The Report Committee for Paige Megginson Jennings
Certifies that this is the approved version of the following thesis report:

The Paradox of Physician Privacy

APPROVED BY
SUPERVISING COMMITTEE:

Supervisor: _____
David C. Warner

Co-Supervisor: _____
William M. Sage

The Paradox of Physician Privacy

by

Paige Megginson Jennings, B.S.

Report

Presented to the Faculty of the Graduate School of

The University of Texas at Austin

in Partial Fulfillment

of the Requirements

for the Degrees of

Master of Public Affairs

and

Doctor of Jurisprudence

The University of Texas at Austin

May 2012

Dedication

In memory of my dad, Lee Jennings, who was a constant source of encouragement, love, and friendship.

Acknowledgements

My sincere thanks go to my readers, Professor David Warner of the Lyndon B. Johnson School of Public Affairs and Professor Bill Sage of The University of Texas School of Law. Their thoughtful comments, insights, and encouragement were invaluable and contributed immeasurably to this Report.

I also thank the LBJ School's Writing Instructor, Talitha May, for the many hours she contributed in assisting Report writers this year and, especially, for her assistance in helping me to think through the structure of this Report.

Finally, I am grateful to my family for their love and support.

Abstract

The Paradox of Physician Privacy

Paige Megginson Jennings, M.P.Aff.; J.D.

The University of Texas at Austin, 2012

Supervisors: David C. Warner, William M. Sage

This Report examines the "paradox" of physician privacy: while physician privacy has been explicitly or implicitly invoked over the last century to defend physicians against greater transparency, proposals that might cause them economic harm, or interference by government or corporate entities, there has been little comprehensive work done to examine the substance and source of any privacy rights physicians may actually enjoy. This Report attempts to make three primary contributions with respect to physician privacy. First, the Report examines the current state of physician privacy and the legal framework that governs it. Second, the Report argues that physician "privacy" is not, and should not be considered, a unitary concept encompassing a singular meaning. Rather it is a broad umbrella term that encompasses not only a variety of legal protections for privacy, but guards against a variety of very different perceived harms. As a result, this Report argues that in evaluating policy initiatives, discussions about "privacy" implications can be counterproductive because the term obscures the real values, concerns, and policy judgments at play. To address this, the Report's third aim is the proposal of an analytical framework that policymakers and others may use to consider the

impact of various initiatives on the values and concerns that physician "privacy" actually protects: professional autonomy; economic considerations; personal dignity; and practical difficulties.

Table of Contents

Introduction

While many people understand the concept of patient privacy and the confidentiality of information about one's own health, physician privacy is something of a paradox. On one hand, at various times throughout the last century, physician privacy has been explicitly or implicitly invoked to defend physicians against greater transparency, proposals that might cause them economic harm, and interference by government or corporate entities. On the other hand, despite the invocation of "privacy" as an occasional defense against specific proposals, there has been little comprehensive work done to examine the substance and source of any privacy rights physicians may actually enjoy.

This Report attempts to make three primary contributions with respect to physician privacy. First, the Report examines the current state of physician privacy and the legal framework that governs it. Second, the Report argues that "privacy" is not, and should not be considered, a unitary concept encompassing a singular meaning. Rather it is a broad umbrella term that encompasses not only a variety of legal protections for privacy, but guards against a variety of very different perceived harms. As a result, this Report argues that in evaluating policy initiatives, discussions about "privacy" implications can be counterproductive because the term obscures the real values, concerns, and policy judgments at play. To address this, the Report's third aim is the proposal of an analytical framework that policymakers and others may use to consider the impact of various initiatives on the values and concerns that physician "privacy" actually

protects: professional autonomy; economic considerations; personal dignity; and practical difficulties.

Once policymakers consider "privacy" in terms of the underlying interests at play, they can more easily balance considerations of "privacy" against competing goals such as improvement of public health and health care quality, the empowerment of patients, and the control of health care costs.

This Report proceeds as follows: Chapter 1 discusses health care privacy protections in the United States and explains why, despite ad hoc efforts to protect physician "privacy," a comprehensive conception of physician privacy rights has largely been neglected. Chapter 2 demonstrates the importance of a more cohesive view of physician privacy to larger health system improvement. Chapter 3 considers the bounds of privacy broadly and outlines existing privacy law in the United States. Because general privacy law is a much larger body of law than that applied to protect physician information, Chapter 4 discusses how physicians have used the law and societal norms to guard their own privacy. A proposed analytical framework for evaluating privacy concerns is presented in Chapter 5. Finally, Chapter 6 concludes the Report and notes areas for future research and scholarship.

Chapter 1: Physician Privacy in a Changing Landscape

For over 2000 years, patients have enjoyed some measure of privacy with respect to their health information. However, the extent of "privacy" protections for physicians is far from clear. Physician privacy has at times been invoked to argue against proposals that would bring greater transparency to the profession and the health system. However, those who invoke physician privacy do so without giving content to the term. Do physicians in fact enjoy any "right to privacy"? If so, what does this right encompass?

HISTORICAL RECOGNITION OF PATIENT PRIVACY

Since 400 BC, doctors have been ethically bound to maintain the confidentiality of their patients' medical information.[1] For most of this time, physicians' obligations derived from professionally imposed norms and patients enjoyed few *legal* protections of their private information.

Legal protections for patient privacy began to be recognized as early as 1920 through a combination of state tort and statutory provisions.[2] However, many such protections were limited to the context of an existing doctor–patient relationship and thus did not extend patient privacy rights much farther than the physician's underlying ethical obligations.

---

[1] The Hippocratic Oath: Text, Translation, and Interpretation (Ludwig Edelstein, Johns Hopkins Press, 1943), *available at* http://www.pbs.org/wgbh/nova/body/hippocratic-oath-today.html#classical ("What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself, holding such things shameful to be spoken about.").

[2] *See, e.g.*, Simonsen v. Swenson, 177 N.W. 831, 832 (Neb. 1920) (recognizing on the basis of a state physician licensure statute a duty of confidentiality, the "wrongful" breach of which "would give rise to a civil action for the damages naturally flowing from such wrong"). *See also* Alan B. Vickery, Note, *Breach of Confidence: An Emerging Tort*, 82 COLUM. L. REV. 1426, 1428–30 (1982) (discussing cases recognizing breach of confidence actions against physicians).

The push for legal patient privacy protections in the United States surged in the latter half of the twentieth century. The factors driving this varied at different points in time. In part, the growth of the federal government led to more general attention to the information being collected and held about individual citizens and gave rise to interest in greater associated legal protections. In the health care context, a growing focus on patient autonomy in the 1960s as well as an increasing reliance on private health insurance and an associated risk that medical information could be used to deny coverage made privacy much more important as well. In the 1980s and 1990s, the emergence of HIV and AIDS brought into the public conscious the possibility that an individual's health status could also result in social, employment, and other discrimination. Finally, the development and increasingly widespread use of information technology in the last few decades has driven concerns about personal privacy in the health care context and beyond.

The result of advocacy driven by these varied factors was the development of state tort and statutory privacy protections and the promulgation of comprehensive federal health privacy regulations in 2000.

THE AD HOC APPROACH TO PHYSICIAN PRIVACY

Missing from the discussions of health privacy over the last 40 years has been any significant consideration of whether physicians have rights to or interests in privacy protection, and if so, what those rights should encompass.[3] Physician privacy rights have certainly been invoked at times to defend against particular initiatives. For example,

[3] *See, e.g.*, Greg Borzo, *Up the Data Stream Without a Paddle: Physicians' Right to Privacy in the Electronic World*, AMERICAN MEDICAL NEWS, Mar. 9, 1998 available at http://www.ama-assn.org/amednews/1998/net_98/logo0309.htm (lamenting the lack of attention paid to physician privacy).

physicians have invoked privacy and other concerns to fight off repeated efforts to make public the National Practitioner Data Bank, which houses information about physician malpractice settlements, judgments, and other disciplinary actions.[4]

However, the occasional mention of physician privacy interests has never resulted in a broader discussion of the privacy rights they currently have or any cohesive theory of the rights they should have.

Why might this issue have been neglected? Three primary reasons seem apparent. The first is the past dominance in health law and policy of the professional authority model and the fact that physicians have historically self-regulated and had the clout to fend off much external influence. The second reason, somewhat related to the first, is the long-vaunted sanctity of the physician-patient relationship and the control that physicians have typically had over their medical records. Third, practical and technological factors have meant that physicians never had to defend their privacy rights because they enjoyed de facto privacy protection.

Impact of the Professional Authority Model

Three primary paradigms—the professional authority model, the "modestly egalitarian social contract" model, and the market competition model—have competed to shape the development of health law in the United States and to influence how decision makers approach and resolve policy questions.[5] The professional authority model predominated from around 1880 to 1960 and had at its core the protection of physician

---

[4] Julie Barker Pape, Note, *Physician Data Banks: The Public's Right to Know Versus the Physician's Right to Privacy*, 66 FORDHAM L. REV. 975, 976–83 (1997) (describing the establishment of the NPDB, efforts to make its contents public, and arguments by the AMA and physicians that such publicity would violate physician).

[5] Rand E. Rosenblatt, *The Four Ages of Health Law*, 14 HEALTH MATRIX 155 (2004).

authority and autonomy and the goal of ensuring physician control over the regulation of their own profession as well as most decisions about medical treatment, delivery, and financing.[6] Professors Rosenblatt, Law, and Rosenbaum put it bluntly: "In virtually every area of health law . . . prevailing legal principles empowered the individual doctor in private practice to do as he saw fit, and insulated him from review and control by patients, hospitals, corporate employers, insurance companies, government, and even from other doctors."[7] Physicians closely guarded their own autonomy, in part by consistently opposing efforts to provide non-indemnity[8] and government-sponsored health coverage[9] and by securing legal prohibitions against the corporate practice of medicine.[10]

While this model was dominant, physicians enjoyed the professional clout and authority to fight off efforts at greater transparency. What's more, they likely faced few serious efforts at required disclosure. Physicians were expected to be more "moral" than other market actors and to have more of a responsibility to their patients,[11] additionally,

---

[6] *Id*. at 162–63. It is important to note that the modern physician, as we recognize her today, is a recently recent phenomenon. Medical education underwent profound changes in the late 19th and early 20th centuries and shifted from an unsophisticated, unregulated, ad hoc system, to one with significant grounding in (and greater legitimacy because of) science and research. After a 1910 report by Abraham Flexner, medical education came under significant centralized (physician) oversight: the number of medical schools was reduced along with the number of graduating physicians and licensure requirements and other barriers to entry into the profession were erected. All of these changes led to increased quality but also put pressure on supply and prices and helped to augment physicians' authority. Physicians eventually controlled access to most medical treatment including prescription drugs, other therapies and facility admissions, etc. *See* PAUL STARR, THE SOCIAL TRANSFORMATION OF AMERICAN MEDICINE (1982).

[7] RAND E. ROSENBLATT, SYLVIA A. LAW, & SARA ROSENBAUM, LAW AND THE AMERICAN HEALTH CARE SYSTEM 2 (1997).

[8] Physicians, through their national association, the American Medical Association (AMA), fought against non-indemnity insurance plans beginning in the 1930s, wanting to deal directly with patients and not wishing to be questioned about the price of their services or their medical judgments. *See id*. at 9–10.

[9] STARR, *supra* note 6.

[10] *Id*.

[11] *See* Kenneth J. Arrow, *Uncertainty and the Welfare Economics of Medical Care*, 53 AM. ECON. REV. 941 (1963).

patients tended to defer to their physicians' decisions and had far from the "consumer" mindset that many patients hold today.

Physician–Patient Relationship

A second reason that physicians had little need to consider privacy in any serious way relates to the physician–patient relationship. American Medical Association principles in 1934 stated that "No third party must be permitted to come between the patient and his physician in any medical relation . . . . The method of giving the service must retain a permanent, confidential relation between the patient and a 'family physician.'"[12] This confidential relationship not only helped to ensure confidentiality for patients, but also meant that information about physicians' practices were protected from external view.[13] In fact, patient medical records developed by a physician were considered to belong to the patient's doctor. Physicians making referrals to specialists would often be sent a letter in return with any new patient records and notes, thus reinforcing the primary physician's "ownership," so to speak, of the physician–patient relationship.[14]

De Facto Privacy Protection

The final reason that physician privacy has been a largely neglected topic is that physicians, even as their professional authority waned, have enjoyed de facto privacy protection. This has resulted in little reason, until recently, to analyze or question the matter further. Until the emergence of the market competition model and the

---

[12] ROSENBLATT, LAW & ROSENBAUM, *supra* note 7 at 25 (quoting the AMA's 1934 principles for "Sickness Insurance Problems in the United States").

[13] William M. Sage, *Regulating Through Information: Disclosure Laws and American Health Care*, 99 COLUM. L. REV. 1701, 1784–85 (1999) ("Historically, the absolute confidentiality of doctor–patient communications served not only legitimate patent care and privacy interests, but also helped the medical profession to preserve its economic power against managerial incursions by third parties.").

