Yale ISPS

Institution for Social and Policy Studies

ADVANCING RESEARCH • SHAPING POLICY • DEVELOPING LEADERS

PATIENT HEALTH DATA PRIVACY

ISPS-BIOETHICS WORKING PAPER

ISPS14-028

[14 OCTOBER 2014]

BONNIE KAPLAN, PHD, FACMI

CENTER FOR MEDICAL INFORMATICS

INTERDISCIPLINARY BIOETHICS CENTER

INFORMATION SOCIETY PROJECT

Beyond IP: The Future of Privacy, ed. Shlomit Yanisky-Ravid, New York: Fordham University Press (forthcoming) – DRAFT CHAPTER

I. INTRODUCTION

How private is medical and health data? Well-known cases of lost, stolen, or hacked computers or storage devices;[1] reported snooping into celebrity data, or even that of neighbors or divorced spouses;[2] and other computer breaches involving health records,[3] are disturbing news. When reported data breaches affect more than 500 individuals, they are posted by the US Department of Health and Human Services. This "wall of shame" makes it evident that hundreds of thousands of data records can be

[1] Six of the ten largest reported data breaches at healthcare organizations in 2013 involved unencrypted stolen computers. The largest occurred when the Utah Department of Health's server containing information on 780,000 patients was hacked (Erin McCann, Infographic: biggest healthcare data breaches of 2012, available at http://www.healthcareitnews.com/news/infographic-biggest-healthcare-data-breaches-2012, (last visited January 29, 2014). Insurers and treatment centers also are vulnerable. Stolen laptops potentially compromised nearly 840,000 individuals insured by Horizon Blue Cross Blue Shield of New Jersey (Marianne Kolbasuk McGee, Unencrypted Laptops Lead to Mega-Breach, Data Breach Today, December 9, 2013, available at http://www.databreachtoday.com/unencrypted-laptops-lead-to-mega-breach-a-6277/op-1, (last visited January 29, 2014) and more than four million patients were affected by theft of unencrypted computers Advocate Medical Group of Chicago, resulting in a class-action lawsuit by patients (Nicole Freeman, Healthcare's Most Significant Data Breaches of 2013, Health IT Security, December 23, 2013, available at http://healthitsecurity.com/2013/12/23/healthcares-most-significant-data-breaches-of-2013/, (last visited January 29, 2014). A missing USB flash drive put 49,000 Kaiser Permanente patients at risk September 25, 2013; the device was unencrypted and not password protected. Also that month a recipient outside the Kaiser network received electronic mail from Kaiser that contained protected patient information, jeopardizing 670 patients (Erin McCann, Kaiser reports second fall data breach, Healthcare IT News, November 26, 2013, available at http://www.healthcareitnews.com/news/kaiser-reports-second-fall-data-breach, (last visited January 29, 2014).

[2] Patrick Ouellette, Cedars-Sinai Experiences Celebrity Patient Data Breach, July 15, 2013, available at http://healthitsecurity.com/2013/07/15/kim-kardashians-patient-data-breached-at-cedars-sinai/, (last visited January 29, 2014; Nicole Freeman, Healthcare's Most Significant Data Breaches of 2013, Health IT Security, December 23, 2013, available at http://healthitsecurity.com/2013/12/23/healthcares-most-significant-data-breaches-of-2013/, (last visited January 29, 2014; Anna Gorman and Abby Sewell, Six people fired from Cedars-Sinai over patient privacy breaches, Los Angeles Times, July 12, 2013, available at http://articles.latimes.com/2013/jul/12/local/la-me-hospital-security-breach-20130713, (last visited January 29, 2014).

