public health promotion.[13]

The Stage 1 meaningful use regulations that became effective in 2012 set standards for data capture, use, and sharing that providers must meet for reimbursement.[14] The Stage 1 standards support EHR format uniformity and thus promote better care coordination and outreach to patients.[15] CMS guidelines clarify that "meaningful use" includes the goal of improving population health outcomes, thus establishing link between HIT in the medical community and public health.

In addition to the standards relating to patient care, Stage 1 meaningful use regulations include standards that can promote secondary uses of health data to support public health activities. For example, providers can demonstrate meaningful use by generating reports of patients with a specific health condition to foster quality improvement, identify and reduce disparities, support research, and facilitate outreach.[16] Providers can demonstrate Stage 1 meaningful use by using EHR systems to submit data to immunization information systems pursuant to applicable law.[17] Stage 1 also allows providers to demonstrate meaningful use by using EHR systems to communicate syndromic surveillance data to public health departments.[18]

For providers who demonstrate Stage 1 standards,[19] the Stage 2 regulations introduce new requirements for demonstrating meaningful use. As in Stage 1, Stage 2 requirements include standards that providers must adopt for incentive payments as well as a menu of standards to give providers some flexibility in demonstrating meaningful use.[20] Many Stage 1 requirements are incorporated in the Stage 2 regulations to aid progression between meaningful use stages.[21] Stage 2 standards include

---

2013) (providing Medicaid payments of $63,750 over six years and Medicare payments of $44,000 over five years for professionals who adopt certified EHRs by 2016, but a 1–3% graduated penalty for only Medicare payments for those physicians who do not by 2015).

[12] This issue brief uses the term electronic health record or EHR to refer to patient record systems operated by healthcare providers. In contrast, the term electronic health information or EHI to refers more broadly to digital health information that may or may not be stored in EHR systems.

[13] HealthIT.gov, *Meaningful Use Criteria and How to Attain Meaningful Use of EHRs*, http://www.healthit.gov/providers-professionals/how-attain-meaningful-use (last accessed Mar. 4, 2015); Health IT.gov, *ONC, and CMS EHR Incentive Programs and Certification* http://www.healthit.gov/policy-researchers-implementers/certification-and-ehr-incentives (last accessed Mar. 4, 2015); *EHR Incentive Programs supra* (laying out specific requirements for professionals under Medicare and Medicaid).

[14] 42 C.F.R. § 492.6.

[15] HealthIT.gov, *supra*.

[16] 42 C.F.R. §§ 495.6(e)(3), (g)(4).

[17] *Id.* §§ 495.6(e)(9), (g)(9).

[18] 42 C.F.R. § 495.6(e)(10), (g)(10).

[19] *See* Medicare and Medicaid Programs; Modifications to the Medicare and Medicaid Electronic Health Record (EHR) Incentive Program for 2014, 79 Fed. Reg. 171, 52910 (Sept. 4 2014) (providing a timetable illustrating the progression of meaningful use stages).

[20] *See* 42 C.F.R. § 495.6(j-m).

[21] *See* CMS.gov, *Stage 1 vs. Stage 2 Comparison Table for Eligible Professional* www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/Downloads/Stage1vsStage2CompTablesforEP.pdf (last accessed Dec. 29, 2014).

requirements for clinical care and interoperability for EHRs, including Health Information Exchanges (HIE), electronic prescribing, transmission of records across settings, and increased patient control.[22] Like Stage 1, Stage 2 includes standards that promote public health activities, including laboratory reporting, reporting to immunization information systems, reporting to cancer registries and other specialized registries, submitting syndromic surveillance data, and identifying patients with specific conditions.[23]

Stage 3, projected to take effect in 2017, seeks to improve quality, safety, efficiency, and health outcomes, emphasizing population health improvement.[24]

Encouraging Electronic Data Use and Sharing with Stakeholders

In addition to encouraging provider adoption of EHR's, HITECH's incentives encourage sharing health information with stakeholders, such as electronic reporting of laboratory results and syndromic surveillance data to public health departments, reporting vaccinations to immunization information systems, and sending healthcare quality data to CMS.[25] However, electronic sharing of EHI depends on the existence of a functioning technological infrastructure, interoperability of separate HIT systems, and, often, presence of organizations that facilitate information sharing between entities.