[14] Conversation with Professor William Sage.

development of more advanced information technology, reliance on paper charts, private payments, and indemnity insurance combined with a lack of corporate oversight or physician practice meant that doctors had near complete control over their practices and any resulting information. Physician services had only recently begun to be covered by health insurance through the formation (by physicians) of pre-paid Blue Shield plans in the 1930s and 1940s. Further, the government did not act as a significant payer until after the enactment of Medicare and Medicaid in 1965 and thus was not accumulating data about doctors either. This meant that it was virtually impossible to gather or compile data about physicians' patient loads, practice habits, outcomes, cost of care, etc.[15] The information remained in office filing cabinets or was otherwise generally decentralized because of a lack of consolidation among payers and a lack of technology. Outside entities could not obtain, much less analyze or aggregate information about physicians to compile quality rankings, practice patterns, comparisons with other providers, or the like.

CURRENT NEED TO CONSIDER PHYSICIAN PRIVACY

Many of the barriers to transparency that were provided by physician authority, the physician–patient relationship, and the practical limitations of data and technology have now subsided, making physician privacy more relevant.

Physician authority likely reached their apex during the 20th century.[16] Beginning in the 1960s, a new paradigm emerged in health law—the "modestly

---

[15] As noted above, this result was intended. Doctors had fought non-indemnity insurance plans in part to ensure as little interference as possible in their affairs.

[16] Sydney A. Halpern, *Medical Authority and the Culture of Rights*, 29 J. HEALTH POL. POL'Y & L. 835, 843 (2004) ("That health care movements and the growth of consumerism have empowered patients and, in doing so, diminished medicine's social standing are the core claims of deprofessionalization theory."). However, not everyone agrees. On the other side, some scholars argue that, although physician practice and physicians relationships with their patients have changed, these changes haven't resulted in a significant negative impact on physician authority. *See id.* at 845 (discussing the view of some that doctors' authority has not declined "over matters related to health and illness").

egalitarian social contract"—which shifted away from the professional dominance model and toward a theory in which the interests of patients and society were afforded greater weight.[17] Twentieth century feminism also contributed to this shift as women questioned their (mostly male) physicians and found alternative sources of medical treatment.[18] The result of these changes was that patients and their advocates placed greater value on patient autonomy and involvement in medical decision making. Patients demanded access to their medical records and generally took more control of their own health care decisions.[19]

The third major paradigm in health law, the market competition model, emerged in 1970s and 1980s and also chipped away at the authority enjoyed by physicians. The market competition has strands running counter to both the social contract and professional authority models previously at play[20] and holds that competition instead of government or professional authority should rein.[21] This model was in part a response to inflationary pressures resulting from existing private indemnity insurance and from the enactment of Medicare and Medicaid.[22] Managed care was one reaction to these cost growth trends and resulted in greater corporate control over physicians (although it also resulted in a brief backlash and resurgence of physician authority as patients rebelled

---

[17] ROSENBLATT, LAW, & ROSENBAUM, *supra* note 7, at 2; William M. Sage, *Reputation, Malpractice Liability, and Medical Error*, *in* ACCOUNTABILITY: PATIENT SAFETY AND POLICY REFORM 162 (Virginia A. Sharpe, ed. 2004) (noting that since the late nineteenth century, "[m]edical paternalism [has] receded as bioethicists focused attention on patient autonomy, and a consumerist mentality began to take hold).

[18] *See, e.g.*, Wendy E. Parmet, *Unprepared: Why Health Law Fails to Prepare Us for a Pandemic*, 11 J. HEALTH & BIOMEDICAL L. 2, 157, 167 (2006) ("Indeed, the women's health movement, which grew out of the women's movement, focused its questioning in particular on medical authority. . . . [The women's health and civil rights] 'movements subscribed to a fierce anti- paternalism, a dogged rejection of the principles of beneficence, a persistent determination to let constituents speak for themselves and define their own interests.'").

[19] *See infra* Chapter 4.

[20] Rand E. Rosenblatt, *The Four Ages of Health Law*, 14 HEALTH MATRIX 155, 175–76 (2004).

[21] *Id.*

[22] ROSENBLATT, LAW, & ROSENBAUM, *supra* note 7, at 16–21.

against cost containment efforts).[23] Physicians also increasingly gave up private practice to become employed by hospitals or health plans.[24]

The doctor–patient relationship has also changed. Not only did the social contract model of the 1960s and a focus on patient autonomy empower patients, but demographic shifts in the United States have significantly changed the relationship between doctor and patient. No longer do patients live in the same town and see the same doctor throughout their lifetimes. Rather population mobility and increasing specialization mean that the doctor–patient relationship is much more fragmented and time-limited.

The transformation of American health care financing in the mid-twentieth century[25] also significantly diminished de facto privacy protections physicians had previously enjoyed. As a greater percentage of the population gained insurance through government programs and non-indemnity health plans, the transmittal of data from physician offices to third party private and government payers soared. Additionally, the emergency of pharmacy benefit managers, large chain drug stores, and data mining firms means that large troves of information that previously rested mainly in physician offices are now housed by external entities. The practical significance is that more data now

---

[23] *Id*. ("Doctors are increasingly practicing in settings where they have less autonomy, and face greater pressures from financial incentives, practice guidelines, and utilization management.")

[24] Today, corporate entities may even find legal loopholes around corporate practice of law statutes in order to be able to employ physicians. In Texas, for instance, hospitals can fund a "501(a)" physician group which legally function as a large physician group with a physician board but which practically act more like employed doctors. *See* DCMS Glossary of Healthcare Terms & Acronyms, Dallas County Medical Society, available at http://www.dallas-cms.org/glossary.cfm.

[25] The success of Blue Shield and Blue Cross plans spurred the entrance of other health insurers and the percentage of the population covered by private health insurance grew from 9.1% in 1940 to 50.3% just ten years later. ROSENBLATT, LAW, & ROSENBAUM, *supra* note 7, at 12 tbl.1. By 1970, the share was up to 77.4%. *Id.* Additionally, Congress enacted Medicare and Medicaid in 1965 resulting in significantly increased coverage in public programs. To assuage physician concerns with Medicare, reimbursements were tied to physicians' usual and customary charges and physicians could bill patients directly and thus price discriminate by charging more than the Medicare rate and requiring patients to seek reimbursement. (These concessions persisted until the early 1980s when cost pressures resulted in the enactment of a prospective payment system.)

rests in non-physician hands, and is increasingly being commercialized or used for secondary purposes other than that originally intended.

Whatever the history, physician privacy is today a topic with which we must contend. As the next Chapter discusses, physicians constitute the first line of contact for those seeking health care and they wield significant control over care decisions including the intensity of diagnostic testing and treatment a patient will undergo. Physicians' decisions have a direct impact on health care costs and quality. Enormous stores of data by payers and other entities in the health care system provide a potential gold mine of information about how to improve care and reduce costs. Yet they also present more risks than ever before to physician privacy.

Chapter 2: Physician Privacy and U.S. Health Care

Although the three paradigms of health law have vied for dominance at different times, none has succeeded in addressing the three primary problems plaguing the U.S. health care system: how to ensure access, improve quality, and control costs.[26] Additionally, although comprehensive health reform was signed into law in 2010,[27] the impact of that reform remains to be seen given uncertainty surrounding the Supreme Court's consideration of the constitutionality of the included individual mandate and the strong possibility that a shift in political control of Congress and the White House in 2012 could result in a significant scaling back of the program. What's more, the reform does not purport to solve all of the nation's health care "ills," but instead seeks to expand coverage and initiate efforts to control costs.

Thus, whatever happens to the health reform law, the United States continues to face the same primary health care challenges it has for decades: rising and widely varying costs, inconsistent quality, unacceptable levels of medical errors, and a lack of access to both coverage and care for too many Americans. Additionally, there is an unfortunate lack of research into what works and what does not. While interest and research in evidence-based medicine has grown, there remains resistance to such efforts as head-to-head comparative effective research particularly when paired with cost-effectiveness

---

[26] Professor Elhauge suggests that perhaps the very existence of competing paradigms explains some of the problems in the health care system. *See* Einer Elhauge, *Allocating Health Care Morally*, 82 CAL. L. REV. 1449 (1994) ("Health law policy suffers from an identifiable pathology . . . . [I]t employs four different paradigms for how decisions to allocate resources should be made: the market paradigm, the professional paradigm, the moral paradigm, and the political paradigm. . . . [R]ather than coordinate these decision making paradigms, health law policy employs them inconsistently, such that the combination operates at cross-purposes.").

[27] Patient Protection and Affordable Care Act, Pub. L. No. 111-148 (2010).

analysis.[28] However, with annual health spending expected to reach $4.6 trillion in 2020 (or 20% of GDP), the urgency has most agreeing that something must be done to reform U.S. health care.

Apart from the health reform law, other significant transformations appear to be underway in the healthcare sphere. States and the federal government are increasingly relying on managed care organizations to provide coverage in both Medicare and Medicaid; many employers continue to express a desire to get out of the business of providing coverage. The U.S. is also witnessing a marked shift away from the historically prevalent small business model of health care in which medical care has been mostly delivered through for-profit solo private practices and small local hospitals.[29] Contributing to this shift is continuing consolidation in the health plan and hospital sector and the increasing employment of physicians by hospitals.

THE PROMISE OF INFORMATION & INFORMATION TECHNOLOGY

Information and information technology (IT) have emerged as important tools in improving the health care system. Information can support research (including disease research and health services and other quality research); it can be used to identify fraud

---

[28] Additional research will not be a panacea. For example, research findings are often not definitive. Moreover, later research may overturn previously held assumptions. *See* Colin Hill, Can Big Data Fix Healthcare?, FORBES, Nov. 17, 2011, *available at* http://www.forbes.com/sites/colinhill/2011/11/17/can-big-data-fix-healthcare/ ("A recent study found that 13 percent of articles concerning a clinical practice published in the New England Journal of Medicine in 2009 were reversals of previous findings. . . . A 2001 review of [clinical practice] guidelines estimated that half had become outdated in less than six years."). Frequent reversals may make patients and some doctors question the reliability of current research. However, a rapid learning health care system is almost certainly better than what we have today.

[29] ROSENBLATT, LAW, & ROSENBAUM, *supra* note 7, at 8 ("[B]etween 1880 and 1980, the medical profession was remarkably successful in persuading Americans that the proper form for health care was the small and medium-sized business, i.e. physician-controlled practices and hospitals.").

and waste; it can also be used as part of a regulatory disclosure regime to promote competition, provide consumers with decision tools, and promote accountability.

The use of electronic health records and other data analytic tools to improve health and health services research may be a crucial aspect of improving U.S. health care. The ability of health services researchers and others to access, manipulate, and analyze data may prove vital to conducting adverse event surveillance, identifying best practices, and discovering the reasons for quality and cost variations, among other possibilities. Some analysts are pointing to "Big Data"[30] as a novel way to improve health care.[31] There is also growing interest in the possibility of interactive health IT tools such as clinical decision support tools for physicians.[32] Finally, particularly in public programs, data is seen as necessary to ferreting out waste, fraud and abuse.

Many also see information *disclosure* as an alternative to either command and control regulation or unfettered market competition and suggest that it could be an important aspect of quality improvement, cost control, and supporting patient autonomy.[33] For instance, greater transparency may be useful in exposing and mitigating

---

[30] *See* Christopher Frank, *Improving Decision Making in the World of Big Data*, FORBES, Mar. 25, 2012, *available at* http://www.forbes.com/sites/christopherfrank/2012/03/25/improving-decision-making-in-the-world-of-big-data/ ("['Big Data'] is the hot term referring to the increasingly large datasets of information being amassed as a result of our social, mobile, and digital world. In the past 12-months, the use of the term in the U.S. has increased 1,211% on the internet.").

[31] *See, e.g.*, Hill, *supra* note 28 ("A recent McKinsey report called Big Data, 'the next frontier for innovation, competition and productivity.' The Aspen Institute reported on the 'promise and perils' of it. The Economist issued a special report about it. O'Reilly Media hosted two conferences on it this year alone."); Tom Groenfeldt, *Big Data Saves Michigan $1 Million Each Business Day*, FORBES, Jan. 1, 2012, *available at* http://www.forbes.com/sites/tomgroenfeldt/2012/01/11/big-data-saves-michigan-1-million-each-business-day/print/ ("Big Data is saving the state of Michigan $1 million each business day, while consolidating 40 data centers into three saved $19 million the first year.").

[32] *See, e.g.*, Clinical Decision Support Initiative, Agency for Healthcare Research and Quality, U.S. Department of Health and Human Services, *available at* http://healthit.ahrq.gov/portal/server.pt?open=512&objID=654&PageID=13665&mode=2&cached=true&wtag=wtag666.

[33] *See, e.g.*, Sage, *supra* note 13. Professor Sage identifies four rationales for information disclosure in health care: the competition rationale, agency rationale, performance rationale, and democratic rationale. Information can support competition by providing consumers with cost and quality information to alleviate

the effects of financial conflicts of interests based on ownership or investment interests or relationships with industry. In this sense, disclosure can serve as a substitute for more stringent regulations preventing or capping physician-industry ties or physician ownership and allow providers to self-police to ensure that financial incentives don't "undermin[e] the independence and integrity of the [medical] profession."[34]

Information disclosure can also serve important patient autonomy interests such as the ability to make informed decisions. For patients, access to their own health information is key to their ability to protect their own health, change physicians when needed, and ensure that care among various treating physicians can be properly coordinated.[35] Patients can also benefit from better decision making tools and greater transparency in selecting physicians and ensuring the quality of the physicians they visit. This is especially important because the increasing mobility of the population, changing lifestyles, and greater specialization among physicians has made it much less likely that patients will have a "medical home" or long-term relationships with their physicians.[36] This absence of established trust relationships makes it all the more important for patients to have ready access to information about the physicians from whom they seek care.