[3] Elizabeth Layman, *Health Informatics: Ethical Issues*, 22 HEALTH CARE MANAGER 2(2003).

exposed in a single breach.[4] Even more are expected.[5] Two highly regarded medical centers, New York-Presbyterian Hospital and Columbia University Medical Center, agreed to pay the largest fine yet imposed because 6800 patients' personal health information was internet-accessible in 2010 due to willful deficiencies in data security practices.[6]

Medical and health care data kept in computer systems are vulnerable to the same kinds of privacy, security, and confidentiality violations as any other data. These violations are not limited to what the news reports, so may escape public attention and legislative action. Data may be exposed in cases of individual identify theft or voluntary sharing of identifiers such as governmental identification numbers or individuals' passwords. Travelers crossing borders may be subject to having their computers searched,[7] or even confiscated, posing other potential threats if data related to health care, treatment, or research is accessible on those devices. Data may be intercepted as it is transmitted between devices, for example, from a mobile phone to a medical electronic record. Malware pre-installed in counterfeit electronic components may leak data to

[4] Section 13402(e)(4) of the HITECH Act requires the Secretary of Health and Human Services to post a list of breaches of unsecured protected health information affecting 500 or more individuals. They are at posted at http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html, (last visited January 14, 2014). The site lists only those breaches that have been reported, and only breaches by covered entities, according to http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html, (last visited January 14, 2014). Linda Koontz, *What Is Privacy?*, *in* INFORMATION PRIVACY IN THE EVOLVING HEALTHCARE ENVIRONMENT (Linda Koontz ed. 2013).

[5] David F. Carr, *Healthcare Data Breaches To Surge In 2014*(December 26, 2013), *available at* http://www.informationweek.com/healthcare/policy-and-regulation/healthcare-data-breaches-to-surge-in-2014/d/d-id/1113259 (last visited January 29, 2014).

[6] Erin McCann, *Groups Hit with Record $4.8M HIPAA Fine*(May 8, 2014), *available at* http://m.healthcareitnews.com/news/group-slapped-record-hipaa-fine (last visited May 12, 2014)..

[7]

criminals and spies.[8] Government agencies such as the US Internal Revenue Service may surveille or seize data, including medical data, with or without warrant, to use for investigations or other purposes for which it was not originally collected. US government fusion centers can combine individual health and medical data with driving and license records, education records, criminal records, voting registration records, and other information in ways difficult for the general public to know for reasons of national security.[9] Also tied to security, but more targeted to health-related data, is on-going biosurveillance to detect bioterrorism as well as public health surveillance (such as that done by the US Centers for Disease Control) needed to track disease patterns and potential epidemics. Further, as disclosed in leaks about the US National Security Administration, widespread data collection, internet transmissions and telephone records are collected, de-encrypted, and stored,[10] making medical records as vulnerable as any other data. Public outcry over these revelations point to the need for more transparency about how personal data – including data related to health – are collected and used. Without this transparency, policy cannot address how to balance privacy and other needs and values.

Additional privacy threats are specific to health care. People have little choice but to reveal intimate information if they want quality health care. Collecting and storing that information is legally mandated, making health data different from most other data.

[8] Christopher S. Tang & Joshua Zimmerman, *Information and Communication Technology for Managing Supply Chain Risks: How to Encourage Ethical Behavior Among All Links in a Global Supply Chain*, 56 COMMUNICATIONS OF THE ACM 27, p. 28 (2013).

[9]

[10] Glenn Greenwald, *Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security*, GUARDIAN WEEKLY, 5 September 2013. 2013, *available at* http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security (last visited September 10, 2013).

It is both information that people would likely want to keep private, but that they must disclose, and that is required to be recorded and stored for future use. Therefore, throughout the world, health data is given special protection and clinicians' duty to confidentiality is recognized. Yet, as electronic records proliferate, medical information is collected and transmitted on a scale impossible with paper records. Health-related information is electronically communicated between clinicians, insurers, and patients via health care delivery enterprise systems, health information networks, electronic mail, smartphones, personal health records, medical devices and sensors, and other electronic and internet services. As technology advances, the potential for privacy protection through technological approaches also advances, but keeping up with risks so as to prevent privacy violations simultaneously becomes more difficult.

Public confidence is undermined when data collected for one purpose is used for another, especially if these uses are not well-known or used for decision making about the individual.[11] Law cannot anticipate novel ways to aggregate and manipulate large volumes of data, nor can public expectations keep up with technological innovations. New technologies and new data uses create new risks that are not well addressed by current laws and policies.