EHI sharing, broadly the "secure health data exchange between two or more authorized and consenting trading partners,"[26] is not possible without a technical infrastructure for the consenting trading partners to communicate. HITECH's incentive payments, which promote the "adoption and meaningful use of certified electronic health record (EHR) technology" by healthcare providers, also incentivize infrastructure development for EHI sharing by increasing the pervasiveness of HIT systems.[27] Moreover, providers may cite sharing EHI as a meaningful use of EHR systems to get HITECH incentive payments.[28]

HITECH also facilitates EHI sharing by giving the Office of the National Coordinator for Health Information Technology (ONC) the authority to endorse technical standards.[29] Electronic sharing of health information requires that EHR systems are interoperable, or capable of communicating with each other. Without set standards, EHR vendors might develop systems that are not interoperable. Because HITECH authorizes ONC to review and endorse technical standards for EHR systems, ONC can guide different EHR vendors on how to develop interoperable systems.

---

[22] Health Information Technology: Standards, Implementation Specifications, and Certification Criteria for Electronic Health Record Technology, 77 Fed. Reg. 171, 54163 (Sept. 4, 2012).
[23] 42 C.F.R. § 495.6(j-m).
[24] 79 Fed. Reg. 171, 52910.
[25] 42 C.F.R. § 495.6.
[26] HiMSS, *HIE and Meaningful Use Stage 2 Matrix*, *available at* http://www.himss.org/files/HIMSSorg/content/files/MU2_HIE_Matrix_FINAL.pdf (Dec. 2012) (last accessed Dec. 3, 2014).
[27] 42 C.F.R. § 495.2 (a).
[28] NORC, *Evaluation of the State Health Information Exchange Cooperative Agreement Program*, http://www.healthit.gov/sites/default/files/casestudysynthesisdocument_2-8-13.pdf (last accessed Dec. 4, 2014).
[29] 42 U.S.C.A. § 300jj-11 (2014).

In addition, ONC developed the State HIE Cooperative Agreement Program, which allocates funds to encourage states to facilitate health information sharing. EHI may be shared through a formalized system such as an HIE or a Health Information Organization (HIO), which can vary in structure, organization, function, and scope based on implementation. Health information sharing receives broad support from states, private entities such as EHR vendors, and the public. Ultimately, promoting health information sharing allows for consolidation of disparate data and communication of health status and risks for both primary and secondary uses.

Protecting Privacy and Ensuring Data Security

The ease with which electronic information can be created and shared highlights the need for the privacy and security of sensitive EHI. Federal laws set the foundation for sharing data from patients' EHRs. Most discussed in the literature are the privacy and security provisions that control the access, use, and disclosure of individually identifiable health information in the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule.[30]

The rules implementing HIPAA define protections for health data acquired for primary uses. The general rule under HIPAA is that patient authorization is required before data are used by or disclosed to other entities.[31] In addition to the protection against use and disclosure, HIPAA allows patients to view their health information and request copies.[32] While HIPAA limits the use and disclosure of health information, it also permits certain secondary use exceptions for public health purposes.

HIPAA provides certain circumstances under which patient data can be disclosed to health departments without patient authorization. Under HIPAA, providers may disclose identifiable patient data (protected health information or PHI) if required by law, allowing states to pass legal exceptions to HIPAA restrictions.[33] Providers may also disclose PHI to health departments without patient authorization for public health activities, such as communicable disease reporting, or to a public health authority to prevent or control disease, injury, or disability under the public health exemption.[34]

A covered entity may access, use, and disclose PHI for clinical research without an individual's authorization if 1) it obtains documentation of waiver of individual's authorization by an institutional

---

[30] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18 U.S.C., 26 U.S.C., and 42 U.S.C.); 45 C.F.R. Parts 160 and 164 (Subparts A and E) (2013); Deven McGraw & Alice Leiter, *A Policy and Technology Framework for Using Clinical Data to Improve Quality*, 12 HOUS. J. HEALTH L. & POL'Y 137, 141 (2012). Other federal laws govern the primary and secondary uses of specific types of data (*see generally* Confidentiality of Alcohol and Drug Abuse Patient Records, 42 C.F.R. pt. 2 (2002); Family Educational Rights & Privacy Act, 20 U.S.C. § 1232g (2013); Privacy Act of 1974, 5 U.S.C. § 552a (2010).