---

asymmetric information problems. It can "strengthen agency relationships and enforce fiduciary obligations" for example by providing information about physician qualifications and conflicts. It can also improve health system performance, for example by measuring and influencing health care quality. Finally, disclosure can support democratic objectives such as monitoring how government programs are functioning. *Id*. Note that this paragraph and the two following paragraphs are loosely adapted from Paige M. Jennings, *Physician Privacy and Information Policy*, Unpublished Paper for Advanced Policy Economics, Lyndon B. Johnson School of Public Affairs (2011).

[34] Robert Steinbrook, *Perspective: Online Disclosure of Physician–Industry Relationships*, NEW ENGLAND JOURNAL OF MEDICINE 360:325-327, Jan. 22, 2009.

[35] *See, e.g.*, David C. Warner & Budd N. Shenkin, *Giving the Patient His Medical Record: A Proposal to Improve the System*, 289 NEJM 688, 688–89 (1973) (proposing that patients be routinely given copies of their medical records and listing information, continuity, choice, and physician-patient relations as important justifications from the patient perspective).

[36] *See* Sage, *supra* note 17, at 162 (noting that since the late nineteenth century, "[u]rbanization and population mobility, along with medical specialization, reduced the continuity of therapeutic relationships").

Hospitals and physicians may also find greater transparency helpful. For example, to the extent that hospitals have greater information about physician quality, they may be able to make better credentialing and hiring decisions. Primary care physicians or others who routinely need to make referrals to specialists can better determine who best to refer their patients to. Physicians can also obtain better information about best practices and about their own performance both objectively and in comparison to other practitioners in the same area or specialty.[37]

The interest in health information technology is partially reflected in the number of physician offices adopting electronic health records, which has doubled in the last two years.[38] The federal government is actively subsidizing health information technology tools for providers. This dissemination of health IT tools is sure to change the health care landscape dramatically. For example, the Department of Health and Human Services is asking providers and others who hold individually identifiable health data to make such data electronically available to their patients in a timely manner (for example through the "Blue Button" or "Direct Project").[39] While patients have had a federal legal right to their health records for about a decade, these efforts may facilitate more electronic communication between patients and their doctors.

---

[37] *See* Warner & Shenkin, *supra* note 35 (noting that "physicians have only limited means of evaluating one another's performance").

[38] Alex Howard, *Data, Health IT and Patient Empowerment Can Revolutionize Healthcare*, FORBES, Mar. 14, 2012, *available at* http://www.forbes.com/sites/oreillymedia/2012/03/14/data-health-it-and-patient-empowerment-can-revolutionize-healthcare/.

[39] *See Putting the 'I' in Health IT: Pledge*, HealthIT.gov, *available at* http://www.healthit.gov/pledge/?submit.x=253&submit.y=34&submit=Send (outlining a pledge for data holders to "make it easier for individuals and their caregivers to have secure, timely, and electronic access to their health information").

COUNTERVAILING LOGISTICAL AND PRIVACY CONCERNS

To the extent information disclosure is used as a regulatory tool to improve performance, this may further challenge physician autonomy and authority.[40] Physicians certainly have legitimate concerns surrounding information disclosure efforts. There are definite limitations to data and the types of research and tools that are feasible. For example, record systems may be incomplete or inaccurate. Apparent problems with quality may represent systemic rather than provider-specific problems or may be a reflection of a sicker than average patient population. Patients and other stakeholders may misunderstand the implications of certain data.

However, improvements in the health care system seem certain to rest at least in part on greater use of information and information technology in research, practice, and transparency initiatives. None of these initiatives can be accomplished without the cooperation and participation of physicians. It will be vital that physicians are on board and willing to share information about themselves and their practices.

In this vein physician privacy becomes all the more important to sort through. To the extent that physicians have concerns about their privacy already, these will likely become more pronounced as greater amounts of information are collected, stored, analyzed, manipulated, disseminated, and sold. This Report is thus intended to help illuminate physician privacy and to devise a framework that can help policymakers perform the necessary balancing between the promise of health system improvements and physician privacy interests.

---

[40] *See* Sage, *supra* note 13, at 1771–1802 (noting that information may be used to monitor provider practices and expose practice discrepancies; set national goals; risk-adjust payments; create feedback loops; and influence patients).

Chapter 3: What is Privacy and How is it Protected?

To understand and explain physician privacy, it is necessary to examine U.S. privacy policy as it applies more broadly. This Chapter discusses various theoretical conceptions of privacy and suggests that the term is far from clear cut and not subject to a unitary definition. U.S. privacy law is also described in order to describe the context in which physician privacy is situated.

WHAT IS PRIVACY?

Privacy is an evolving concept that remains ill-defined.[41] Historically, privacy protections have taken many forms. Some of the earliest societal rules or norms regarding privacy relate, perhaps coincidentally, to medical care and the obligation of doctors to maintain their patients' privacy.[42] Between the sixteenth century and nineteenth centuries, the English common law began to recognize an action for "breach of confidence" for unwarranted disclosures of confidential information.[43]

Some scholars argue that current U.S. privacy law grew out of, and then away from, the law of confidential relationships or communications, which is largely based on fiduciary duties between individuals rather than on an individual's own right to safeguard his personal information outside the context of a trust-based relationship with another.[44]

---

[41] *See* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 477–78 (2006) (describing "privacy" as "a concept in disarray" and as "too vague a concept to guide adjudication and lawmaking").
[42] Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 133 (2007) (citing the Hippocratic Oath as an example of the concept of "confidentiality" as far back as antiquity).
[43] *Id.* at 133–34.
[44] *See Id.* (quoting a sixteenth century rhyme reciting "[t]hese three give place in court of conscience, Fraud, accident, and breach of confidence"); *id.* at 136 (discussing a 1758 English case allowing the equitable restraint of publication of a manuscript); *id.* at 123 ("Well before 1890, a considerable body of

For example, the breach of confidence tort may protect privacy rights in trust-based relationships. However, that tort has not been extensively relied upon in the United States where, instead, tort law has developed to protect against specific types of disclosures or intrusions, regardless of the identity of the actor.

As discussed in more detail below, "privacy" in the United States has been protected in many different ways, including through federal and state constitutional provisions, federal and state statutes, tort law, and evidentiary privileges.[45] Historically, privacy was primarily protected only from certain government interference, such as the protection from unwarranted searches and seizures.[46] However, in the late 19th and early 20th centuries, notions of privacy began to expand.[47] Some of this transformation appears to have been driven in part by technological and societal changes such as the invention of the still camera.[48] Around this time, Louis Brandeis and Samuel Warren, then practicing attorneys, published a seminal article, The Right to Privacy, suggesting individuals might have some inherent interest in privacy that they could enforce against the world, rather than solely against government actors or those with whom they had a

---

Anglo-American law protected confidentiality, which safeguards the information people share with others. Warren, Brandeis, and later Prosser turned away from the law of confidentiality to create a new conception of privacy based on the individual's "inviolate personality.")

[45] *See* Solove, *supra* note 41, at 483 (". . . Prosser focused only on tort law. American privacy law is significantly more vast and complex, extending beyond torts to the constitutional "right to privacy," Fourth Amendment law, evidentiary privileges, dozens of federal privacy statutes, and hundreds of state privacy statutes.").

[46] U.S. CONST. amend. IV.

[47] Samuel Warren and Louis Brandeis described privacy rights as "the right to be left alone." Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890) (quoting Judge Cooley's opinion in Winsmore v. Greenbank, Willes, 577 (1745)). They went on to suggest that individuals could prevent publication of matters concerning "the private life, habits, acts, and relations of an individual, [that] have no legitimate connection with his fitness for a public office . . . or for any public or quasi public position . . . and have no legitimate relation to or bearing upon any act done by him in a public or quasi public capacity." *Id.* at 216.

[48] *Id*. (discussing photograph numerous times throughout the article and noting that "[i]nstantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life . . . ."); *see also* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE (2004) (discussing Warren and Brandeis's concerns about candid photographs); .

trust-based relationship. In time, tort law developed allow individuals to protect these privacy interests against non-governmental actors and to seek redress, for example, if others disclosed information that would be "highly offensive" or that put them in a false light.[49]

Numerous scholars have since attempted to explain or categorize privacy law and privacy rights.[50] Some have described privacy in terms of states of being or relationships with other people;[51] some have characterized it as a set of overlapping notions of physical space, choice, and personal information;[52] others have sought to describe the legal frameworks that protect privacy including tort law[53] or tort law combined with federal and state constitutional protections.[54]

Professor Daniel Solove has proposed a "taxonomy" of privacy in which the larger, amorphous concept is conceptualized in terms of four types of activities that raise privacy concerns: information collection, information processing, information dissemination, and invasion.[55] Although his taxonomy is not explicitly organized around the harms that privacy law protects against, he identifies many of these harms including: "'mental pain and distress'" or "'injury to feelings;'"[56] dignitary harms (such as damage

---

[49] *See* William Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960) (describing the torts of intrusion on seclusion, public disclosure of private facts, false light, and appropriation of name or likeness).
[50] *See* Solove, *supra* note 41, at 482 & n.19 (cataloging some of the ways in which scholars have defined privacy).
[51] *See id*. (describing Alan Westin's conception of solitude, intimacy, anonymity, and reserve as the four "basic states of individual privacy").
[52] *See id*. (discussing Jerry Kang's work in this area).
[53] *See id*. (noting that Professor William Prosser examined four harms that could be remedied through private suits but that Prosser's framework only addressed interests an individual could remedy through private causes of action in the courts).
[54] *See id*. (discussing Ken Gormley's conception of privacy law).
[55] Solove, *supra* note 41, at 489.
[56] *Id.* at 487 (quoting Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890)).

to reputation, "lack of respect," incivility, etc.);[57] the *risk* of harm caused by lack of structural privacy safeguards;[58] financial harm due to fraud or identity theft;[59] and potentially societal harm due to the chilling of unprotected activity that individuals do not want exposed.[60]

THE CURRENT PRIVACY LEGAL FRAMEWORK

It is beyond the scope of this Report to outline the whole of U.S. privacy law or to add to the scholarship conceptualizing privacy broadly. However, a non-exhaustive description of current U.S. privacy law can illuminate the broader context in which physician privacy should be considered.

U.S. privacy law tends to fall into four broad categories: 1) protection from government intrusion which tend to protect values of democracy, dignity, fairness, autonomy; 2) sectoral privacy rules governing particular categories or sources of information; 3) tort law to remedy harmful disclosures or invasions by private actors; and 4) confidentiality within trust or contractual relationships.

As these categories suggest, there is no overarching right to privacy in U.S. law. Rather, a patchwork of Constitutional, statutory, regulatory, and common law protections operate together to provide individuals with some level of privacy protection. However, this patchwork results in a system that is both over- and under-protective of privacy in differing contexts. Additionally, because each type of legal protection was created at a different time and in response to different concerns, each reflects a separate set of underlying value judgments and guards against a different type of harm.

---

[57] *Id.* at 487.
[58] *Id.*
[59] *Id.*
[60] *Id.*

The U.S. Constitution has been held to protect privacy in a number of contexts. Perhaps most overtly, the 4th Amendment protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[61] This privacy right is centered around protected spaces and persons (one's home or one's person) and only protects individuals from government interference. Similarly, the Fifth Amendment protects individuals from compelled self-incrimination,[62] which arguably relates to the privacy of one's innermost thoughts and feelings from government interference. The First Amendment has also been held to protect privacy by ensuring that individuals be protected from compelled disclosure of their associations.[63] The confluence of the various privacy interests recognized in the Bill of Rights led the Supreme Court to also recognize a "penumbra" of privacy rights[64] that has been applied to protect rights to contraception use,[65] the right to abortion,[66] and private, consensual sexual activity.[67]

The Supreme Court's due process jurisprudence, while not nominally about privacy, also has implications for it, particularly with respect to information collection and disclosure.[68] In *Wisconsin v. Constantineau*,[69] for example, the Supreme Court invalidated a statute that allowed public officials to post notices prohibiting the sale of alcohol to specified individuals deemed excessive drinkers. The Court found that such

---

[61] U.S. CONST. amend. IV.
[62] U.S. CONST. amend. V ("No person . . . shall be compelled in any criminal case to be a witness against himself . . . .").
[63] U.S. CONST. amend. I; *see also* NAACP v. Alabama, 357 U.S. 449 (1958).
[64] Griswold v. Connecticut, 381 U.S. 479 (1965).
[65] *Id.*
[66] Roe v. Wade, 410 U.S. 113 (1973).
[67] Lawrence v. Texas, 539 U.S. 558 (2003).
[68] The remainder of this paragraph and the following two paragraphs are adapted from Jennings, *supra* note 33.
[69] 400 U.S. 433 (1971).

public posting without prior notice and hearing would expose targeted individuals to "public embarrassment and ridicule" and violate the Due Process Clause.[70] "Where a person's good name, reputation, honor, or integrity is at stake because of what the government is doing to him, notice and an opportunity to be heard are essential."[71] Nevertheless, only five years later the Court appeared to make a sharp departure from the requirement of due process where reputational harms were at issue. In *Paul v. Davis*, the Court held that individuals do not have Constitutionally protected liberty or property rights in their reputations per se.[72] The Court distinguished *Constantineau* by noting that, in that case, the reputational stigma was accompanied by loss of another right and that government actions affecting an individual's reputation require more than mere stigma to trigger due process rights.

