J Ambulatory Care Manage
Vol. 38, No. 1, pp. 29–38

OPEN

Big Data and Ambulatory Care

Breaking Down Legal Barriers to Support Effective Use

Jane Hyatt Thorpe, JD;
Elizabeth Alexandra Gray, JD, CHC

Abstract: Big data is heralded as having the potential to revolutionize health care by making large amounts of data available to support care delivery, population health, and patient engagement. Critics argue that big data's transformative potential is inhibited by privacy requirements that restrict health information exchange. However, there are a variety of permissible activities involving use and disclosure of patient information that support care delivery and management. This article presents an overview of the legal framework governing health information, dispels misconceptions about privacy regulations, and highlights how ambulatory care providers in particular can maximize the utility of big data to improve care. **Key words:** *big data, confidentiality, disclosure, health information, health information exchange, HIPAA, legal, privacy, quality improvement, security*

WHAT IS BIG DATA?

The relatively new term "big data" is commonly understood as data exceeding the processing capacity of a conventional database system. Data are characterized as "big" relative to three Vs:

Volume: Big data comes in large, complex quantities. In 2013, the world's data supply was equivalent to 4.4 trillion gigabytes (Turner et al., 2014, p. 1).

Velocity: Big data arrives and must be analyzed quickly. For example, patient monitoring equipment produces about 1000 readings per second; in total, 2.3 trillion gigabytes of data are produced daily (IBM, n.d.). Analysis of data often must occur upon arrival so that useless information can be discarded and space preserved to store useful information (Dumbill, 2012). Furthermore, certain applications require real-time response to data.

Variety: Big data is of varying provenance, including:

- Web and social media (Facebook status);
- machine-to-machine (pacemaker feed);
- transactional (coded cost reports);
- biometric (fingerprints); and

Author Affiliation: *Department of Health Policy, Milken Institute School of Public Health at the George Washington University, Washington, District of Columbia.*

Professor Thorpe and Ms. Gray are both funded by the Robert Wood Johnson Foundation for work to develop and maintain an online resource of federal and state laws related to health information, including analyses, decision support tools, and comparative maps (www.healthinfolaw.org). In addition, Professor Thorpe is funded under a subcontract with ResDAC to provide guidance related to the Centers for Medicare & Medicaid Services' data release policies. Professor Thorpe also serves as a senior advisor in the U.S. Department of Health and Human Services Office of the National Coordinator for Health Information Technology. The authors thank Dr. Jeffrey Lerner and the ECRI Institute for addressing Big Data at their November 2013 annual conference and inviting Professor Thorpe to speak, which prompted this article.

The authors have disclosed that they have no significant relationships with, or financial interest in, any commercial companies pertaining to this article.

Correspondence: *Jane Hyatt Thorpe, JD, Milken Institute School of Public Health, George Washington University, 950 New Hampshire Avenue NW, 6th Floor, Washington, DC 20052 (jthorpe@gwu.edu).*

DOI: 10.1097/JAC.0000000000000059

- human-made (e-mails). (Institute for Health Technology Transformation, 2013, p. 6)

These data must be standardized, which can be time-consuming and expensive. Structured big data can be sourced from multiple marketplaces, including:

- pharmaceutical research;
- clinical information;
- activity and cost data; and
- patient behavior data. (Manyika et al., 2011, p. 42)

Multisource data permit the development of layered insights. However, proprietary rights and legal concerns may inhibit data's availability from some sources.

Three additional "Vs" are useful in understanding big data in health care (Marcus, 2014, p. 2):

Veracity: Data may be inaccurate when generated or lose meaning in translation, but the veracity of information used in medical decision making is of extreme importance.

Variability: Big data is variable when the same information has different meanings. A record listing "Oxford" as a patient's location may refer to the Oxford in any of 23 states or four countries. Abbreviations and misspellings add complexity. Big data solutions must resolve these ambiguities.

Value: Big data's value exists in its use, in accomplishing on a large scale what cannot be achieved on a smaller scale (Mayer-Schonberger & Cukier, 2013, p. 6). Aggregating all available information into a usable data set permits analysis to reveal correlations, trends, and patterns across populations.

