HSR Health Services Research

DOI: 10.1111/j.1475-6773.2010.01140.x
SPECIAL ISSUE: HEALTH SERVICES RESEARCH IN 2020

Data Governance and Stewardship: Designing Data Stewardship Entities and Advancing Data Access

Sara Rosenbaum

U.S. health policy is engaged in a struggle over access to health information, in particular, the conditions under which information should be accessible for research when appropriate privacy protections and security safeguards are in place. The expanded use of health information—an inevitable step in an information age—is widely considered be essential to health system reform. Models exist for the creation of data-sharing arrangements that promote proper use of information in a safe and secure environment and with attention to ethical standards. Data stewardship is a concept with deep roots in the science and practice of data collection, sharing, and analysis. Reflecting the values of fair information practice, data stewardship denotes an approach to the management of data, particularly data that can identify individuals. The concept of a data steward is intended to convey a fiduciary (or trust) level of responsibility toward the data. Data governance is the process by which responsibilities of stewardship are conceptualized and carried out. As the concept of health information data stewardship advances in a technology-enabled environment, the question is whether legal barriers to data access and use will begin to give way. One possible answer may lie in defining the public interest in certain data uses, tying provider participation in federal health programs to the release of all-payer data to recognized data stewardship entities for aggregation and management, and enabling such entities to foster and enable the creation of knowledge through research.

Health services research rests on the twin assumptions that good evidence can be created from health and health care data on patients, providers, and health care systems, and that these data will be available. This article focuses on the

second assumption, examining both the concept of data stewardship as well as the considerable legal barriers to data access and use that can exist, even when stewardship is present. A central policy question in the coming years is whether the growth of stewardship capabilities, coupled with increased expectation of evidence-informed health care providers and consumers, will combine to lessen or eliminate these barriers.

An intense struggle over health information access has been a hallmark of the health care system for decades. Advocates of greater data access insist on the need for data at the patient, provider, and health care system level, in order to advance understanding of quality, efficiency, safety, and health (McGlynn et al. 2003). Opponents raise a host of concerns, citing patient privacy, the confidential nature of the patient/professional relationship, and health information security. Naturally, opponents also are focused on their own interests, given the potentially deleterious impact of uncontrolled data access on their liability under a host of civil and criminal laws, as well as on their competitive market position. Indeed, a study of more than 500 HIPAA Privacy Rule cases found that one of the most common types of cases involved providers who resisted releasing health data to their own patients out of liability concerns (Rosenbaum et al. 2007). Despite the fact that shielding information from patients or failing to make use of information carries liability risks of its own (Institute of Medicine 2001; Rosenbaum et al. 2005; Rosenbaum and Painter 2010), health care providers and health plans tend to fight against broad health information transparency (Beckerman et al. 2008; Terry 2009).

If laws governing data access are to evolve, a key consideration will be the ability to demonstrate data stewardship, that is, the existence of mechanisms for responsibly acquiring, storing, safeguarding, and using data. Permitting greater access to data for the creation of knowledge about how the health system works will depend on whether policy makers are able to strike a balance between the importance of health information to society on the one hand and the need to protect legitimate patient and provider interests on the other (interests that actually may work at cross purposes, at least when consumers, patients, and payers want more accessible information about network provider performance) (Cartwright-Smith and Rosenbaum 2009).

Part of the equation in striking this balance will be whether data used for research can be safely and securely handled, so that evidence can be created

---

Address correspondence to Sara Rosenbaum, JD, Department of Health Policy, George Washington University, 2021 K Street NW, Suite 800, Washington, DC 20006; e-mail: sarar@gwu.edu

without compromising these legitimate interests. The evolution of health information storage and use technology, discussed elsewhere in this collection, has made the effort involved in trying to strike this balance more worthwhile perhaps, because it is now possible to manage research in safe and secure data enclave environments. The question becomes how long the social and legal realignment will take in order to assure full use of this technology, a question that has arisen in health policy many times before, as new technologies alter the health care landscape. Indeed, technology transformed social expectations regarding the professional standard of care itself, producing enormous changes in the law as a result (Jacobson 2006). This time is no different, and indeed, the health information technology provisions of the American Recovery and Reinvestment Act of 2009[1] (which included the HITECH Act), coupled with health reform's focus on efficiency, performance improvement, and comparative effectiveness research, suggest a quickening of the interest in health information. Indeed, the Patient Protection and Affordable Care Act (PSL 110-148) places a premium on health information to create the knowledge that is essential to improving quality, reducing cost, and promoting population health.