Whether the Constitution provides a right to *informational* privacy remains somewhat of an open question. The Supreme Court, in two cases decided in 1977, *Whalen v. Roe*[73] and *Nixon v. Administrator of General Services*,[74] suggested the possibility that government collection or dissemination of information might implicate privacy interests or rights. *Whalen*, the more notable opinion, coincidentally deals with the collection of information from physicians. In that case, the Court considered the constitutionality of a state law requiring doctors to report the names of patients to whom they prescribed drugs with a potential for abuse, which the state then stored along with the names of prescribing physicians. The Supreme Court held the law to be constitutional because it did not "pose a sufficiently grievous threat to establish a

[70] *Id.* at 436–37.
[71] *Id.* at 437.
[72] 424 U.S. 693 (1976).
[73] 429 U.S. 589 (1977).
[74] 433 U.S. 425 (1977).

constitutional violation"[75] and because it reflected the state's interest in preventing abuse of the targeted prescription medications. The Court also noted that provisions had been implemented to maintain the confidentiality of the information submitted. While not recognizing a "right" to informational privacy, the Court acknowledged that individuals have an "interest in avoiding disclosure of personal matters"[76] and an interest in making some types of "important decisions" free from government interference.[77] The Court went on to recognize the "threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files . . . much of which is personal in character and potentially embarrassing or harmful if disclosed."[78] However, because the law at issue did not pose the concerns outlined above, the Court did not address the constitutionality of "unwarranted *disclosure* of accumulated private data—whether intentional or unintentional" or of systems lacking "comparable security provisions."[79]

Few subsequent Supreme Court decisions have dealt with rights to "informational" privacy. However, in 2011, the Supreme Court in *NASA v. Nelson*, "assume[d], without deciding, that the Constitution protects a privacy right of the sort mentioned in *Whalen*"[80] In *NASA*, the Court upheld the collection of information about government employees because the questions asked of them were "reasonable," subject to protection from public disclosure under the Privacy Act, and because they were asked

---

[75] *Id.* at 600.
[76] *Id.* at 599.
[77] 429 U.S. at 599–600 & 600 n.26 (citing Roe v. Wade, 410 U.S. 113, (1973); Doe v. Bolton, 410 U.S. 179, (1973); Loving v. Virginia, 388 U.S. 1, (1967); Griswold v. Connecticut, 381 U.S. 479 (1965); Pierce v. Society of Sisters, 268 U.S. 510, (1925); Meyer v. Nebraska, 262 U.S. 390, (1923); Allgeyer v. Louisiana, 165 U.S. 578, (1897)).
[78] *Id.* at 605.
[79] *Id*. at 605–06 (emphasis added).
[80] NASA v. Nelson, 131 S.Ct. 746, 751 (2011).

by the government in its role as an employer rather than its role as a sovereign.[81] Further, the Court noted that any constitutional privacy interest need not be accompanied by an "ironclad disclosure bar," but rather that relevant cases have focused on "*unwarranted* disclosure" or "*undue* dissemination."[82] Justice Scalia, concurring in the decision but not the Court's reasoning, sharply criticized the Court's willingness to assume the existence of a privacy right of this sort, stating bluntly that "[a] federal constitutional right to "informational privacy" does not exist"[83] and that neither *Whalen* nor *Nixon* "supplied any coherent reason why a constitutional right to informational privacy might exist."[84]

Constitutional protections for privacy appear to be grounded in the values such as democracy, dignity, justice, and autonomy and which affect not only individual privacy interests but societal goals as well. For example, the Fourth Amendment protection from unreasonable searches and seizures and the Fifth Amendment protection from compelled self-incrimination would seem to be predominantly grounded in Democratic concerns and the desire to protect individuals from government subjugation. These are further supported by goals of justice as well as basic dignity and autonomy. Likewise, First Amendment associational privacy is vital to a democratic society and the ability to freely meet and discuss ideas. Penumbral privacy rights which have been used to protect decisions related to contraceptive use, abortion, and private sexual activity seem more grounded in dignity, autonomy, and certain fundamental decisions related to the family and intimate relationships. To the extent that informational privacy exists, it seems to be

---

81 *Id*. at 756–57.
82 *Id.* at 762 (emphasis added).
83 *Id.* at 764 (Scalia, J., concurring).
84 *Id.* at 766.

related to concerns about overreaching by government as well as dignity and emotional components (for instance, embarrassment) and the right to self-determination.

Federal and state statutes also protect privacy though in a more haphazard, and often information- or sector-specific, way. These are directed at a combination of government and private actors. Because of the siloed way in which they have been enacted, they are also driven by very different concerns.

Many of the federal regulatory and statutory protections came about in response to the growth of the federal administrative state during the twentieth century and the emergence of computerized data systems. The federal government had begun to collect more and more information about those touching or participating in federal programs. In 1973, then-Department of Health Education and Welfare released a set of Fair Information Practices, which, among other things, called for a prohibition on secret personal-data record-keeping systems and a requirement that individuals be able to prevent nonconsensual secondary uses of data about themselves and to amend or correct records.[85]

In 1974, Congress passed what has been called the "most ambitious" and "most comprehensive" federal law regulating the collection and dissemination of individually identifiable information by the U.S. government, the Privacy Act.[86] The release of the Fair Information Practices and the Watergate Scandal, in which the Nixon Administration took advantage of federally-held personal information to target political opponents, have been cited as precipitating events leading to passage.[87] The Privacy Act provides that

---

[85] U.S. DEP'T OF HEALTH, EDUCATION, AND WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY'S ADVISORY COMM. ON AUTOMATED PERSONAL DATA SYSTEMS (1973). Note that this paragraph and the two that follow are adapted from Jennings, *supra* note 33.
[86] *See* Lior Jacob Strahilevitz, *Reunifying Privacy Law*, 98 CALIF. L. REV. 2007, 2024 (2010).
[87] *Id.*

"[n]o agency shall disclose any record which is contained in a system of records . . . except with the prior written consent of[] the individual to whom the record pertains."[88] This may apply to information about an individual that is held by an agency, including financial transactions. Records may be released if they are required to be reported by the Freedom of Information Act (FOIA).

FOIA, in turn, governs the information that federal agencies *must* disclose to the public upon request[89] but provides privacy protections by exempting from disclosure personnel, medical, and "similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy."[90] Information that "applies to a particular individual"[91] may result in a "clearly unwarranted invasion of personal privacy" if a "substantial" privacy interest is at stake[92] and the privacy interest is not outweighed by the public interest in disclosure.[93] Courts have held that individuals have substantial privacy interests in financial information such as hourly pay.[94] Other factors suggesting a privacy interest have included the "prospect of misleading publicity, possibility of unwarranted professional and public criticism, and damage to professional reputation."[95]

---

[88] 5 U.S.C. § 552a(b).
[89] *Id.* § 552(a)(3).
[90] *Id.* § 552(b)(6).
[91] U. S. Dep't of State v. Wash. Post Co., 456 U.S. 595, 599, 602 (1982) ("Similar files" are not limited to "a narrow class of files containing only a discrete kind of personal information" but instead "information which applies to a particular individual . . . ."). "Congress' primary purpose in enacting Exemption 6 was to protect individuals from the injury and embarrassment that can result from the unnecessary disclosure of personal information." *Id.*
[92] *Consumers' Checkbook*, 554 F.3d at 1050.
[93] *Id.* at 1056.
[94] *Id.* at 1050.
[95] Pub. Citizen Health Research Grp. v. Dep't of Health, Educ. and Welfare, 477 F. Supp. 595, 598¬–99, 603 (D.D.C. 1979), rev'd on other grounds, 668 F.2d 537 (D.C. Cir 1981).

Because the United States, in contrast to the European Union, has taken a sectoral approach to privacy, many other federal statutes include privacy protections as well.[96] For example, the Gramm-Leach-Bliley Act requires the establishment of standards for financial institutions to safeguard the "security and confidentiality" of customer information, to protect against certain reuses of information by third parties, and to allow customers to opt out of sharing their information with third parties.[97] Driven by very different concerns, the Children's Online Privacy Protection Act requires that websites guard the "confidentiality, security, and integrity of personal information collected from children" and provide parents with access to this information.[98] Finally, of most relevance to this Report, the Privacy Rule issued pursuant to the 1996 Health Insurance Portability and Accountability Act (HIPAA), provides privacy protections for individually identifiable health information collected by covered entities.[99] The Rule specifies permitted uses of such information, which primarily can only be used for health care treatment, payment, and operations.[100] The Rule also provides individuals with rights to access their own health information.[101] However, the rule does not provide privacy protections for physicians except to the extent that patient information shielded from disclosure has the practical effect from shield some physician information as well.

Tort law regulates interactions between individuals as opposed to controlling state actors and is less sector-specific than many of the statutory privacy protections. The Comments to the Second Restatement of Torts note that before Warren and Brandeis's

---

[96] SOLOVE, *supra* note 48, at 67 (noting that Congress has passed over twenty "narrowly tailored" laws related to privacy since the 1970s).
[97] Solove, *supra* note 41, at 518, 521, 525 (discussing various aspects of the Gramm-Leach-Bliley Act).
[98] *Id*. at 518, 525.
[99] 45 C.F.R. § 164.508(a) (2001).
[100] *Id*.
[101] 45 C.F.R. § 164.524 (2001).

famous 1890 "Right to Privacy" article, "no English or American court had ever expressly recognized the existence of the right [to privacy]" though some decisions "in retrospect appear to have protected it in one manner or another."[102] Many states allow tort actions to be brought for invasions of privacy on the basis of one of four distinct torts: "unreasonable intrusion upon the seclusion of another";[103] "unreasonable publicity given to [another's] private life";[104] "publicity that unreasonably places [another] in a false light before the public";[105] or "appropriation of the . . . name or likeness" of another.[106] The first three torts all require an "unreasonable" and "highly offensive" invasion.[107] The last tort, appropriation, "appears rather to confer something analogous to a property right upon the individual."[108]

Tort law may also be used to protect privacy through actions for intentional infliction of emotional distress whereby a person "by extreme and outrageous conduct intentionally or recklessly causes severe emotional distress to another."[109] Similarly, defamation suits may be brought for "false and defamatory statement concerning another" to a third party.[110] However, in order to be actionable, these statements must "tend[] so to harm the reputation of another as to lower him in the estimation of the community or to deter third persons from associating or dealing with him."[111]

The privacy-related torts seem to be driven by a combination of concern for autonomy and dignity or the "right to be let alone" as Brandeis and Warren put it. Even

---

[102] Restatement (Second) of Torts § 652A cmt. a (1977).
[103] *Id*. § 652B.
[104] *Id*. § 652D.
[105] *Id*. § 652E.
[106] *Id*. § 652C.
[107] *Id*. § 652B, 652D, 652E.
[108] *Id*. § 652A cmt. b.
[109] *Id.* § 46 (1977).
[110] *Id.* § 558.
[111] *Id.* § 559.

the tort of appropriation of likeness, which has something of conferring property protection over one's likeness, has also been said to protect dignitary concerns.[112]

Nevertheless, the four invasion of privacy torts are only infrequently relied upon and it can be difficult for plaintiffs to succeed in obtaining recovery through their use.[113] Further, some privacy scholars note that the torts have not fared well as tools to protect informational privacy.[114]

A final important aspect of privacy protection in the United States is confidentiality protection based on certain trust or fiduciary relationships. This type of legal protection is primarily concerned with fostering trust and particular relationships. However, the tort of breach of confidence has only been used with any degree of frequency over the last few decades.[115] The tort has primarily been applied to physicians, though some courts have applied it to attorneys, hospitals, banks, and other entities or professionals with whom an individual might have a trust-based or fiduciary type relationship.[116]

The above discussion illustrates the fragmented nature of U.S. privacy law and the many different values underpinning it. As the next Chapter will show, physician privacy protection is similarly piecemeal and similarly may be both over- and under-protective of physician privacy.

---

[112] *See* Solove, *supra* note 41, at 380–81 (discussing the two competing rationales offered for the injury protected by the appropriation tort: "an affront to dignity" and "protection of property rights").
[113] Richards & Solove, *supra* note 42, at 155.
[114] *Id*. ("[T]he privacy torts have struggled when addressing emerging privacy problems in the Information Age, such as the collection, use, and disclosure of personal data by businesses.").
[115] *Id*. at 157.
[116] *Id*.

Chapter 4: The Current State of Physician Privacy

As Chapter 1 demonstrated, physicians historically enjoyed both de facto privacy protection and a certain level of professional immunity for efforts to require greater disclosures of information. However, the state of physician privacy is very different today, primarily because significant changes in the U.S. health system and the role of physician autonomy have resulted in more and more information being shifted away from physician practices and into the hands of others. This Chapter provides a more detailed, though not exhaustive, look at some of the ways in which physicians have sought to protect their privacy interests through legal rules and societal norms. It also discusses countervailing initiatives that run counter to physician privacy by requiring greater information disclosure or transparency.