Maximizing big data's utility requires innovative and cost-effective technology and analytics platforms. Supported by appropriate technical solutions, big data can be transformative for individuals, organizations, and populations. Consider that scientists spent 10 years and $1 billion to sequence the human genome. Using big data analytics today to accomplish the same task would take about two days and $5000 (Kolata, 2013).

BIG DATA AND HEALTH CARE

The abundance of digitized information creates numerous opportunities for a range of industries, many of which are leveraging big data to improve business processes and performance. Retailers such as Target and Amazon use big data to predict customer behavior, tailor marketing, and optimize supply chains (Schneider, 2013). In health care, big data has primarily been the province of organizations such as insurance companies and pharmaceutical firms, which generally have access to large amounts of information and the capital to do something useful with it. Health care, particularly the ambulatory care setting, lags behind other sectors in harnessing big data's potential, due to structural obstacles including underinvestment in information technology, legal concerns related to privacy and security, and technical complications with information exchange. Despite these barriers, health care has reached the tipping point, as more data, data sources, and solutions to collect, store, and process it are available than ever before at reasonable costs (Kayyali et al., 2013). A new era of data-driven care has arrived, ushered in by major changes to our health care system; ambulatory care providers should be prepared to join the big data revolution.

The pressure for better value in health care demands better payment and delivery methods that improve efficiency and cost-effectiveness. The advent of new models that incentivize greater coordination, including accountable care organizations, bundled payment programs, and health homes, requires the compilation and exchange of health information across the care continuum.

The supply of health care data is increasing exponentially as electronic health records (EHRs) grow ubiquitous. The proliferation of health information exchanges (HIEs) enables data sharing across providers and care settings. These technical innovations expand the breadth and depth of the information accessible to stakeholders (Kayyali et al., 2013).

Recent federal legislation and incentives have paved the way for big data. These include the Health Information Technology and Clinical Health (HITECH) Act's incentives for EHR use and the Patient Protection and Affordable Care Act's (ACA) new delivery and reimbursement models, the success of which depends on data collection and exchange between and among stakeholders. For example, avoiding the penalty for preventable readmissions requires the transfer of patient-level information among payers, hospitals, and ambulatory care providers. In addition, the Office of the National Coordinator for Health Information Technology (ONC) is facilitating information exchange through development of standards and technology-specific certification programs that harmonize exchange efforts and governance.

BENEFITS OF BIG DATA FOR HEALTH CARE

There are myriad examples of the ways big data can be leveraged to transform health care delivery, including reducing errors, identifying high-risk populations, supporting evidence-based medicine, and improving organizational processes. The examples briefly discussed later highlight reported innovations in inpatient care but are illustrative of the improvements that can result from applying big data innovations in ambulatory and other health care settings.

Reduce errors

Clinical decision support systems enhance efficiency, quality, and safety. Big data solutions use automated algorithms to make decisions in response to real-time information and check for risks against huge data sets of clinical information (Manyika et al., 2011). Computerized provider order entry is a clinical decision support tool that compares physician entries against medical guidelines and alerts for potential errors at the point of care (Terry, 2005, p. 141). Vanderbilt University's pediatric critical care unit integrated a big data solution into its computerized provider order entry and within three months reduced all types of errors by 95.9% (Potts et al., 2004).

Identify high-risk patients

Predictive models help providers tailor care to improve outcomes and reduce costs. Texas's Parkland Health integrated an application to scan for clinical and social indicators in patients' records before discharge and flag individuals likely to be readmitted unnecessarily (Jacob, 2013). Implementation of this big data solution led to a 31% reduction in certain readmissions, saving an estimated $500 000.

Evidence-based medicine

Big data solutions mine information to determine the most effective treatments of a given condition and improve treatment protocols. The University of Michigan Health System used big data to review blood transfusions and develop standardized procedures, reducing transfusions by 31% and monthly expenses by more than $200 000 (Institute for Health Technology Transformation, 2013, p. 8).