Privacy scholars identify tensions between privacy and a variety of some other concern, including security, antidiscrimination, gender equality, innovation, accountability, consent, and notice.[12] Health care brings additional considerations into

[11] Koontz, What Is Privacy? 2013.; Deven McGraw, *Building Public Trust in Uses of Health Insurance Portability and Accountability Act De-identified Data*, 20 JAMIA (JOURNAL OF THE AMERICAN MEDICAL INFORMATICS ASSOCIATION) 29(2013).

[12] Ariel Porat & Lior Strahilevitz, *Personalizing Default Rules and Disclosure with Big Data,*, 112 MICHIGAN LAW REVIEW p. 45 forthcoming(2014).; The Elon University School of Law Fall 2010 Symposium was entitled "Transparency, Secrecy, and the Internet: Striking a Balance between the Ideals of

play. Considering only tensions between privacy and one seemingly competing need precludes thorough analysis and judicious balancing among competing values and social goods. Because of its sensitive nature, separate laws and regulations govern privacy risks of medical records. Privacy of health-related information seems deceptively simple, yet involves many converging issues. What constitutes "privacy," and how it is defined legally and thought of socially is complex enough. Also complex is how "public good" is construed when weighed against privacy. For health data, add to that how to balance privacy with numerous uses for the data: for individual patient care; for public health, research, and biosurveillance; for reimbursement; for insurance; for access to health care; for marketing of health-related products, medications, and devices; for monitoring individual health; and for monitoring the functioning of medical devices. Further complicating health data privacy is how it relates to norms involving professional practice, privilege, autonomy, paternalism, and protected communication.[13]

Both US law and EU data protection policies make special note of health information. The European Union takes a comprehensive general approach to privacy, reflected in the 1995 Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.[14] Unlike in

---

Privacy and Accountability in the Digital Age." One of the goals was "to explore… how society balances the desire for increased access to information with the need for secrecy, privacy, and control." http://www.elon.edu/e-web/law/law_review/symposia.xhtml, (last visited January 18, 2014). The Elon Law Review, Vol. 3, No. 2, February 2012 included papers from the panel on "Data, Transparency and Accountability" as well as papers from other panels. http://www.elon.edu/docs/e-web/law/law_review/Elon%20Law%20Review_Fall%202010%20Symposium_Panel%20Descriptions.pdf , (last visited January 18, 2014); Koontz, What Is Privacy? 2013.

[13] Bonnie Kaplan, *Selling Health Data: De-Identification, Privacy, and Speech*, CAMBRIDGE QUARTERLY OF HEALTHCARE ETHICS (in press);Bonnie Kaplan, *How Should Health Data Be Used? Privacy, Secondary Use, and Big Data Sales*, CAMBRIDGE QUARTERLY OF HEALTHCARE ETHICS (in review).

[14] European Union, *EU Directive 95/46/EC - The Data Protection Directive available at* http://www.dataprotection.ie/docs/EU-Directive-95-46-EC--Chapter-2/93.htm (last visited March 23, 2014); European Union, *The European Data Protection Supervisor*, *available at* http://europa.eu/about-

European countries where the EU Data Protection Directive takes an expansive view of privacy, in the US, there is no omnibus privacy law. Laws addressing health data privacy have developed in separate legal domains. Privacy, too, is affected by governance related to property and ownership (as in identity *theft*), speech, research, public health, and law enforcement. Protections in one domain are undercut by requirements in another. Different governmental units and jurisdictions regulate different aspects of health data collection, use, and privacy. Fragmentation and siloing makes it difficult to understand the entire realm of health data regulation and know which domain applies to which data or data use. Expertise is required for even partial understanding. A past Director of the Office of Information Management of the US Government Accountability Office, who advises the Chief Privacy Officer of the Office of the National Coordinator for Health Information Technology (ONC), considers that "*health information privacy is incredibly complex* and challenging [emphasis in original]."[15] Law, regulation, and common practice are confusing and popularly misunderstood. Legal tools are insufficient, conflicting, lack transparency, and do not take account of new developments. Health data vulnerabilities point to the need for greater privacy protection of personal medical information. Law, policies, and practices need to newly balance values of privacy, personal and public health, research, professionalism, free speech, and national security.