HISTORICAL AND CURRENT LAW PRIVACY PROTECTIONS

Medical Records

Until recently, the medical records maintained by physicians were shielded from view even from the patients to whom they pertained. These were considered to belong to the treating physician and as of the early 1970s, patients in the vast majority of states could obtain their medical records only through litigation.[117] It took another decade for the American Medical Association to officially endorse the idea that physicians should provide patients with access to their own medical records upon request.[118] States began

[117] Warner & Shenkin, *supra* note 35 ("By law, patients can obtain their medical records in 41 states only through litigation, in three states only through an attorney . . . , in one through showing good cause, and in one only after discharge from care.").
[118] *Id*. at 329.

to enact statutes in the late 1970s and early 1980s to provide individuals with the right to access their own medical records,[119] but it was not until the early 2000s, with promulgation of the Federal Health Privacy Rule under HIPAA, that patients had a uniform, federal right to access their medical records.[120]

Physicians' opposition to required disclosure of medical record information, even to the patients about whom they pertained, appears to have been driven by multiple concerns. Early in the twentieth century, professional authority bolstered this norm. Medicine had a paternalistic bent and doctors had complete discretion as to what information to share with their patients. For example, many physicians did not even inform patients with terminal illness of their prognosis.[121] As a result, the notion of sharing notes and records with patients likely seemed not only unnecessary but perhaps even counterproductive to many physicians. Professional autonomy and authority may also have led to concerns that more open records would expose doctors to review by their peers and potentially expose their care as substandard.[122] Further, allowing records to be shared with other physicians could facilitate patients switching doctors and thereby erode the physician's practice and income.[123] Finally, fear that records could be used to expose or support malpractice liability certainly led physicians to closely guard the records they developed in practice.[124]

---

[119] Joy L. Pritts, *Altered States: State Health Privacy Laws and the Impact of the Federal Health Privacy Rule*, 2 YALE J. HEALTH POLICY, LAW & ETHICS 325, 332 (2002).
[120] *Id*. at 341; 45 C.F.R. § 164.524 (2001).
[121] See, e.g., Warner & Shenkin, *supra* note 35 (citing a 1973 study from Great Britain suggesting that only 6 percent of patients with terminal illness were informed of the prognosis).
[122] Warner & Shenkin, *supra* note 35, at 690 (describing "an almost pathologic fear among practitioners that their practices will be found deficient").
[123] *Id*. (noting that patients' inability to obtain medical records inhibits them from judging their own physician or changing physicians).
[124] *Id*.

Tort Law

Tort law has been used by physicians to prevent or obtain compensation for damaging disclosures by colleagues. For example, individual physicians may bring claims such as defamation, tortious interference, and intentional infliction of emotional distress to seek redress from those they allege have inappropriately disclosed information about them.[125] However, tort law as a tool to enforce privacy has significant limitations. Most obviously, it can be expensive, time-consuming, and lacks any guarantee of a positive or intended result. Further, a physician's own reputation and relationships may be harmed by bringing tort claims against colleagues, patients, or others in their communities, particularly since the lawsuit itself may draw attention to the underlying conduct in controversy.[126] Finally, tort actions require physicians to prove issues such as causation, harm, and generally that the conduct or comments were unreasonable, for instance because they were false or deliberately intended to harm.[127] Despite the limitations of tort law to protect physician privacy, their importance for purposes of this Report is the harm they seek to address. Tort law is primarily used to guard physician privacy by deterring and seeking compensation for reputational, emotional, and economic harms.

Peer Review, Malpractice, and Patient Safety

Concern about reputational and economic harm to physicians has also driven privacy protections contained in state peer review statutes. Almost all states have statutes

---

[125] *See, e.g.*, Poliner v. Texas Health Systems, 2003 U.S. Dist. LEXIS 17162 (N.D. Tex. 2003); *see also* Jeffrey Segal, et al., *Legal Remedies for Online Defamation of Physicians*, 30 J. LEGAL MED. 349, 358–61 (2009) (describing efforts by physicians to use the tort of defamation to redress reputational harms caused by allegedly false statements).
[126] *See* Segal, *supra* note 125.
[127] *Id*.

ensuring that peer review committee proceedings about particular physicians remain confidential and privileged.[128] These committee proceedings, generally conducted by a body of practicing physicians, may be regular, periodic, or convened to discuss a particular doctor's performance. The results may have implications for a doctor's clinical privileges or membership in a professional society.[129] Confidentiality and privilege for peer review proceedings is normally justified for two primary reasons: first confidentiality is deemed essential to the willingness of physician review body members to freely evaluate their peers; second, confidentiality protects proceedings from disclosure in case of a later lawsuit by the doctor being reviewed.[130]

Confidentiality protections for peer review may not, however, have resulted in robust peer review proceedings.[131] Concerns about the ability of state bodies to police physicians and the fear that poor quality physicians could simply reestablish practice in a new state after disciplinary action lead to the creation of the National Practitioner Data Bank (NPDB) in 1986.[132] The enacting statute requires the reporting of provider-specific adverse licensure, privileging, or peer review actions as well as medical malpractice payments.[133] The statute provides privacy and confidentiality protections for physicians

---

[128] Alissa Marie Bassler, Comment, *Federal Law Should Keep Pace with States and Recognize a Medical Peer Review Privilege*, 39 IDAHO L. REV. 689, 690 (2003) (noting that forty eight states and the District of Columbia had enacted statutes to protect peer review proceeding confidentiality).

[129] *See* American Medical Association, Medical Peer Review, http://www.ama-assn.org/ama/pub/physician-resources/legal-topics/medical-peer-review.page.

[130] *See* Bassler, *supra* note 128, at 690 (describing the rationales for peer review confidentiality); see also, American Medical Association, supra note 120 (detailing the provisions of the Health Care Quality Improvement Act of 1986 (HCQIA), 42 USC §11101 et seq, which protects members of peer review bodies from liability based on their determinations).

[131] *See, e.g.*, Susan O. Scheutzow, *State Medical Peer Review: High Cost But No Benefit—Is it Time for a Change?*, 25 AM. J.L. & MED. 7, 55 (1999) (suggesting that "neither the state peer review immunity statutes nor the privilege statutes encourage peer review").

[132] *The Data Bank – About Us*, THE DATA BANK: NATIONAL PRACTITIONER/HEALTHCARE INTEGRITY & PROTECTION, http://www.npdb-hipdb.hrsa.gov/topNavigation/aboutUs.jsp. Portions of the remainder of this subsection are adapted from Jennings, *supra* note 33.

[133] *The Data Bank – About Us*, THE DATA BANK: NATIONAL PRACTITIONER/HEALTHCARE INTEGRITY & PROTECTION, http://www.npdb-hipdb.hrsa.gov/topNavigation/aboutUs.jsp; *see also* Ruth E. Flynn, *Demand*

whose information is reported to the bank. For example, access to the Data Bank is restricted to specified users and unavailable to the public and violations of associated confidentiality provisions are subject to civil monetary penalties of up to $11,000 per offense.[134] Efforts to make Data Bank information more public have consistently failed.[135] As of now, only an aggregated Public Use Data File is available to allow the public to obtain summary information about malpractice payments and adverse licensure or clinical privilege events not linked to particular providers.[136] By statute, HRSA must release the data only in a form not identifiable by physician nor capable of being aggregated with other information to disclose physician identities.[137] Recently, access to even the NPDB Public Use Data File was closed after the Kansas City Star newspaper was able to link information from the Data File to other information to identify a Kansas neurosurgeon who had been sued at least 17 times.[138] HRSA, which is responsible for hosting the database, has since reopened access to the data file subject to certain restrictions to ensure that information can never be combined to reveal provider identities.[139]

Similar privacy protections are included in the Patient Safety and Quality Improvement Act of 2005 (Patient Safety Act), which established a voluntary system for

---

for Public Access to the National Practitioner Data Bank: Consumers Sound Their Own Death Cry, 18 HAMLINE J. PUB. L. & POL'Y 251, 252 (1996);

[134] 42 U.S.C. § 11137(b); *The Data Bank – About Us*, THE DATA BANK: NATIONAL PRACTITIONER/HEALTHCARE INTEGRITY & PROTECTION, http://www.npdb-hipdb.hrsa.gov/topNavigation/aboutUs.jsp.

[135] Pape, *supra* note 4, at 978 (1997).

[136] Resources: Public Use Data File, THE DATA BANK: NATIONAL PRACTITIONER/HEALTHCARE INTEGRITY & PROTECTION, http://www.npdb-hipdb.hrsa.gov/resources/publicData.jsp.

[137] 42 U.S.C. § 11137(b).

[138] *See* Dave Helling, *Senator Joins Fight to Reopen Database Website Shut Down by Government*, KANSAS CITY STAR, Nov. 3, 2011, *available at* http://www.kansascity.com/2011/11/03/3247032/senator-joins-fight-to-reopen.html.

[139] Alina Selyukh, *Government Reopens Doctor Data Access, with Some Caveats*, REUTERS, Nov. 9, 2011, *available at* http://www.reuters.com/article/2011/11/09/us-usa-malpractice-database-idUSTRE7A87QJ20111109.

medical error reporting to Patient Safety Organizations (PSOs).[140] Information reported to PSOs is confidential and privileged from discovery in order to encourage error reporting.[141]

Concerns about privacy in the context of both the National Practitioner Data Bank and the Patient Safety Act appear to be driven largely by fears of reputational harm.[142] In addition to expressing concerns about invasions of privacy and reputational harm, physicians argue that disclosure of information housed in the NPDB will lead to an increase in malpractice litigation as more physicians refuse to settle frivolous claims or fight claims to avoid being reported to the databank.[143] The increased costs from this litigation, it is argued, will be passed on to patients and physicians will be distracted from their core medical duties.[144] Physicians have also opposed efforts to make the NPDB public based on the argument that publicity will inhibit them from sharing information with peer review bodies for fear that it will be made public through the NPDB.[145] Similarly, in the case of the Patient Safety Act, the voluntary nature of the reporting system led policy makers to view confidentiality as a necessary protection to encourage physicians and others to report medical errors.

---

[140] Patient Safety and Quality Improvement Act, Pub. L. No. 109-41, 119 Stat. 424 (2005).
[141] *Id.*; *see also* Patient Safety Organizations, AGENCY FOR HEALTHCARE RESEARCH AND QUALITY, U.S. DEP'T OF HEALTH & HUMAN SERVICES, http://www.pso.ahrq.gov (last visited May 16, 2011).
[142] See, e.g., Sage, *supra* note 17, at 159 (suggesting that physicians' longstanding hatred of malpractice litigation is driven mainly by concern about public reputation, rather than concerns about issues like the cost judgments (which are borne by insurers) or the time involved in defending against suits).
[143] Pape, *supra* note 4, at 989–90 (1997).
[144] *Id*.
[145] *Id*. at 990–91

Health Plan and Patient Evaluations

Reputational concerns also influence how physicians have responded to public rating and evaluation of physicians by health plans and patients. However, accuracy, the ability to correct and respond to information, and other practical considerations are also very much at the forefront of concerns about these programs. Physicians have relied on several legal tools to contest the structure of the physician evaluation programs that large health plans have begun to offer.[146] For example, between 2007 and 2011, physicians sought to challenge ranking programs through state law claims such as breach of contract and negligent misrepresentation and by supporting governmental investigations into unfair business practices.[147]

Physicians have also responded to the growing number of websites that allow patients to rate or comment on doctors. Patients may now rate their experiences with particular doctors through any of 50 or more online ranking websites started since 2004.[148] Some physicians have responded by asking patients to sign non-disclosure agreements preventing them from commenting online about the care they receive.[149] Such contractual agreements prevent online criticism by prospectively assigning to the

---

[146] *See* Stephanie Kanwit, Special Counsel, America's Health Insurance Plans, Presentation at FTC Innovations in Health Care Delivery Public Workshop: Transparency in Principle and in Practice: Health Insurance Plan Perspectives (Apr. 24, 2008), *available at* http://www.ftc.gov/bc/healthcare/hcd/docs/Kanwit.pdf.

[147] Cal. Med. Ass'n v. Blue Shield of Cal. Life & Health Ins., No. RG10535619 at 2 (Cal. Super. Ct. 2011) (granting defendant Blue Shield's motion to strike the complaint alleging six causes of action against Blue Shield's "Blue Ribbon" provider rating program). Similarly, in a move supported by state and national medical societies, New York Attorney General Andrew Cuomo launched an investigation of several health insurers' physician ranking programs in 2007. The Attorney General expressed support for transparency initiatives but noted that ratings may cause consumer confusion or deception if certain conditions are not met. *See, e.g.*, Letter from Linda A. Lacewell, Counsel for Economic and Social Justice, Office of the Attorney General of New York, to James E. Brown, Regional General Counsel, Aetna (Aug. 16, 2007), *available at* http://www.ag.ny.gov/media_center/2007/aug/Aetna%20Final.pdf.

[148] Sandra G. Boodman, *To Quell Criticism, Some Doctors Require Patients to Sign 'Gag Orders*,' WASH. POST, July 21, 2009, at HE01, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2009/07/20/AR2009072002335_pf.html.

[149] *Id.*

physician copyright ownership of any online reviews authored by the patient. Consumer advocates have challenged the legality of such agreements[150] and the Department of Health and Human Services Office of Civil Rights recently required one physician office to cease the practice of requiring such agreements in exchange for his compliance with HIPAA privacy rules.[151] Thus, such attempts by physicians to prevent negative feedback may have been short lived; in fact, it is reported that one of the primary companies helping physicians to craft such contracts has ceased to offer advice on the practice.[152]

FOIA and the Privacy Act

Slightly different, though related, concerns seem to underpin privacy protections currently enjoyed by physicians under FOIA and the Privacy Act. Courts have interpreted FOIA and the Privacy Act to prevent the release of individually identifiable information about the payments physicians earn from Medicare. The Department of Health and Human Services, still under the continuing effect of a 30-year-old permanent injunction based on FOIA, has also determined that it may not release physician-identifiable information about Medicare compensation. Several parties are currently seeking to challenge the 30-year injunction, including Dow Jones, the owner of the Wall Street Journal.[153] The determination that this information is protected even from FOIA

---

[150] For example, under consumer protection and anti-Strategic Lawsuits Against Public Participation (anti-SLAPP) laws.