Improve processes

Using big data solutions, health care leaders can conduct root-cause analysis of poor or varied performance, optimize processes, and streamline operations (Hewlett Packard, 2012). California's MemorialCare Health System tracked and analyzed provider performance and used the results to reduce average patient stays by 0.2 days, lower the average cost per admission by $280, and improve several quality indicators, resulting in savings of $13.8 million in one year (Mathews, 2013).

Big data has big potential and challenges. Ambulatory care managers can capitalize on this potential by collecting the right data and applying the appropriate technical solution. Managing its challenges includes ensuring that all big data activities operate within the complicated and often misunderstood legal framework governing health care information privacy and security. While health information is subject to heightened protection, this need not operate as a barrier to its robust

use, as the laws permit a variety of activities through which to utilize big data. Understanding this framework and the various ways information can be used will enable ambulatory care managers to focus on maximizing big data's potential to improve health care delivery while avoiding common misconceptions related to complex health care information privacy and security laws and regulations.

LEGAL FRAMEWORK

The federal framework governing health information is a patchwork of disparate but often overlapping laws protecting certain types of information and information held by certain entities. States also have their own laws governing health information, which may be broader or more protective than federal laws.*

Federal laws and regulations

The Health Information Portability and Accountability Act of 1996

The Health Information Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules (the Rules) govern "protected health information" (PHI), information about an individual's physical or mental health condition, health care, or payment for care that identifies the person or includes information permitting identification (e.g., address, telephone number) (HIPAA Administrative Simplification Rules, 2013). The Rules do not apply to "de-identified information," which is information providing no reasonable basis to identify an individual. De-identification occurs when 18 specific identifiers are removed or an expert certifies that there is minimal risk that the information could be used to identify the individual. The Rules apply to "covered entities" (health plans, health care clearinghouses, and health care providers who electronically transmit health information) and "business associates" (entities that have access to or use PHI while performing certain functions or services on a covered entity's behalf)—collectively referred to in this article as "regulated entities."

The Privacy Rule

The Privacy Rule establishes the ways in which these regulated entities are permitted or required to disclose PHI without the individual's written authorization; any other type of disclosure requires authorization. Regulated entities are *required* to disclose PHI to the individual or his or her designated representative and to the Secretary of Health and Human Services for compliance investigations or enforcement. The Rule permits disclosure of most types of PHI *without authorization* in accordance with one of 13 broad exceptions, although authorization is generally required if disclosing psychotherapy notes or a minor's PHI. Regulated entities must limit most permissive disclosures to the minimum amount of PHI necessary to achieve the intended purpose for which the information was released.

Treatment, payment, and operations

Generally, regulated entities may disclose PHI without authorization for treatment, payment, or health care operations activities.

Treatment is the provision, coordination, or management of health care and related services among providers; consultation between providers; or patient referrals. Regulated entities may disclose PHI to enable the covered entity's or another provider's treatment activities.

Payment includes activities associated with obtaining premiums, fulfilling coverage responsibilities, providing benefits, and obtaining reimbursement. Regulated entities may disclose PHI to facilitate the covered entity's payment activities or the payment activities of another covered entity or health care provider.

Health care operations include six specified activities.† Regulated entities may disclose PHI to carry out the covered entity's operations and may disclose PHI to another

*For information about health information privacy laws: www.healthinfolaw.org

†See 45 C.F.R. § 164.501.

covered entity for certain operations if both covered entities have (or had) a relationship with the individual and the PHI pertains to that relationship.

Public interest and benefit activities

Regulated entities may disclose PHI without authorization for a variety of public interest activities, including to:

- legally authorized authorities to conduct surveillance, investigations, and interventions;
- Food and Drug Administration (FDA)-regulated entities regarding the quality, safety, or effectiveness of FDA-regulated products or activities; and
- a health oversight agency for audits and investigations of the health care system and government benefits.

Research

Regulated entities may disclose PHI without authorization for research if:

1. an institutional review board (IRB) or Privacy Board issues an authorization waiver;
2. the PHI will only be used "preparatory to research" (e.g., preparing a research protocol), will not be physically removed from the covered entity, and is necessary to complete the research; or
3. the research is solely on decedents' PHI.