Data Stewardship and Governance Defined: Insight into Stakeholder Views

The concept of data stewardship is rooted in the science and practice of data collection and analysis and reflects the values of fair information practice (Diamond et al. 2009). Data stewardship denotes an approach to the management of data, particularly data, however gathered, that can identify individuals. Data stewardship can be thought of as a collection of data management methods covering acquisition, storage, aggregation, and deidentification, and procedures for data release and use. The concept of a data steward is intended to convey a fiduciary (or trust) relationship with data that turns on a data manager whose loyalty is to the interests of individuals and entities whose data are stored in and managed by the system.

Data governance is defined as the process by which stewardship responsibilities are conceptualized and carried out, that is, the policies and approaches that enable stewardship. Data governance establishes the broad policies for access, management, and permissible uses of data; identifies the methods and procedures necessary to the stewardship process; and establishes the qualifications of those who would use the data and the conditions under

which data access can be granted. With the advice of system stakeholders, stewardship prioritizes resource investment into the knowledge creation deemed essential to health system reform.

Experts have posited that health data stewardship necessitates entities that acquire, hold, and aggregate information, releasing it for use in research. Stewardship of health information data compels "trust and competency; adoption of technology; and new models for data exchange (and new skills for managing health information) that include the patient as part of the data supply chain."[2] Health data stewardship rests on critical assumptions: first, that it is possible to gain access to data; second, that data stewardship will deal with identifiable patient and provider information; and third, that research protocols and technology exist to enable the safe and secure use of personal health data, such as research protocols that avoid the creation of large, static data bases susceptible to leaks or tampering.[3]

Insight into how stakeholders view data stewards can be gleaned from public comments in response to a 2007 request for information (RFI) focusing on a national data stewardship project, which was issued by the Agency for Health Care Research and Quality (AHRQ). The comments shed light on stakeholder positions regarding the need for and value of data stewardship entities with the capacity to both manage data in a safe and secure manner while also assuring proper governance over matters of data policy.

The 2007 RFI represented AHRQ's effort, acting under its broad agency mandate, to enable the types of technology advances that would in turn help improve health care quality.[4] The RFI sought information on the establishment of a national health data stewardship entity (NHDSE) to support a performance measurement and reporting effort of the type recommended by the Institute of Medicine (2004) in an earlier report. The RFI sought stakeholder public comments regarding the structure, functions, and roles of a data stewardship entity (the terms "stewardship" and "stewardship entity" were left undefined). AHRQ sought input on the characteristics and functions of an NHSDE, identifying a series of areas of agency interest, including public–private governance, mission, and the adoption of "uniform operating rules and stands for sharing and aggregating public and private sector data on quality and efficiency."[5] AHRQ also sought input on the entity's role in guiding the " implementation of . . . national operating rules and standards" and in providing "a framework for collecting, aggregating and analyzing data, to afford means of more effective oversight of health care data analyses and reporting.. ."[6] AHRQ thus envisioned an entity that, in addition to acting as a data repository and manager, would possess policy making

functions, advising public agencies in standard-setting regarding the acquisition, management, and use of health information, as well as on priority matters for research.

The RFI envisioned an entity apart from AHRQ itself and possessed of certain powers, including the power to collect and hold data and the power to advise agencies on research priorities and on the methods and approaches to be used in evaluating the data. In this sense, the entity would go beyond the technical functions of a repository and would enter the realm of policy development and advisement. Reflecting this desire to go beyond technical aspects, AHRQ posited a series of proposed precepts: objectivity; independence in governance; knowledge-based conduct and procedures; responsiveness; trustworthiness; adaptability; transparency; timeliness; collaborative style; and sustainability.[7] ARHQ sought input into the need for and value of such an entity: its roles and responsibilities; key challenges and risks in creating and sustaining the entity; the entity's potential role in characterizing and evaluating the "comprehensiveness, accuracy, and reliability of shared and aggregated health care quality measurement data"[8] stakeholder governance models; methods for assuring the avoidance of conflicts; priority areas of activity; and whether existing organizations might be suitable to perform such a role.

The responses from the field were notable both for the number of commentators and the breadth of their responses. In all, AHRQ received 136 responses (24 from organizations or corporations and 112 from individuals).[9] The responses, as summarized by AHRQ,[10] illuminated a range of viewpoints regarding a health information data steward with a potentially expansive role.