[151] All Case Examples: Private Practice Ceases Conditioning of Compliance with the Privacy Rule, U.S. Department of Health and Human Services, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/allcases.html#case29.

[152] Medical Justice Terminates Illegal Doctor Review Contracts, Center for Democracy & Technology, Dec. 2, 2011, https://www.cdt.org/pr_statement/medical-justice-terminates-illegal-doctor-review-contracts.

[153] On September 26, 2011, the U.S. District Court for the Middle District of Florida granted motions to intervene in the injunction from Dow Jones and two other parties, giving them the opportunity to now challenge the continuing need for the order. It is reported that an evidentiary hearing to consider the interveners' motions to vacate the injunction is set for June 2012. *See* American Medical Association, Case Summaries by Topic: Freedom of Information Act, Florida Medical Association v. United States

requests is based on the courts' interpretation of the exemption from FOIA disclosure of personnel, medical, and "similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy."[154] The courts' findings that Medicare reimbursements and claims fall into this category seem to be based in part on the fact that this is financial information and also that, when combined with other information to generate reports, it could lead to the "prospect of misleading publicity, possibility of unwarranted professional and public criticism, and damage to professional reputation."[155]

The FOIA example is differs from other physician privacy protections in that FOIA is a statute of general applicability and thus the decision to prevent the disclosure of physician payment information is only partially related to underlying health policy considerations. The prime motivation for the courts' reading of the statute seems to be a general concern that the release of individual financial information is inherently a violation of personal privacy. Courts have also considered the possibility that the information could be used in a way that negatively impacts providers' reputations.

Prescribing History Data

A final, quite interesting example of an attempt to protect physician privacy did not survive Supreme Court review. However, it remains an important example of the ways in which policymakers may seek to maintain the confidentiality of data about

---

Department of HEW, 479 F.Supp. 1291 (1979), http://www.ama-assn.org/ama/pub/physician-resources/legal-topics/litigation-center/case-summaries-topic/freedom-information-act.page.

[154] *See, e.g.*, Consumers' Checkbook, Ctr. for the Study of Servs. v. U.S. Dep't of Health and Human Servs., 554 F.3d 1046, 1050 (D.C. Cir. 2009) (denying, partly because of physician privacy concerns, consumer group's request for Medicare claims data to determine the frequency with which certain procedures are performed, whether Medicare was paying physicians with questionable histories, and whether individual doctors are complying with the standard of care).

[155] Pub. Citizen Health Research Grp. v. Dep't of Health, Educ. and Welfare, 477 F. Supp. 595, 598¬–99, 603 (D.D.C. 1979), rev'd on other grounds, 668 F.2d 537 (D.C. Cir 1981).

physicians. Between 2006 and 2008, Vermont, Maine, and New Hampshire all enacted laws attempting to prohibit the unauthorized sale or dissemination of physician-identifiable prescribing history data for marketing purposes.[156] When patients fill prescriptions, pharmacies collect information about the prescribing physician and the medication prescribed.[157] Pharmacies may later sell that information to data mining companies, which use it to try to glean information about physician prescribing habits.[158] Pharmaceutical manufacturers in turn lease such information in order to more effectively market their drugs.[159] The Vermont legislature enacted their Prescription Confidentiality Law in part to protect the privacy of physician prescribers, and Vermont raised this as an important state interest in its brief to the Supreme Court, arguing that the law "protects a real and substantial privacy interest" of doctors as "customers" of pharmaceutical companies and because of the doctor-patient relationship.[160] However, in considering the case the court of appeals held that the referenced privacy interest was "too speculative" to justify restrictions on commercial speech.[161] The Supreme Court agreed, and in 2011 in *Sorrell v. IMS Health*,[162] struck down the Vermont law holding that it violated First Amendment commercial speech rights.[163] Although the Court acknowledged many of the reasons the legislature passed the bill (including, to "safeguard medical privacy and diminish the likelihood that marketing will lead to prescription decisions not in the best

---

156 *See* Sorrell v. IMS Health, 131 S.Ct. 2653, 2662 (2011) (describing the Vermont law).
157 William S. Bernstein, et al., *Supreme Court Strikes Down Vermont Prescriber Data-Restriction Law*, June 24, 2011, MANATT, http://www.manatt.com/newsletter-areas.aspx?id=14436.
158 *Id.*
159 *Id.*
160 *Id.*
161 *Id.* at 18.
162 131 S.Ct. 2653 (2011).
163 *Id.* (noting that the "creation and dissemination of information are speech within the meaning of the First Amendment").

interests of patients or the State,"[164] "avoidance of harassment, [protecting] the integrity of the doctor-patient relationship. . . improv[ing] public health and reduc[ing] healthcare costs,"[165] the Court held that the law was not "drawn to serve that interest" because pharmacies could continue to release physician prescribing information as long as it was not used for marketing.[166] The Court, however, seemed to leave open the possibility that Vermont and other states could protect physician prescribing information if they had better tailored the law.[167] Nevertheless, as of today, physician prescribing information remains unprotected and may still be sold, analyzed, and used for commercial purposes by pharmacies, data miners, and pharmaceutical companies.

THE TRANSPARENCY COUNTERWEIGHT

Although physicians have been modestly successful at achieving ad hoc privacy protections, these are clearly driven by very different, if sometimes overlapping, concerns. Additionally, the increased focus on patient autonomy and choice, quality, cost containment, and fraud detection have exerted opposing pressures on physician privacy. As a result, efforts to increase transparency in the health care field exert a powerful counterweight to efforts to protect physician privacy.

Physicians are now subject to numerous requirements to disclose individually identifiable information to patients or the public. Most of these requirements are of relatively recent vintage with the exception of informed consent doctrine. The informed consent doctrine requires that in communicating with patients about treatment decisions,

---

[164] *Id.* at 2659.
[165] *Id.* at 2668.
[166] *Id.*
[167] *Id.* at 2672 ("If Vermont's statute provided that prescriber-identifying information could not be sold or disclosed except in narrow circumstances then the State might have a stronger position.").

physicians have a duty to disclose "information material to a reasonable patient's informed decision."[168] However, because this is a state tort doctrine, it differs from state to state. In some cases, a physician's failure to disclose a history of substance abuse or the receipt of economic incentives has been held to contribute to a breach of the duty of informed consent.[169] Other cases, however, have not recognized the need to disclose similar information and many have rejected arguments that a physician should disclose information about his or her qualifications to treat the patient.[170] Additionally, it is important to note that informed consent is only helpful as a legal remedy to patients who are seeking treatment from a particular physician. The doctrine also requires an injury and that the plaintiff show that a reasonable patient would have declined treatment had they known of the information not disclosed.[171]

Some states have required the disclosure of physician-specific quality information and the federal government appears to be moving in this direction for the Medicare program. For instance, New York has for decades reported mortality rates associated with coronary artery bypass graft (CABG) surgery performed by individual surgeons.[172]

---

[168] Matthies v. Mastromonaco, 733 A.2d 456, 461 (N.J. 1999).

[169] Pape, *supra* note 4, at 986 (1997) (arguing that the "strongest argument for giving medical consumers information about their physicians is based on the doctrine of informed consent" and citing cases requiring the disclosure of information related to substance abuse, HIV-status, and economic incentives); *see also* Moore v. Regents of the University of California, 793 P.2d 479 (Cal. 1990) (allowing claims premised on informed consent and breach of fiduciary duty to proceed based on a physician's failure to disclose his intent to remove tumor cells from a patient for the creation of a cell line that he planned to patent).

[170] *See* Barry R. Furrow, *Doctors Dirty Little Secrets: The Dark Side of Medical Privacy*, 37 WASHBURN L.J. 283 (1998) (citing cases such as Ditto v. McCurdy, 947 P.2d 952, 958 (Haw. 1997); Abram v. Children's Hosp. of Buffalo, 524 N.Y.S.2d 418, 419 (N.Y. App. Div. 1989); and Whiteside v. Lukson, 947 P.2d 1263, 1265 (Wash. Ct. App. 1997)).

[171] *Matthies*, 733 A.2d at 462.

[172] *See,* William Sage, Joshua Graff Zivin, & Nathaniel B. Chase, *Bridging the Relational–Regulatory Gap: A Pragmatic Information Policy for Patient Safety and Medical Malpractice*, 59 VAND. L. REV. 1263, 1303–04 (2006). Although reporting was technically required, physician concerns with potential reputational harms may have led many to try to "game" the reporting system by avoiding complex cases or performing unnecessary bypasses on healthier patients. *Id.* Portions of the remainder of this subsection are adapted from Jennings, *supra* note 33.

However, some have expressed concerns that this disclosure requirement may have resulted in some doctors avoiding sicker patients who might have a higher risk or mortality in surgery.

Physicians must also now disclose many financial conflicts of interest to patients or to federal or state governments. For example, physicians must disclose ownership interests they hold in specialty hospitals or certain ancillary equipment such as MRIs, CTs, or PET machines.[173] However, disclosure of these ownership interests mostly occur within the physician–patient relationship (i.e. from a physician to a current patient) and thus may not be available to the public at large or prospective patients.

Over the last two decades, in response to concerns about physicians' financial conflicts of interest, some states have enacted financial reporting or disclosure policies. Minnesota, for example, enacted a requirement in 1993 to require that pharmaceutical companies disclose gifts over $100 annually to physicians.[174] Additionally, as of 2009, five other states and the District of Columbia had implemented legislation or regulations relating to pharmaceutical conflicts of interest. Most, though not all, of the laws apply only to pharmaceutical payments and do not require reporting of compensation from device or biologics manufacturers.[175] Additionally, only the Minnesota law explicitly requires disclosures to be public records[176] and even this requirement has not resulted in effective public availability. For example, Public Citizen noted in Congressional

---

[173] *Changes to the Federal Physician Self-Referral Law Included in the Patient Protection and Affordable Care Act*, EPSTEINBECKERGREEN, Apr. 19, 2010, www.ebglaw.com/files/39133_Implementing%20Health%20and%20Insurance%20Reform%20Stark%20Matyas%204%209%2010%20.pdf.

[174] Testimony of Peter Lurie, M.D., M.P.H., Deputy Director, Public Citizen's Health Research Group on State Laws Requiring Disclosure of Pharmaceutical Company Payments to Physicians before the Senate Special Committee on Aging, June 27, 2007, *available at* http://www.citizen.org/Page.aspx?pid=740#testimony.

[175] *Id.*

[176] Steinbrook, *supra* note 34.

testimony that its researchers had to physically travel to Minnesota and make copies of each submitted disclosure at a cost of $0.25 per page in order to obtain the data.[177]

Perhaps in response to Congressional investigations and high-profile news stories about physicians receiving millions of dollars in consulting fees from pharmaceutical manufacturers, drug makers and large health centers have begun to voluntarily disclose financial arrangements with individual physicians.[178]

In 2010, Congress passed the Affordable Care Act, which included a number of provisions related to physician transparency. The Act requires the public disclosure of information relating to the financial relationships of physicians and teaching hospitals with pharmaceutical, device, and medical supply manufacturers. Specifically, manufacturers must disclose financial arrangements with individual physicians to the Secretary of Health and Human Services.[179] The Secretary must make the previous year's disclosures available through a searchable website in a form that can be easily downloaded by physician and aggregated.[180] Manufacturers and physicians have an opportunity to review the information and submit corrections before publication.[181]

The ACA also requires physician-owned hospitals to report annually to the Secretary the names of each physician owner and the "nature and extent of all ownership

---

[177] Testimony of Peter Lurie, *supra* note 174.

[178] Senator Chuck Grassley (R-IA) has spent considerable time investigating relationships between physicians and pharmaceutical, device, and biologic makers. Beginning in early 2008, he began to investigate the industry ties of medical researchers. Controversy erupted later that year when it was reported that one of the physicians, Dr. Charles Nemeroff, Chairman of the Department of Psychiatry at Emory University, had earned $2.8 million in consulting fees from pharmaceutical manufactures from 2000 to 2007. Of that amount, he had failed to disclose at least $1.2 million to Emory in violation of both the University's policies and National Institutes of Health grant recipient rules. *See* Steinbrook, *supra* note 34; Reed Abelson, Cleveland Clinic Discloses Doctors' Industry Ties, N.Y. TIMES, Dec. 2, 2008, *available at* http://www.nytimes.com/2008/12/03/business/03clinic.html?pagewanted=all.

[179] Patient Protection and Affordable Care Act, Pub. L. No. 111-148, § 6002 (2010).