Limited data sets

Regulated entities may disclose a limited data set without authorization for research, public health, or health care operations. A limited data set is PHI devoid of 16 direct identifiers but may include the following: city, state, zip code; dates; and characters or codes that are not direct identifiers. The parties must enter into a data use agreement that ensures the privacy and security of the limited data set.

Authorizations

PHI may be disclosed in accordance with an individual's written authorization. Patient authorizations must contain specific elements, and additional requirements apply when the intended disclosure involves the sale of PHI, marketing, or psychotherapy notes. The authorization must inform the individual of the possibility that PHI may be redisclosed by the recipient, which may not be a regulated entity.

"Compound authorizations," or an authorization to use or disclose PHI combined with any other legal permission related to a research study (e.g., informed consent), are permitted in certain circumstances.

The Security Rule

The Security Rule applies to regulated entities but protects only electronic PHI. Regulated entities must maintain appropriate administrative, physical, technical, and organizational safeguards to protect electronic PHI.*

The Common Rule

The Common Rule (2013) protects human subjects involved in federally funded research as well as identifiable information obtained from a subject. The Rule does not govern studies on existing patient information. Researchers generally must secure subjects' informed consent, receive approval from an IRB, and ensure compliance with the Rule in writing. Researchers may obtain an IRB waiver of informed consent requirements if risk to subjects is limited to breach of confidentiality. Ambulatory care providers conducting or assisting with clinical trials must comply with the Rule, as must providers collecting data on medical treatment to develop new knowledge and/or for publication.

The Genetic Information Nondisclosure Act of 2008

The Genetic Information Nondisclosure Act of 2008 (GINA) prohibits health plans and issuers from using genetic information to make eligibility, coverage, underwriting, or premium-setting decisions and from requesting or requiring that beneficiaries undergo genetic testing or provide genetic information.

*For more information: http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityruleguidance.html

Requests for voluntary provision of genetic information for research are permitted.

GINA also prohibits employers from discriminating against employees or applicants based on genetic information or using genetic information in employment decisions. Exceptions include acquiring genetic information in conjunction with voluntary employer-sponsored health or genetic services, through commercially and publicly available documents, or via workplace monitoring of biological effects of toxic substances. Permissibly acquired information may be disclosed to an occupational or health researcher and a public health organization in limited circumstances.

GINA is relevant when providers wish to acquire genetic information from employers and/or health insurers for research purposes.

The Privacy Act of 1974 and the U.S. Freedom of Information Act

The Privacy Act of 1974 protects identifiable information about individuals held by the federal government. A federal agency may release information to identified persons or their designees with written consent or pursuant to one of 12 exemptions,* including disclosures for statistical research and required by the U.S. Freedom of Information Act (FOIA).

FOIA provides that any person may request and access information contained in federal agency records, unless information is exempted from disclosure (FOIA, 2010). Exemption 6 exempts "personnel, medical, and similar files" from disclosures that "would constitute a clearly unwarranted invasion of personal privacy."

A 1979 court order held that physician-identifiable Medicare payment data were covered by FOIA Exemption 6 and disclosure would violate the Privacy Act (*Fla. Med. Ass'n v. U.S. Dep't of Health, Educ. & Welfare*). A 2013 order reversed this ruling, and in January 2014, the Centers for Medicare & Medicaid Services (CMS) announced its intention to release individual physicians' Medicare billing data in response to FOIA requests, meaning ambulatory care providers and others may request Medicare claims data under FOIA (Modified Policy on Disclosure of Amounts Paid to Individual Physicians Under the Medicare Program, 2014). CMS recently released claims data for Part B services provided by physicians and other health care professionals in 2012; these data may be used by anyone for any purpose (U.S. Department of Health and Human Services, 2014).