Commenters offered variable understanding of a data steward, including its definition, duties, mission, and functions. No clear group of proponents or opponents emerged. Consumer groups appeared to both support and oppose to the stewardship concept, as were health data information organizations, quality review organizations, payers, governmental agencies, and the health care industry.

On the threshold question of need for an entity, views ranged considerably. Proponents viewed a broadly conceived steward as offering an essential oversight mechanism for health data issues, organizing the various data collection, aggregation and sharing systems, assuring privacy, empowering consumers, and fostering collaboration among stakeholders. Opponents objected to a stewardship entity as an unnecessary competitor; others raised concerns about the absence of clear legal authority on which to act.[11] Others opposed the entity on more fundamental grounds related to the impact of such an entity on health care.

Commenters viewed data stewardship functionalities relatively narrowly, encompassing data storage and administration of data use "rules of the road." Numerous commenters viewed the entity as bringing no added value to the health information enterprise, indicating that private sector data managers already were doing a good job, again underscoring the proprietary interest in data control and access. Specific opinions on entity roles ranged from the granular (e.g., the entity could carry out quality review activities) to the broadly conceptual and collaborative, such as working with various stakeholders to set priorities, procedures, and standards for data collection, sharing, analysis, and use. The comments evidenced tension over whether a data steward should take on standard-setting and policy making functions or simply carry out technical responsibilities related to data collection, aggregation, and use. In other words, there was no consensus over whether a steward would be a policy actor, a consensus builder, a standard setter, a technician, or all of the above.

With respect to the question of public/private collaboration, commenters voiced concern over the potential conflict between government as both a health care regulator and a health information and performance standard-setter. Some commenters viewed government as identifying sources of data, building consensus around standard performance measures, and providing guidance on data collection, aggregation, and use methods. At the same time, numerous commenters viewed the private sector as the actual data collectors and information producers, underscoring the proprietary interest in data.[12]

Few commenters offered views on entity structure and governance, focusing instead on technical functions rather than on questions such as the process of governance (i.e., whether such an entity should have the public access trappings of a formal governmental advisory committee) such as public notice and open access, comment periods on pending policies, and a public record for decision making. In addition, the comments identified numerous technical, operational, risk-management, financial, legal compliance, and political challenges and noted the difficulty of gaining buy-in to the concept of group acceptance. AHRQ's own analysis of the comments found that "stakeholders providing comments generally agree that it will be a challenge to provide a framework that encourages participants to conform to community-wide data quality expectations."

Of most interest perhaps were the philosophical comments, suggesting the depth of skepticism about the notion of health information access and use. Certain commenters viewed stewardship as an inherent risk to the provider/patient relationship because of what they saw as the tension between the

provider/patient relationship and the intrusion of health information via a data steward with large powers into that relationship. Rather than viewing information as strengthening the provider/patient relationship, these commenters concluded, in AHRQ's words, that health information actually would lead to an "erosion of patient rights" including

> "unwanted disclosures and research, potential embarrassment, fear in and outside the doctor's office, privacy violations, genetic discrimination, breaches in the confidential patient–doctor relationship, profiling and surveillance, outside controls on the practice of medicine, and health care rationing. This concern extends to the notion that an NHDSE would "own" medical data of individuals and lead to the elimination of the citizen's ability to exercise privacy, consent, and ownership rights over medical record information—including genetic information and DNA, placing these rights in the hands of NHDSE directors.[13]

These commenters focused not on the operational and practical, but instead on the enduring conceptual issue: whether information about health care performance at the provider level should be more accessible. In this regard, the comments reflect the perpetual tension over the role of government and over the extent to which efforts to produce knowledge about health care can be perceived as piercing the relationship between health care professionals and patients in damaging ways.

The Underlying Tension: Access to Data

A data steward assumes the availability of data to be stewarded. In this regard, the environment is clouded. Concerns reflect those that are familiar to persons steeped in issues of privacy and confidentiality, namely, the capacity of stewardship to enable the unmasking of data generated by health care, for use in a broader system context. But the concerns go beyond those embedded in patient rights and reach into the business side of health care, which like any business, depends on the ability of competitors to shield information that may carry business, legal, or social costs.

Without question, government has the power to establish a data steward, and indeed has done so through enactment of a Federal Coordinating Council for Comparative Effectiveness Research under health reform.[13a] Indeed, government has routinely authorized the collection and use of health information to guide its own practices, relying on its power to tax, to spend, and to regulate commerce (Chemerinsky 2008). Vast amounts of health care data are reported to federal agencies under Medicare and Medicaid and numerous other federal

health programs authorized under an array of federal laws. Hospitals' disciplinary actions against physicians are similarly collected and analyzed. Public health agencies at all levels of government collect, store, and use personal information as part of public health practice (Lee and Gostin 2009).