[180] *Id.*

[181] *Id.*

and investment interests" in the hospital.[182] This information is to be updated annually and published on the CMS website.[183] Additionally, physician-owned hospitals must require referring physician owners or investors to inform referred patients about their ownership interest in the hospital as well as the ownership or investment interests of the treating physician.[184]

Although physician resource utilization data is not yet public, the ACA requires that the Secretary begin to send reports to physicians comparing their resource use under Medicare with that of other physicians.[185] The reports, which began to be released to physicians in four states in March 2012,[186] rely on claims data and are "confidential." The program will be important in determining the feasibility of tracking and disclosing information about physician resource utilization and may expose any administrative or methodological difficulties in producing useful reports.[187]

---

[182] Patient Protection and Affordable Care Act, Pub. L. No. 111-148, § 6001 (2010).
[183] *Id.*
[184] *Id.*
[185] Patient Protection and Affordable Care Act, Pub. L. No. 111-148, § 3003.
[186] *See* Jordan Rau, *Medicare to Tie Doctors' Pay to Quality, Cost of Care*, KAISER HEALTH NEWS, Apr. 15, 2012, available at http://www.kaiserhealthnews.org/Stories/2012/April/15/medicare-doctor-pay.aspx (describing the release of the reports).
[187] *See id*. (noting that the method used to generate the reports is "widely considered so crude that few expect CMS will ultimately use it in payment" and quoting one health plan official as saying "[t]here really are very few measures that . . . can [be] reliably evaluate[d] on the individual doctor level").

Chapter 5: Developing a Physician Privacy Framework

The previous Chapter showed that physicians have succeeded in protecting their "privacy" in a number of ways despite some countervailing requirements for transparency. However, the piecemeal nature of privacy protections and disclosure requirements demonstrates the absence of any cohesive theory of physician privacy. It also shows that while "privacy" can be a convenient shorthand buzzword, it is not a unitary term and its use obscures the many different interests and values underlying it. Policymakers need a more precise analytical framework for evaluating the true impact of various proposals on physicians' nominal "privacy" interests.

I argue that efforts to protect physician privacy ultimately reflect four primary considerations: (1) the protection of physicians' professional authority and autonomy; (2) concerns about the economic and competitive impact of information disclosure; (3) personal dignity; and (4) the practical limitations of information collection, use, storage, and disclosure.

These considerations are not completely distinct and there is substantial overlap between the four categories. For example, reputational concerns fall under multiple categories because they not only affect income-producing factors such as the ability to obtain patients and hold hospital privileges, but also the physician's personal dignity and desire to be respected in the eyes of his or her peers and practical concerns regarding potentially inaccurate data.

Although all of the categories are relevant, two appear to predominate in efforts to protect physician privacy. Professional authority and autonomy and economic concerns are almost always at the core of efforts to retain the confidentiality of physician

information. This is not to say that personal dignity impacts and practical considerations are not important. They are significant and the practical limitations of transparency efforts in particular should not be understated. Nevertheless, the most heated debates seem to be more related to economic and autonomy considerations.

Below, I discuss the four aspects of the framework in further detail and show how efforts to protect physician privacy reflect each.

PROFESSIONAL AUTONOMY & AUTHORITY

Protection of professional autonomy and authority is a recurring theme underlying concerns about physician "privacy." As Chapter 1 illustrated, the professional authority paradigm dominated U.S. health law and policy for almost a century and continues to hold sway to some degree today. Physicians and others remain concerned about the interference of government and corporate actors in the provision of health care, whether that interference is explicit or more subtle. This should not be surprising given the historical effort by physicians to guard the practice of medicine as the exclusive domain of doctors. Physicians, for instance, have insulated their authority by lobbying for laws banning the practice of medicine by corporations, requiring prescriptions for the dispensing of pharmaceuticals, and retaining hospital admitting privileges, among other tools. These types of efforts are not atypical of a "profession." For example, sociology professor Eliot Friedson defined a "professional" as "a person involved in an occupation which has assumed a dominant position in a division of labor so that it gains control over the determination of the substance of its own work."[188]

---

[188] Clark C. Havighurst, et al., HEALTH CARE LAW AND POLICY 294 (2d ed., 1998) (quoting Eliot Freidson, PROFESSION OF MEDICINE xvii (1970)).

The historical maintenance of control over patient medical records is the most obvious example of efforts to maintain physician authority through privacy. However, patients have had a federal right to access their medical records for over a decade and physicians have endorsed a similar right for nearly thirty years. Thus, the example has only limited relevance to future discussions about physician privacy.

However, concerns raised about health plan and patient evaluations seem particularly relevant to physician autonomy. In particular, health plan efforts to publicly rate physicians or to otherwise police the quality of the care they provide may be viewed as a direct intrusion into physician autonomy. Such practices mean that physicians must conform their practice habits to meet the standards against which they will be evaluated by plans. To the extent that physicians disagree with the measures or standards chosen by the plan, they may or may not have an opportunity to contest these measures or to explain to patients why they disagree with the plan's evaluation.

These concerns relate to similar, but distinct, worries about the unintended behavioral effects of transparency initiatives in terms of both innovation and the treatment of sicker patients. Physicians whose performance is being publicly disclosed may be inhibited from departing from the standard of care in innovative ways that could benefit patients. They may also avoid treating seriously ill or complex patients who are more likely to experience poor outcomes and thus make the physician appear to be lower performing. By influencing behavior in this way, even if unintended, such initiatives may directly affect physician autonomy and authority. Such an effect would be even more pronounced should plans or other entities use physician information to develop best practices or clinical decision support tools that physicians are required or incentivized to use.

Another autonomy concern is not so much about a compulsion to practice in a certain way or unintended behavioral effects, but about *intended* external influences that may bias physician decision making. This is one of the issues apparently driving the state laws found unconstitutional in *Sorrell v. IMS Health*. These laws sought to restrict the dissemination or sale of physician-identifiable prescribing data for purposes of pharmaceutical marketing. Many physicians may prefer that their prescribing patterns or other medical decisions not be used to target them with advertisements or marketing. Such efforts attempt to influence medical judgment and thus directly implicate physician autonomy.

ECONOMIC HARMS

Privacy protections sought by physicians have often sought to protect against economic harm that might result from transparency or disclosure of certain information. Negative reputational effects are a chief concern in this area because of the impact they can have on physician privileging, referrals, patient base, and potentially, preferred provider status in health plan networks. The tort law tools mentioned above, such as defamation suits, are used to obtain redress for damaging information that may harm physician reputation and in turn result in economic harm. Reputational concerns and the potential for malpractice claims are also some of the factors that have driven the desire to maintain the confidentiality of peer review proceedings, the National Practitioner Data Bank, and medical error reporting to Patient Safety Organizations.

Greater transparency and disclosure also raises other questions about financial liability, both for the physician about whom data relates and any entity disclosing physician-identifiable information. There seems to be a general fear that greater

transparency could lead to more frequent malpractice suits. Additionally, to the extent that physicians are responsible for disclosing any information about other physicians, they could be subject to civil liability for defamation or other tort claims.

Increased transparency may also impact competition with other physicians or providers. Although competition and profit motive have historically been anathema to medical ethics, a changing health care market and greater comparative information about providers could lead physicians to more openly compete for patients, hospital privileges, and preferred provider status. Additionally, physicians whose practice information is more public may face competition from non-physician providers such as retail clinics and from hospitals and health plans purchasing physician group practices.

There is a final economic undercurrent to some of the efforts to maintain physician privacy. There is an aspect of privacy that seems related to "found value" in data and the prevention of uncompensated appropriation of information for others' economic gain. For example, physician prescriptions are no longer simply used to transmit a prescription order from doctor to pharmacist. Instead, they may now be aggregated, analyzed, and sold to pharmaceutical companies to marketing purposes. This type of value creation with physician data is not limited to the pharmaceutical context. Heath plans and data analytic firms can use physician claims data to support disease and quality research. These types of secondary data uses may raise legitimate concerns about the uncompensated use of data created by physicians for economic gain by a third party. Although it is no doubt the case that an individual physician's data is less valuable to her than to those who can aggregate it with other data, possible concerns about uncompensated appropriation remain.

PERSONAL DIGNITY

Physicians have several types of dignitary concerns with the widespread disclosure of more information about themselves. These include reputational concerns, embarrassment, and the ability to make decisions for one's self and the ability to control the flow of identifiable information about one's self.

A physician's reputation is not only a key component of his or her ability to enjoy professional and financial success, but has psychic and emotional value as well. As with most professionals, most physicians value the respect of their peers and the self esteem they gain from feeling that they do important and high quality work.[189] To the extent that transparency exposes substandard care, mistakes, or inaccurate information suggesting substandard care or mistakes, this could embarrass physicians and affect some of the emotional benefit they gain from their work.

This type of reputational or emotional concern seems to be one concern regarding transparency of the National Practitioner Data Bank, which houses information about malpractice payments and disciplinary actions. Greater disclosure of such information could subject physicians to negative publicity or cause patients or their peers to question their competence. This impacts not only professional autonomy and economic interests, but a physician's dignitary interests as well.

Physician privacy in the FOIA context also seems to play into concerns about reputation and embarrassment. For some reason, the disclosure of information about Medicare compensation makes some physicians squeamish. This does not seem to be

---

[189] *See, e.g.*, Sage, Zivin, & Chase, *supra* note 172, at 1297 (2006) (noting that, with respect to disclosure of medical errors, physicians' "resistance to public disclosure of their mistakes extends beyond a fear of courts . . . [given that] reputation has traditionally been at the center of medical professionalism, affecting self-image, collegial relationships, and the economics of access to patients").

driven by concerns about possible identity theft or other economic harms, but about some sort of distaste for the release of information about money earned from Medicare.

A final dignitary concern relates to the inability of physicians to control the future flow of data about themselves. Although this ties into the economic concerns outlined above regarding uncompensated uses of data, there is a slightly different fear at play here. Rather than a lack of compensation or a concern that others will "cash in" on one's information, this concern relates to a more basic human desire to be able to make decisions for one's self and to determine what information one will share publicly. This is not as much about professional autonomy as it is about personal autonomy and self-determination. For instance, although some physicians might be willing to voluntarily share information with others about their prescribing habits or outcomes, subsequent *unauthorized* secondary use of this information seems somehow offensive.

PRACTICAL BARRIERS

Numerous practical considerations may suggest the need to ensure that physicians have privacy protections for certain types of information or data. As discussed earlier, privacy and confidentiality protections have been granted in the context of medical peer review and medical error reporting in order to convince providers to engage in these initiatives. Privacy becomes a necessary condition of widespread reporting.

Another consideration that may underlie physicians' desire to keep some information private is the time, effort, and cost of disclosing the data. Data disclosure may require more detailed record-keeping, additional staff, time spent inspecting and correcting errors, etc. Heavier administrative burdens translate into less time for patient care. Some of these concerns may be partially alleviated by having larger entities, rather

than physicians, responsible for reporting certain information. For example, ACA provisions relating to payments from pharmaceutical and device makers require that the manufacturers report the required data rather than having individual physicians report. Additionally, to the extent that medical records and billing are becoming increasingly digitized, reporting burdens could be reduced. However, the ease with which larger entities and those with more advanced health IT systems can report data may also put them at a competitive advantage over smaller practices if they are able to more easily adapt to new transparency efforts.

A similar concern relates to the overall feasibility of maintaining accurate data and developing quality and cost measures that truly reflect provider care. Data used for quality measurement, research, and cost control may include poorly defined fields, inconsistency or variation in how practitioners report, misreporting from patients, and a host of other practical and technological problems. Any transparency initiative that involves the disclosure of physician-identifiable data is likely to be accompanied by concerns that data will be inaccurate, will need to be corrected, or will need to be explained in some manner. Even when data is not technically "inaccurate" it may not obviously show the underlying causes of seemingly high costs or poor quality. For instance, medical errors may be caused by institutional or systemic deficiencies rather than provider mistake. High mortality rates may be attributable to treating sicker patients with multiple chronic illnesses. Higher costs may reflect local practice patterns and prices. If not explained, such indicators may unfairly put some physicians in a negative light.

A final practical concern for many physicians is data security. Even if doctors are willing to share much information about themselves with government, health plans,

researchers, and/or patients, they will want to ensure that their data is used for the intended purpose and that breaches do not result in misuse, identity theft, or the like.

Conclusion

The framework outlined in the previous Chapter reflects the primary concerns that appear to be driving physician unease about the issues of transparency and privacy. The concerns are not wholly distinct but interact with one another in a variety of ways. Some specific worries are multifaceted, with aspects falling into multiple categories (for example, reputational harm or unauthorized secondary uses of information). Other concerns more clearly relate to one category or another.

The goal of devising a framework like this is to help physicians, policymakers, and others to better articulate the considerations and values that underlie discussions about privacy and transparency. If stakeholders can better convey their priorities and fears, they are more likely to come up with cooperative solutions to improve the health care system. While not perfect, this framework can hopefully spur discussion about a neglected but critical topic.

It is important to note what this framework and this Report do *not* do. First, neither the Report nor the framework make a normative claim about the level of privacy protection that physicians *should* enjoy. This is something that policymakers and scholars should consider by weighing privacy values and interests against the needs for health system improvement.

The framework cannot take account of all of the heterogeneity in the medical profession. For example, different interests will be more or less important to particular physicians. The composition of a physician's patient population, the share of his or her income from public or private payers, and his or her status as a salaried employee will all affect how he views privacy matters.

This framework is a suggested starting point for thinking about physician privacy, but it is also important to recognize the changes in the health care system that could alter it. For example, the health system has of late been moving away from the historic small business model toward the provision and funding of medical care by larger corporate entities and hospital- or plan-employed physicians. These types of system-wide shifts may significantly alter how we think about physician privacy and some of the underlying concerns at play.

Finally, this Report does not attempt to address interplay of physician and patient privacy interests. This is important to note because information about physicians will almost always pertain to patients as well. There may be areas in which physicians are more than willing to allow disclosure of their own data to government, researchers, or others, but where contrary patient concerns suggest a need to keep such information confidential. One example of this might be the use of anonymized, aggregate surveillance data used to detect adverse pharmaceutical effects. While physicians may not be concerned with the sharing of this type of non-identifiable information with the Food and Drug Administration, for example, some patients may not want their data used for any purpose.