42 C.F.R. Part 2 (Part 2)

Forty-two C.F.R. Part 2 (Part 2, 2013) limits its disclosure of identifying information that could or does reveal that an individual received substance abuse treatment and applies to federally assisted programs providing substance abuse diagnosis, treatment, or referral. Almost all programs are federally assisted, including providers who participate in Medicare, have a Drug Enforcement Administration (DEA) number, or are federally tax-exempt.

Written patient consent is required for disclosure, with limited exceptions including disclosures to researchers with an IRB-approved protocol. Each disclosure made with consent must include a statement prohibiting the recipient from further disclosing the information without written consent or unless permitted by Part 2.

Part 2 is more restrictive than HIPAA. For example, providers subject to Part 2 cannot disclose substance abuse patient information outside the program for treatment, payment, or operations without consent. State law requirements may be even more restrictive.

State laws and regulations

States have wide latitude to define their own privacy framework. When using or disclosing identifiable health information, providers generally must comply with all applicable federal laws *and* any state laws providing enhanced privacy protections. States commonly have laws in the following areas:

Mental health: States' mental health laws may apply to certain facilities, practitioners, or patients, or govern all mental health information. Some states permit treatment

*See 5 U.S.C. § 522a(b).

disclosures to any provider, others permit disclosure only within the facility, and others require patient consent for any disclosure (Jost, 2006).

HIV/AIDS: States vary in the scope of laws governing confidentiality of HIV/AIDS information. States generally govern test results, although some protect all HIV-related information (Centers for Disease Control and Prevention, 2013). Some states prohibit any disclosure of test results without consent, whereas others provide no specific protections. Nearly every state permits disclosure without consent for treatment, and about half permit disclosure for anonymous research.

Minors: Federal laws are generally more protective of minors' information but defer to states to define the scope of a minor's privacy rights and capacity to consent to disclosures. For example, under Part 2, minors can consent to disclosure when the state grants minors the right to obtain substance abuse treatment without parental consent.

Case law

There is a growing body of case law addressing health information privacy. In *Sorrell v. IMS Health Inc.* (2011), the United States Supreme Court held that a Vermont law prohibiting the sale of records containing a physician's prescribing practices or the use of such records for marketing without the physician's consent was an unconstitutional violation of pharmaceutical and data-mining companies' free speech rights. In *Liberty Mutual Insurance v. Donegan* (2014), the Second Circuit Court of Appeals invalidated a Vermont law requiring insurers to submit claims, eligibility, and provider data to a state all-payer claims database, finding the law preempted by the Employee Retirement Income Security Act (ERISA).

Providers should be aware of the ways their information may be used and disclosed—the *Sorrell* case and CMS' new Medicare data disclosure policy open the door to disclosures that identify not just patients but providers as well.

OPPORTUNITIES AND BARRIERS

The actual and perceived legal challenges associated with utilizing patient health information are not unique to ambulatory care settings or even to big data itself. However, big data solutions can be used to improve care and lower costs in ways that may be of particular interest to ambulatory care managers. Several of these opportunities are discussed later, highlighting ways to use, release, and exchange patient information to support health care delivery while remaining compliant with the privacy and security laws and regulations.

Sharing and exchanging data using HIEs

Participation in HIEs offers providers an opportunity to access a broad cross-section of data. The HIPAA treatment and payment disclosure exceptions are particularly applicable. Providers may disclose PHI to any health care provider to coordinate or manage patient care, which enables exchange of patient information via an accountable care organization or health home. This information can be shared using an HIE if participants have business associate agreements with the disclosing providers. HIEs also enable information exchange between providers and entities operating outside the regulated domain. They can collect data from consumer research firms, for example, and make that information available for use by its participant providers.

HIEs can also facilitate the creation and exchange of de-identified data. HIPAA is the only law with specific requirements for de-identifying information, thus satisfying HIPAA's requirements is likely sufficient to comply with other privacy laws (U.S. Department of Health and Human Services, n.d.). Big data solutions can de-identify volumes of information or scrub-sensitive information from entire data sets; health information organizations—entities that perform oversight and governance functions for HIEs—can perform these activities as business associates and share that information with HIE participants and third parties.