At the same time, certain considerations have prompted government to take a "go slow" approach to the task of using its powers to create and amass information that flows from health care and that in turn would enable more rational decisions regarding the allocation of resources or the advancement of population health. Some of these considerations reflect the ongoing and unsettled nature of privacy and security safeguards, despite advances (Chemerinsky 2008). Others reflect the professional and powerful business interests inherent in health information, which have the capacity to push back against disclosure despite the enormous federal investment in health care. Indeed, even as government officials have become increasingly focused on the need to know more, the health care industry has succeeded in introducing even greater legal shields to protect their conduct from public view. Recent examples include the Patient Safety Quality Improvement Act,[14] which establishes a federal privilege against the disclosure of "patient safety work product," and the special exemptions from public reporting applicable to Medicare Part D prescription drug plans.[15]

Health Information Privacy

Numerous experts point to the imperfect nature of existing privacy and security standards.[16] Amendments to the HIPAA Privacy Rule contained in ARRA are designed to strengthen existing standards by expanding the range of entities subject to the reach of the Privacy Rule, adding security protections, imposing sanctions for failure to notify of breaches, and broadening of patients' rights to withhold consent for certain uses of information.[17]

The Common Rule[18] applies to research, providing added safeguards against unauthorized use of data. In its study, the Institute of Medicine (2009) recommended simplification of data use in research, chief of which were reforms to allow health information custodians to disclose personally identifiable health information without consent to "prescribed persons or entities" who have in place "practices policies and procedures to protect the privacy and confidentiality of personally identifiable health information."[19] The IOM reports similar practices in the United Kingdom, where the practice of strong data stewardship and advances in data technology[20] support such evolutionary standards.

Other federal and state laws addressing access to and use of certain types of data, such as genetic information[21] or information related to mental illness or addiction disorders (Beckerman et al. 2008) pose challenges as well, in their requirements for specific informed consent about data use. How these laws may evolve over time will depend in all likelihood on the safety and security track record that is amassed by data stewards, as well as the extent to which the value of the knowledge gained from better data access is understood in relation to the risks associated with allowing patient and provider data to be amassed and translated into health system evidence.

Data Ownership and Access

While privacy considerations slow the march toward data access, issues of ownership—in both a personal and business context—become highly pertinent as well. There is surprising and wide-ranging uncertainty in the law regarding the ownership of health information contained in medical records, claims forms, and other data repositories spread throughout the far reaches of the health care system. The law regards records holding data as property owned by their creators (with certain access rights granted to patients, insurers, and government agencies as a matter of federal or state law, as is the case with the HIPAA Privacy Rule).[22]

But the question is whether the data themselves are owned. There are strong arguments that health information cannot be owned, at least not in its original form. The continuing unsettled nature of the problem can be expected to intensify as paper medical records give way to an electronic highway along which information is free to move. As Professor Mark Hall has observed, ownership of information was never in doubt in an age of paper, because the paper record containing the information was owned by its creator (subject to certain rights of access at common law and under federal and state statutes). However, the electronic information age has ushered in an era in which the content of information can be "digitized and freed from any particular storage medium," (Hall 2009) thereby creating uncertainty as to the right of ownership and control.

Thus, while the Privacy Rule may create a right of access for individual patients or government investigations, it does not settle the far larger question where the future of research is concerned: how to gain access to the vast amounts of information essential to understanding health care quality, safety, efficiency, and health outcomes. Disclosure can create professional, business, and legal liability risks, as evidence of ineffectual health care—or care that falls

below evidence-based standards—becomes available potentially at an identifiable system practice level. Furthermore, health information can be commoditized into a lucrative business of its own. Professor Marc Rodwin has written that "organizations with medical, prescription, and billing records treat patient data as if those data were their private property" (Rodwin 2009). As Rodwin notes, the health care industry is able to sell deidentified patient data for billions of dollars, creating an additional business rationale for withholding data from a publicly accountable stewardship entity.