Regardless of these limits, this Report should help to illuminate a subject that needs attention and provide a possible framework for further work. By breaking out the various values underlying physician privacy, the framework can also help physicians, industry, government, and other stakeholders to talk about privacy in a more productive manner by honing in on the concerns and values that affect physicians most.

Bibliography

Abelson, Reed. "Cleveland Clinic Discloses Doctors' Industry Ties." *New York Times* (December 2, 2008) http://www.nytimes.com/2008/12/03/business/03clinic.html?pagewanted=all.

"Access of individuals to protected health information." *Code of Federal Regulations*. Title 45. Section 164.524 (2001).

Administrative Procedure Act, 5 U.S.C. § 552a(b).

Administrative Procedure Act, 5 U.S.C. § 552(a)(3).

Administrative Procedure Act, 5 U.S.C. § 552(b)(6).

American Medical Association, Medical Peer Review, http://www.ama-assn.org/ama/pub/physician-resources/legal-topics/medical-peer-review.page.

Arrow, Kenneth J. "Uncertainty and the Welfare Economics of Medical Care." *American Economic Review* 53 (1963): 941–973.

Bassler, Alissa Marie. "Comment, Federal Law Should Keep Pace with States and Recognize a Medical Peer Review Privilege." *Idaho Law Review* 39 (2003): 689–712.

Bernstein, William S., et al. "Supreme Court Strikes Down Vermont Prescriber Data-Restriction Law." Manatt (June 24, 2011) http://www.manatt.com/newsletter-areas.aspx?id=14436.

Boodman, Sandra G. "To Quell Criticism, Some Doctors Require Patients to Sign 'Gag Orders,'" *Washington Post* (July 21, 2009) http://www.washingtonpost.com/wp-dyn/content/article/2009/07/20/AR2009072002335_pf.html.

Borzo, Greg. "Up the Data Stream Without a Paddle: Physicians' Right to Privacy in the Electronic World." *American Medical News* (March 9, 1998), http://www.ama-assn.org/amednews/1998/net_98/logo0309.htm.

Cal. Med. Ass'n v. Blue Shield of Cal. Life & Health Ins., No. RG10535619 at 2 (Cal. Super. Ct. 2011)

———. Case Summaries by Topic: Freedom of Information Act, Florida Medical Association v. United States Department of HEW, 479 F.Supp. 1291 (1979), American Medical Association, http://www.ama-assn.org/ama/pub/physician-resources/legal-topics/litigation-center/case-summaries-topic/freedom-information-act.page.

———. Changes to the Federal Physician Self-Referral Law Included in the Patient Protection and Affordable Care Act, EpsteinBeckerGreen (April 19, 2010), http://www.ebglaw.com/files/39133_Implementing%20Health%20and%20Insurance%20Reform%20Stark%20Matyas%204%209%2010%20.pdf.

Clinical Decision Support Initiative, Agency for Healthcare Research and Quality, U.S. Department of Health and Human Services, http://healthit.ahrq.gov/portal/server.pt?open=512&objID=654&PageID=13665&mode=2&cached=true&wtag=wtag666.

Consumers' Checkbook, Ctr. for the Study of Servs. v. U.S. Dep't of Health and Human Servs., 554 F.3d 1046 (D.C. Cir. 2009).

The Data Bank – About Us, The Data Bank: National Practitioner/ Healthcare Integrity & Protection. http://www.npdb-hipdb.hrsa.gov/topNavigation/aboutUs.jsp.

DCMS Glossary of Healthcare Terms & Acronyms, Dallas County Medical Society, http://www.dallas-cms.org/glossary.cfm.

Elhauge, Einer. "Allocating Health Care Morally." *California Law Review* 82 (1994): 1449–1544.

Flynn, Ruth E. "Demand for Public Access to the National Practitioner Data Bank: Consumers Sound Their Own Death Cry." Hamline Journal of Public Law and Policy 18 (1996):251–279.

Frank, Christopher. "Improving Decision Making in the World of Big Data." *Forbes* (March 25, 2012) http://www.forbes.com/sites/christopherfrank/2012/03/25/improving-decision-making-in-the-world-of-big-data/.

Furrow, Barry R. "Doctors Dirty Little Secrets: The Dark Side of Medical Privacy." *Washburn Law Journal* 37 (1998): 283.

Griswold v. Connecticut, 381 U.S. 479 (1965).

Groenfeldt, Tom. "Big Data Saves Michigan $1 Million Each Business Day." *Forbes* (January 1, 2012) http://www.forbes.com/sites/tomgroenfeldt/2012/01/11/big-data-saves-michigan-1-million-each-business-day/print/

Halpern, Sydney A. "Medical Authority and the Culture of Rights." Journal of Health Politics, Policy & Law 29 (2004): 835–852.

Havighurst, Clark C., et al. *Health Care Law and Policy*. Foundation Press, 1998.

Health Care Quality Improvement Act of 1986, 42 U.S.C. § 11137(b).

Helling, Dave. "Senator Joins Fight to Reopen Database Website Shut Down by Government." *Kansas City Star* (November 3, 2011) http://www.kansascity.com/2011/11/03/3247032/senator-joins-fight-to-reopen.html.

Hill, Colin. "Can Big Data Fix Healthcare?" *Forbes* (November 17, 2011) http://www.forbes.com/sites/colinhill/2011/11/17/can-big-data-fix-healthcare/.

———. The Hippocratic Oath: Text, Translation, and Interpretation (Ludwig Edelstein, Johns Hopkins Press, 1943), http://www.pbs.org/wgbh/nova/body/hippocratic-oath-today.html#classical

Howard, Alex. "Data, Health IT and Patient Empowerment Can Revolutionize Healthcare." *Forbes* (March 14, 2012) http://www.forbes.com/sites/oreillymedia/2012/03/14/data-health-it-and-patient-empowerment-can-revolutionize-healthcare/.

Jennings, Paige M. "Physician Privacy and Information Policy." Unpublished manuscript prepared for Advanced Policy Economics, Lyndon B. Johnson School of Public Affairs, last modified December 2011. Microsoft Word file.

Johnson v. Kokemoor, 545 N.W. 2d 495 (Wis. 1996).

Kanwit, Stephanie. "Transparency in Principle and in Practice: Health Insurance Plan Perspectives." Presentation at the FTC Innovations in Health Care Delivery Public Workshop, Washington, D.C., April 24, 2008, http://www.ftc.gov/bc/healthcare/hcd/docs/Kanwit.pdf.

Linda A. Lacewell, Counsel for Economic and Social Justice, Office of the Attorney General of New York. Letter to James E. Brown, Regional General Counsel, Aetna (Aug. 16, 2007). http://www.ag.ny.gov/media_center/2007/aug/Aetna%20Final.pdf.

Lawrence v. Texas, 539 U.S. 558 (2003).

Matthies v. Mastromonaco, 733 A.2d 456, 461 (N.J. 1999).

———. Medical Justice Terminates Illegal Doctor Review Contracts. Center for Democracy & Technology (December 2, 2011) https://www.cdt.org/pr_statement/medical-justice-terminates-illegal-doctor-review-contracts.

Moore v. Regents of the University of California, 793 P.2d 479 (Cal. 1990)

NAACP v. Alabama, 357 U.S. 449 (1958).

NASA v. Nelson, 131 S.Ct. 746 (2011).

Nixon v. Administrator of General Services, 433 U.S. 425 (1977),

Pape, Julie Barker. "Note, Physician Data Banks: The Public's Right to Know Versus the Physician's Right to Privacy." Fordham Law Review 66 (1997): 975–1028.

Parmet, Wendy E. "Unprepared: Why Health Law Fails to Prepare Us for a Pandemic." *Journal of Health and Biomedical Law* 2 (2006): 157–193.

Patient Protection and Affordable Care Act, Pub. L. No. 111-148 (2010).

Patient Protection and Affordable Care Act, Pub. L. No. 111-148, § 3003 (2010).

Patient Protection and Affordable Care Act, Pub. L. No. 111-148, § 6001 (2010).

Patient Protection and Affordable Care Act, Pub. L. No. 111-148, § 6002 (2010).

Patient Safety and Quality Improvement Act, Pub. L. No. 109-41, 119 Stat. 424 (2005).

Patient Safety Organizations, Agency for Healthcare Research and Quality, U.S. Department of Health and Human Services, http://www.pso.ahrq.gov.

Paul v. Davis, 424 U.S. 693 (1976).

Poliner v. Texas Health Systems, 2003 U.S. Dist. LEXIS 17162 (N.D. Tex. 2003).

Pritts, Joy L. "Altered States: State Health Privacy Laws and the Impact of the Federal Health Privacy Rule." *Yale Journal of Health Policy, Law and Ethics* (2002): 325–349.

Prosser, William. "Privacy." California Law Review 48 (1960): 383–423.

Pub. Citizen Health Research Grp. v. Dep't of Health, Educ. and Welfare, 477 F. Supp. 595 (D.D.C. 1979), *rev'd on other grounds*, 668 F.2d 537 (D.C. Cir 1981).

Putting the 'I' in Health IT: Pledge, HealthIT.gov, http://www.healthit.gov/pledge/?submit.x=253&submit.y=34&submit=Send.

Rau, Jordan. "Medicare to Tie Doctors' Pay to Quality, Cost of Care." *Kaiser Health News* (April 15, 2012) http://www.kaiserhealthnews.org/Stories/2012/April/15/medicare-doctor-pay.aspx.

———. Resources: Public Use Data File, The Data Bank: National Practitioner/ Healthcare Integrity & Protection, http://www.npdb-hipdb.hrsa.gov/resources/publicData.jsp.

Restatement (Second) of Torts (1977).

Richards, Neil M. and Daniel J. Solove. "Privacy's Other Path: Recovering the Law of Confidentiality." Georgetown Law Review 96 (2007): 123–182.

Roe v. Wade, 410 U.S. 113 (1973).

Rosenblatt, Rand E. "The Four Ages of Health Law." Health Matrix 14 (2004): 155–196.

Rosenblatt, Rand E., Sylvia A. Law, and Sara Rosenbaum. *Law and the American Health Care System*. Foundation Press, 1987.

Sage, William M. "Regulating Through Information: Disclosure Laws and American Health Care." Columbia Law Review 99 (1999): 1701–1829.

Sage, William M. "Reputation, Malpractice Liability, and Medical Error." Chap. 10 in *Accountability: Patient Safety and Policy Reform*. Georgetown University Press, 2004.

Sage, William, Joshua Graff Zivin and Nathaniel B. Chase. "Bridging the Relational–Regulatory Gap: A Pragmatic Information Policy for Patient Safety and Medical Malpractice." Vanderbilt Law Review 59 (2006): 1263–1308.

Scheutzow, Susan O. "State Medical Peer Review: High Cost But No Benefit—Is it Time for a Change?" *American Journal of Law and Medicine* 25 (1999): 7–58

Segal, Jeffrey, et al. "Legal Remedies for Online Defamation of Physicians." *Journal of Legal Medicine* 30 (2009): 349–388.

Selyukh, Alina. "Government Reopens Doctor Data Access, with Some Caveats." *Reuters* (November 8, 2011) http://www.reuters.com/article/2011/11/09/us-usa-malpractice-database-idUSTRE7A87QJ20111109.

Simonsen v. Swenson, 177 N.W. 831 (Neb. 1920).

Solove, Daniel J. *The Digital Person: Technology and Privacy in the Information Age*. NYU Press, 2004.

Solove, Daniel J. "A Taxonomy of Privacy." *Pennsylvania Law Review* 154 (2006): 477–564,

Sorrell v. IMS Health, 131 S.Ct. 2653, 2662 (2011)

Starr, Paul. *The Social Transformation of American Medicine*. Basic Books, 1982.

———. *State Laws Requiring Disclosure of Pharmaceutical Company Payments to Physicians*. Before the Senate Special Committee on Aging, 110th Cong. (2007) (statement of Peter Lurie, M.D., M.P.H., Deputy Director, Public Citizen's Health Research Group).

Steinbrook, Robert. "Perspective: Online Disclosure of Physician–Industry Relationships." *New England Journal of Medicine* 360 (2009):325–327.

Strahilevitz, Lior Jacob. "Reunifying Privacy Law." *California Law Review* 98 (2010): 2007–2048.

"Uses and disclosures for which an authorization is required." *Code of Federal Regulations*. Title 45. Section 164.508(a) (2001).

U.S. Const. amend. I.

U.S. Const. amend. IV.

U.S. Const. amend. V.

U.S. Department of Health, Education, and Welfare. Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Commission on Automated Personal Data Systems (1973).

U. S. Dep't of State v. Wash. Post Co., 456 U.S. 595 (1982).

Vickery, Alan B. "Note, Breach of Confidence: An Emerging Tort." *Columbia Law Review* 82 (1982): 1426–1468.

Warner, David C. and Budd N. Shenkin. "Giving the Patient His Medical Record: A Proposal to Improve the System." *New England Journal of Medicine* 289 (1973): 688–692.

Warren, Samuel D. and Louis D. Brandeis. "The Right to Privacy." Harvard Law Review 4 (1890): 193–220.

Whalen v. Roe, 429 U.S. 589 (1977).

Wisconsin v. Constantineau, 400 U.S. 433 (1971).