Providers may cultivate relationships to pursue data-sharing opportunities,

particularly where partnerships with private institutions provide access to valuable information. Examples of these relationships abound: Premier, a group purchasing organization provides members with data-driven informatics derived from integrated sets of member-contributed data (Premier, 2014). Providers utilizing an EPIC EHR solution can access benchmark and reference clinical data from all EPIC customers (EPIC Systems Corporation, 2014).

Sharing and exchanging data to support alternative care delivery models

Many alternative patient engagement and care delivery models present an opportunity to cull data from sources outside the traditional health care domain, including patient-generated health information, which is not subject to HIPAA's requirements. Personal health records encourage patients to participate in their care through sharing information. Web sites such as www.PatientsLikeMe.com permit individuals to share health information to "compare experiences ... and control [their] health"—these data can then be used for research. Remote patient monitoring through mobile technologies such as mHealthCoach can be used to identify higher-risk patients and deliver targeted messages (mHealthCoach, 2013).

Health information can also be sourced from "exhaust data"—consumer behavior and sentiment data generated outside the health care space describing patient activities and preferences (Terry, 2014). Information curated by retailers and search engines can be a surrogate for traditional health information. Buying a pregnancy test with a pharmacy loyalty card and "liking" a disease support group on Facebook are transactions generating useful data. Integrating nontraditional data sources with clinical, claims, and administrative information using big data solutions offers opportunities to improve health and health care delivery.

Big data tools that leverage integrated data sets to support new models of care continue to develop. For example, Rise Health created a customizable accountable care organization dashboard that aligns patient data with provider goals to improve health care across multiple dimensions (Rise Health, 2014).

Sharing and exchanging data to improve quality

Big data can improve both health care delivery and administrative quality. The HIPAA operations exception permits disclosure of PHI for quality assessment and improvement; population-based activities to improve health or reduce costs; and business planning, development, management, and administration. Operations activities leveraging big data include analyzing EHR data to identify outcome variations or disease predictors; examining revenue cycles and targeting processes for optimization; and benchmarking provider productivity (Manyika et al., 2011). Tools that facilitate these activities include OutcomesMiner, which allows comparative analysis of data to identify and study clinical nuances in patient outcomes (Deloitte Consulting LLP, 2013). The Privacy Act and FOIA permit ambulatory care providers to access volumes of information from government agencies that can be used for benchmarking performance. Providers should consider the value of accessing their peers' information for use in implementing big data innovations.

Because HIPAA does not define "operations" beyond listing broad categories of acceptable activities, there is wide latitude to conform disclosures to this exception. Disclosures must support the disclosing provider's own operations, with disclosures for another covered entity's operations limited to quality assessment and improvement, evaluating provider performance, and fraud/abuse detection or compliance. Activities that "contribute to generalizable knowledge" are research and fall outside the operations exception. This is particularly relevant when distinguishing quality improvement from research—generally, quality improvement utilizes well-established techniques and is intended to immediately improve care (Welsh, 2013, pp. 867-868). Where providers produce knowledge of general importance to the health care system, the activity becomes research,

subject to HIPAA's research provisions and to the Common Rule.

Sharing and exchanging data to reduce costs

The government uses big data solutions to track fraud, waste, and abuse. Penalties for false claims submission can cost millions and bar providers from federal health care program participation. Providers should consider using big data solutions to identify false claims before submitting data to the government. Analyzing patient information to reduce or eliminate fraud, waste, and abuse is a permissible HIPAA operations activity.

Master key to all data: Patient consent

The common element in every federal statute and most state privacy laws is permitted disclosure with patient consent. In this big data era, obtaining patient consent to data use is a master key to unlock all of a patient's health information. Despite variations in legal requirements, efforts are underway to develop common consent forms enabling an entire care team (which may include nonmedical members) to use and access a patient's information for individual and population health purposes.

Obtaining consent may sometimes be impracticable, particularly when dealing with large patient populations, but providers should consider it an opportunity to engage patients in their care. Protecting patient privacy may improve the quality and reliability of health data (Hodge et al., 1999). A 2003 study indicated that patients were most likely to consent to data release when asked by their provider, indicating the importance of maintaining a trustworthy and open environment (Kass et al., 2003). The more providers connect with patients, the more providers can do with their information.