[31] 45 C.F.R. § 164.508(a)(1).

[32] *Id.* § 164.502; 45 C.F.R. § 164.524; 45 C.F.R. § 164.528; *but see* 45 C.F.R. § 164.512.

[33] 45 C.F.R. § 164.512(a) (2013).

[34] *Id.* § 164.512(b) (2013).

review board or privacy board; 2) the PHI is necessary for this research; or 3) the research is using PHI of decedents.[35]

Providers may disclose EHI without patient authorization when the data have been "de-identified," which usually involves removing 18 types of identification or data aggregation.[36] De-identification often limits the data's utility for surveillance of routine clinical data, but still permits re-identification by providers or regional health information organizations through randomized patient source codes should a public health alert or case report become necessary.[37]

Finally, providers may disclose a "limited data set," including dates and zip codes, without authorization and still re-identify patients if they maintain patient codes derived from certain identifiers.[38] For other ancillary secondary uses, including institutional "learning" related to quality assessment and improvement activities, HIPAA permits healthcare entities to access PHI.[39] These exemptions and permitted uses are central to many existing and future secondary uses of EHI.[40]

This issue brief was prepared by Tara Ramanathan, JD, MPH, public health analyst, Cason Schmit, JD, Oak Ridge Institute for Science and Education (ORISE) fellow, Akshara Menon, JD, MPH, ORISE fellow, Dawn Pepin, JD, MPH, ORISE fellow, and Gregory Sunshine, JD, ORISE fellow with the assistance of Matthew Penn, Director, JD, MLIS, with the Public Health Law Program (PHLP) within the Centers for Disease Control and Prevention's (CDC's) Office for State, Tribal, Local and Territorial Support.

PHLP provides technical assistance and public health law resources to advance the use of law as a public health tool. PHLP cannot provide legal advice on any issue and cannot represent any individual or entity in any matter. PHLP recommends seeking the advice of an attorney or other qualified professional with questions regarding the application of law to a specific circumstance. The findings and conclusions in this summary are those of the authors and do not necessarily represent the official views of CDC.

This issue brief includes laws enacted through December 2014. Published March 19, 2015.

---

[35] *Id.* § 164.512(i) (2013). HIPAA rules separately define clinical research as any investigation or evaluation created to develop or enhance generalizable knowledge. 45 C.F.R. § 164.501 (2013). The Common Rule further governs the use of PHI by participating departments and agencies researching human subjects (*see* Federal Policy for the Protection of Human Subjects, 45 C.F.R. pt. 46 (2005))

[36] Data can also be deemed to be de-identified if an expert determines that there is a "very small" risk that data could be re-identified. 45 C.F.R. § 164.514(b) (2013).

[37] Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 157 (Aug. 14, 2001); 45 C.F.R. § 164.514(b).

[38] 45 C.F.R. § 164.514(e) (2013); *see also* Soumitra Sengupta, Neil S. Calman, George Hripcsak, *A Model for Expanded Public Health Reporting in the Context of HIPAA*, 15 J. AM. MED. INFORMATICS ASS'N 5, 569–70 (2008).

[39] 45 C.F.R. § 164.501 (2013) (defining health-care uses of PHI); U.S. DEPARTMENT OF HEALTH & HUMAN SERVICES, *OCR Privacy Brief: Summary of the HIPAA Privacy Rule* 4–10 (2003), *available at* http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf (last accessed Mar. 4, 2015).

[40] Centers for Disease Control and Prevention, HIPAA Privacy Rule and Public Health: Guidance from CDC and the US Department of Health and Human Services, 52 MMWR 1 (Apr. 11, 2003), *available at* http://www.cdc.gov/mmwr/preview/mmwrhtml/m2e411a1.htm (last accessed Mar. 4, 2015).