The conflicts between providers and consumers that these divergent interests can create can be seen in Freedom of Information Act litigation brought by consumers to gain access to Medicare physician fee data in order to provide public information regarding regional physician practice and medical costs. Holding that the consumer interest in data access under FOIA is outweighed by provider interest in privacy under the Federal Privacy Act, a federal appeals court denied data access.[23] This of course is not to say that the federal government cannot realign the balance of interests, which it has done in specific situations, such as the public reporting of performance data by Medicare participating hospitals and nursing facilities. But the rebalancing tends to take place under narrowly circumscribed conditions, ones that are more constrained than the broader data access needs of researchers.

A Way Forward

Data ownership versus data access suggests two distinct approaches to its resolution. The first, consistent with the concept of health information ownership (a position also supported by market advocates such as the Heritage Foundation) (Haislmeier 2009) would be to incentivize data access through payment for information. That is, part of the job of a data stewardship entity would be the purchase of health information considered by experts to be essential to the types of studies envisioned in the realm of patient safety, quality, comparative effectiveness, and population health. With the information output of health care essentially monetized, the government could negotiate with the industry over the scope and terms of access and use. The strength of this model is its recognition of data ownership rights. Its chief limitations are cost as well as the uncertainties that surround any market negotiation. The cost is particularly a matter of concern, since taxpayers essentially would be asked to pay twice: once for their support of federal health programs, taxpayer-supported coverage arrangements, and tax benefits

flowing to nonprofit health care entities; and then again for access to the information that their expenditures effectively created.

An alternative approach is to treat the information output of health care as a public good, available for use by entities structured and operated in accordance with principles of data stewardship. Stewardship entities could be federally chartered, with broad authority to collect, prepare, and support the use of health information in research. This model would achieve the broad goals set by advocates of evidence-driven care. In many respects it is this model that won the day in health reform, although subject to important limitations on the use of data.

A possible additional step would be to designate certain data uses as being in the public interest and to designate certain data as falling within a required data submission category as a condition of participation in federal health programs. In this context, the term "federal health programs" might span Social Security Act programs (e.g., Medicare and Medicaid), health programs of the Public Health Service Act (public health, health resources development and health professions, health research, and other direct population health investments). Congress' Article I Constitutional powers are sufficiently broad so that the reach of such a data submission requirement could encompass not only patient-level data emanating from provision of care directly under federal programs but also data resulting from the provision of care to all payers. Health data governed by submission requirements could be aggregated, managed, and prepared for use by data stewardship entities, which in turn could freely license the data for use by researchers who are able to demonstrate compliance with data stewardship responsibilities. This approach leaves data at the provider level available for subsequent uses, while at the same time assuring a flow of relevant health care data into stewardship entities capable of supporting the type of research enterprise viewed as essential to health system reform.

The comparative effectiveness research provisions in both the American Recovery and Reinvestment Act and health reform certainly point in this direction. The Patient Protection and Affordable Care Act broadly conceives of a new research authority with the power to both accelerate research related to comparative effectiveness and develop the research tools and supports necessary to enable research to flourish. The Federal Coordinating Council for Comparative Effectiveness Research envisioned by health reform is positioned to play the type of broad policy making role that in turn can lead to the establishment of data stewardship entities. Working under transparent policy standards and with authority to collect, aggregate, manage, and secure data,

these entities can enable the research and investigation on which a reformed health system rests, while linking to one another in common purpose to enable advances in population health.

ACKNOWLEDGMENTS

Joint Acknowledgment/Disclosure Statement: None.

NOTES

1. P. L. 111–5, 111th Congress First Session (2009).
2. AWA Invitational Meeting, Creating a Strategy for Data Aggregation and Stewardship" (Remarks of David Kibbe) [accessed on May 24, 2009]. Available at http://www.ahrq.gov/qual/performance/perform6.htm
3. Collecting and Sharing Patient Data, op. cit.
4. 72 Federal Register 30803 (June 4, 2007).
5. 72 Federal Register 30804.
6. Ibid, 30804.
7. Ibid, 30804–30805.
8. Ibid, 30805.
9. AHRQ, Summary of Responses: National Health Data Stewardship Entity Request for Information, issued by the Agency for HealthCare Research and Quality (AHRQ) on June 4, 2007 (FR04JN07-43).
10. AHRQ, Summary of Responses: National Health Data Stewardship RFI [accessed on April 5, 2009]. Available at http://healthit.ahrq.gov/portal/server.pt/gateway/PTARGS_0_7330_816199_0_0_18/NationalHealthDataStewardship_SummaryResponses.doc
11. AHRQ Summary Responses, p. 12.
12. See, for example, the Centers for Medicare and Medicaid Services (CMS) statement regarding its role in the development of quality measures and public reporting on provider performance [accessed on April 6, 2009]. Available at http://www.cms.hhs.gov/QualityInitiativesGenInfo/
13. AHRQ Summary Responses, op. cit, p. 12.