CONCLUSION

"The U.S. healthcare system . . . is characterized by more to do, more to know, and more to manage than at any time in history" (Institute of Medicine, 2001). Big data offers a variety of solutions to manage this knowledge and mission creep. Perceived barriers to use of health information are borne from misconceptions surrounding the legal framework for privacy. In reality, privacy laws offer a wealth of opportunities to effectively use health information and leverage big data solutions. Value in health care is derived from balancing health care spending and patient outcomes (Kayyali et al., 2013). Ambulatory care providers may be able to effectively and efficiently strike that balance using big data solutions.

REFERENCES

Centers for Disease Control and Prevention. (2013). *State HIV laws*. Retrieved from http://www.cdc.gov/hiv/policies/law/states/

Deloitte Consulting LLP. (2013, June 24). *Deloitte, Intermountain launch OutcomesMiner solution*. Retrieved from https://www.deloitte.com/view/en_US/us/Insights/browse-by-role/media-role/36a45fbd3b57f310VgnVCM3000003456f70aRCRD.htm

Dumbill, E. (2012, January 11). *What is big data? An introduction to the big data landscape*. Retrieved from http://strata.oreilly.com/2012/01/what-is-big-data.html

EPIC Systems Corporation. (2014). *Services: Content*. Retrieved from http://www.epic.com/services-content.php

Fla. Med. Ass'n, Inc., et al. v. U.S. Dep't. of Health, Educ., & Welfare, 479 F. Supp. 1291 (M.D. Fla. 1979).

Genetic Information Nondisclosure Act of 2008 (GINA), Pub. L. 110-223, 122 Stat. 881, Title II codified at 42 U.S.C. § 2000ff *et seq.* (2008).

Hewlett Packard. (2012). *From big data to knowledge: Value chain for CSPs* [White paper]. Retrieved from http://www.vertica.com/wp-content/uploads/2013/02/From-Big-Data-to-Knowledge-Value-Chain-for-CSPs-4AA4-3407ENW1.pdf.

HIPAA Administrative Simplification Rules, 42 C.F.R. Part 160, *et seq*. (2013).

Hodge, J.C., Gostin, L.O., & Jacobsen, P. D. (1999, October 20). Legal issues concerning electronic health information: Privacy, quality, and liability. *JAMA*, *282*(15), 1466–1471.

IBM. (n.d.). *What is big data?* Retrieved from http://www-01.ibm.com/software/data/bigdata/what-is-big-data.html

Institute for Health Technology Transformation. (2013). *Transforming healthcare through big data*. Retrieved from http://ihealthtran.com/big-data-in-healthcare

Institute of Medicine. (2001, March). *Crossing the quality chasm: A new health system for the 21st century* [Report brief]. Retrieved from http://www.iom.edu/Reports/2001/Crossing-the-Quality-Chasm-A-New-Health-System-for-the-21st-Century.aspx

Jacob, S. (2013, June 13). Health systems use 'big data' to cut costs, improve quality. *Healthcare Daily*. Retrieved from http://healthcare.dmagazine.com/2013/06/13/health-systems-use-big-data-to-cut-costs-improve-quality/

Jost, T. J. (2006). Appendix B: Constraints on sharing mental health and substance-use treatment information imposed by federal and state medical records privacy laws. In *Improving the quality of Healthcare for mental and substance-use conditions: Quality chasm series*. Retrieved from http://www.ncbi.nlm.nih.gov/books/NBK19829/

Kass, N. E., Natowicz, M. R., Hull, S. C., Faden, R. R., Platinga, L., & Gostin, L. O. (2003). The use of medical records in research: What do patients want? *Journal of Law, Medicine & Ethics, 31*, 429–433.

Kayyali, B., Knott, B., & Van Kuiken, S. (2013, April). *The 'big data' revolution in healthcare: Accelerating value and innovation*. Retrieved from McKinsey & Company website: http://www.mckinsey.com/insights/health_systems_and_services/the_big-data_revolution_in_us_health_care

Kolata, G. (2013, April 15). Human genome, then and now. *The New York Times*, p. D3.

Liberty Mutual Insurance Co. v. Donegan, __ F.3d. __, 2014 WL 401708 (2d Cir., February 4, 2014).

Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C., . . . Byers, A. H. (2011, May). *Big data: The next frontier for innovation, competition, and productivity*. Retrieved from McKinsey Global Institute website: http://www.mckinsey.com/insights/business_technology/big_data_the_next_frontier_for_innovation

Marcus, B. (2014). *Brainstorming outline: Combined subgroup deliverables* (Input Listing Doc. No. M0092). Retrieved from the National Institute of Standards and Technology Big Data Working Group website: http://bigdatawg.nist.gov/show_InputDoc.php

Mathews, A. W. (2013, July 11). Hospitals prescribe big data to track doctors at work. *The Wall Street Journal*. Retrieved from http://online.wsj.com/news/articles/SB10001424127887323551004578441154292068308

Mayer-Schonberger, V., & Cukier, K. (2013). *Big data: A revolution that will transform how we live, work, and think*. New York, NY: Houghton Mifflin Harcourt.

mHealthCoach. (2013). Retrieved from http://mhealthcoach.com/

Modified Policy on Disclosure of Amounts Paid to Individual Physicians Under the Medicare Program, 79 Fed. Reg. 3205 (January 17, 2014).

Part 2, 42 C.F.R. Part 2. (2013).

Potts, A. L., Barr, F. E., Gregory, D. F., Wright, L., & Patel, N. R. (2004, January 1). Computerized physician order entry and medication errors in a pediatric critical care unit. *Pediatrics, 113*(1), 59–63.

Premier. (2014). *About Premier: Mission and vision*. Retrieved from https://www.premierinc.com/wps/portal/premierinc/public/aboutpremier/missionvision

Rise Health. (2014). *Our products*. Retrieved from http://www.risehealth.com/our-products/

Schneider, S. (2013). 20+ examples of getting results with big data [Web log]. Pivotal POV: the official weblog of GoPivotal. Retrieved from http://blog.gopivotal.com/pivotal/news-2/20-examples-of-getting-results-with-big-data

Sorrell v. IMS Health Inc., 131 S.Ct. 2653 (U.S. 2011).

Terry, N. P. (2005). To HIPAA, a son: Assessing the technical, conceptual, and legal frameworks for patient safety information. *Widener Law Review*, *12*, 133–182.

Terry, N. P. (2014). Big data proxies and health privacy exceptionalism. *Health Matrix*. Advance online publication. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2320088

The Common Rule, 45 C.F.R. Part 46. (2013).

The Freedom of Information Act (FOIA), Pub. L. No. 89-487, 80 Stat. 250, codified as amended at 5 U.S.C. § 552. (2010).

The Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896, codified as amended at 5 U.S.C. § 552a.

Turner, V., Reinsel, D., Gants, J. F., & Minton, S. (2014). *The digital universe of opportunities: Rich data and the increasing value of the Internet of things* [White paper]. Retrieved from International Data Corporation website: http://idcdocserv.com/1678

U.S. Department of Health and Human Services, Centers for Medicare & Medicaid Services. (2014). *Medicare provider utilization & payment data: Physician and other supplier* [Data file and code book]. Retrieved from http://www.cms.gov/Research-Statistics-Data-and-Systems/Statistics-Trends-and-Reports/Medicare-Provider-Charge-Data/Physician-and-Other-Supplier.html

U.S. Department of Health and Human Services, Office for Human Research Protections. (n.d.) Appendix F. In *Secretary's Advisory Committee on Human Research Protections*. Retrieved from http://www.hhs.gov/ohrp/sachrp/appendixf.html

Welsh, B. C. (2013). Regulatory overlap and the Common Rule: Redefining research on human subjects and quality improvement. *University of Memphis Law Review, 43*, 847–878.