13a. PPACA §3302.

14. 42 U.S.C. §299 et. seq.
15. SSA Sec. 1860D-15 originally was interpreted as barring the use of Part D Plan data for purposes other than plan payment. Subsequent federal regulations expanded allowable uses to include research, public health, quality improvement 42 USC 1860D-12.
16. Ethical collection, storage, and use of public health data, op. cit.
17. ARRA Title XX, Subtitle D, §§13401–13410.
18. 45 C.F.R. §46.1 et. seq.

19. *Beyond the Privacy Rule*, p. 32.
20. Collecting and Sharing Data, op. cit.
21. Genetic Information Non-Discrimination Act of 2008, 42 U.S.C. §300gg-91.
22. 45 C.F.R. 160.310© (2009).
23. *Consumers' Checkbook Center for the Study of Services v United States Department of Health and Human Services*, 554 F. 3d 1046 (DC Cir., 2009).

REFERENCES

Beckerman, Z., J. Potts, J. Leifer, and S. Rosenbaum. 2008. "Health Information Privacy, Patient Safety, and Health Care Quality: Issues and Challenges in the Context of Treatment for Mental Health and Substance Use." *BNA Health Care Policy Report* 16 (2): 1–3.

Cartwright-Smith, L., and S. Rosenbaum. 2009. "Fair Process in Physician Performance Rating Systems: Overview and Analysis of Colorado's Physician Designated Disclosure Act." *BNA Health Care Policy Report* 17: 1–4.

Chemerinsky, E. 2008. *Constitutional Law*. New York: Aspen.

Diamond, C., et al. 2009. "Collecting and Sharing Data for Population Health." *Health Affairs* 28 (2): 454–66, 457.

Haislmeier, E. F. 2009. Health Care Information Technology: Getting the Policy Right (Web Memo 1131) [accessed on July 12, 2009]. Available at http://www.heritage.org/Research/HealthCare/wm1131.cfm

Hall, M. 2009. *Property, Privacy, and the Pursuit of Integrated Electronic Medical Records*. Wake Forest University Legal Studies # 1334963 SSRN [accessed on April 6, 2009]. Available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1334963

Institute of Medicine. 2001. *Crossing the Quality Chasm*. Washington, DC: National Academy Press.

Institute of Medicine. 2004. *Performance Measurement: Accelerating Improvement*. Washington, DC: National Academy Press.

Institute of Medicine. 2009. *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health through Research*. Washington, DC: National Academy Press.

Jacobson, P. 2006. "Medical Liability and the Culture of Technology." In *Medical Malpractice and the U.S. Health Care System*, edited by W. Sage and R. Kersh, pp. 112–28. New York: Cambridge University Press.

Lee, L., and L. Gostin. 2009. "Ethical Collection, Storage, and Use of Public Health Data." *Journal of the American Medical Association* 301 (1): 82–4.

McGlynn, E. A., S. M. Asch, J. Adams, J. Keesey, J. Hicks, A. DeCristofaro, and E. A. Kerr. 2003. "The Quality of Health Care Delivered to Adults in the United States." *New England Journal of Medicine* 348: 2635–45.

Rodwin, M. 2009. "The Case for Public Ownership of Patient Data." *Journal of the American Medical Association* 302 (1): 86–8.

Rosenbaum, S., P. C. Borzi, L. Repasch, T. Burke, and J. F. Benevelli. 2005. *Charting the Legal Environment of Health Information*. Washington, DC: GWUMC and the Robert Wood Johnson Foundation [accessed on July 11, 2009]. Available at

http://www.rwjf.org/files/research/Legal%20Environment%20Long%20Version.pdf

Rosenbaum, S., P. Barzi, and T. Burke. 2007. Does HIPAA Privacy Pose a Legal Barrier to Health Information Transparency and Interoperability?" *BNA's Health Care Policy Report* 15 (11): 1–13.

Rosenbaum, S., and M. Painter. 2010. "When New Is Old: Professional Medical Liability in the Information Age." In *Medical Professionalism in the New Medical Age*, edited by D. Blumenthal and D. Rothman, pp. 113–140. Piscataway, NJ: Rutgers University Press.

Terry, N. P. 2009. "What's Wrong with Health Privacy." *Journal of Health and Biomedical Law (V)*: 1–32.