---

eu/institutions-bodies/edps/index_en.htm (last visited March 23, 2014) maintained or enhanced in European Union, *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52012PC0011:en:NOT (last visited March 23, 2014).

[15] Koontz, What Is Privacy? pp. iii, xi 2013.

Common misconceptions about what is protected and what is permissible make it difficult for law adequately to address health data privacy. Confusion and lack of transparency both highlight and obscure the need for new policy or law. They thwart democratic deliberation and the making of wise policy. "Patients should not be surprised to learn what happens to their health information," according to the subcommittee of the Health Information Technology Policy Committee that advises the ONC,[16] yet data may be made available outside of a patient's or clinician's expectations, further making informed policy and individual consent problematic.

Piecemeal legislation and balkanization reduces transparency, exacerbates confusion and opaqueness, and creates barriers to public knowledge of what the law is and how to interpret requirements correctly. This, in turn, interferes with patients' ability to give *informed* consent for how their personal and sensitive health information is used. Approximately half of the thousand patients surveyed nationally at the end of 2011 were concerned about privacy and security, whether or not their doctors used electronic health records.[17] It also undercuts comprehensive understanding of the regulatory landscape by those responsible for creating or enforcing it. Legislators and regulators are patients, too.

The combination of various values, norms, and legal tools that constitute the health data privacy mix are little discussed. Often, others' proposals address privacy and one other aspect, generally consent and notice. Thoughtful as these proposals are, a broader holistic approach is needed -- one that goes beyond others' calls to take account

[16] Id. at, 1-20.
[17] Jessica S Ancker, et al., *Consumer Experience With and Attitudes Toward Health Information Technology: A Nationwide Survey*, 20 JAMIA (JOURNAL OF THE AMERICAN MEDICAL INFORMATICS ASSOCIATION) 152(2013).

of Fair Information Practice Principles underlying both US law and the EU Data Protection Directive[18] -- to protect privacy in ways consistent with other legal rights and societal values that come into play when considering health data privacy. New thinking, based on transparency and democratic deliberation, is needed to replace the fragmented approach that creates legal mazes, unintended consequences, and reflects the complexity of health and health care.

This review makes three contributions. First, it addresses multiple issues and regulatory domains. Second, it therefore begins to describe a fuller legal landscape than the usual focus on one specific issue. Lastly, it takes a more patient-centric approach because more serious consideration of how to weigh conflicting needs, values, and theories is difficult without public, and hence legislative and regulatory, understanding. Data privacy threats and solutions come from both the public and private sectors.

In Section II, I discuss US public sector law and privacy risks inherent in the many requirements, exceptions, and exclusions, and reliance on de-identification (or anonymization) that characterizes US and other countries' law. I focus on The Health Insurance Portability and Accountability Act (HIPAA), The Health Information Technology for Economic and Clinical Health (HITECH) Act, and the Patient Protection and Affordable Care Act (ACA). The multiplicity of laws and regulations makes it extremely difficult for non-specialists in this area of law to understand what is and is not to be kept confidential when. Neither transparency nor consistency is served. Section III provides a range of private sector developments, including threats and ways to mitigate

[18] Koontz, What Is Privacy? 2013;Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA LAW REVIEW 1701 pp. 1734-1735 (2010);McGraw, JAMIA (JOURNAL OF THE AMERICAN MEDICAL INFORMATICS ASSOCIATION), (2013).

them associated with new technologies and big data. Section IV discusses proposals to balance privacy and other values with data access needs for public and commercial purposes. I address data aggregation and ownership, data as speech and free speech, and informed consent, all related to health data privacy. Though each has been thought a potential solution, none alone is adequate. Thus, throughout I delineate a multiplicity of health data privacy tools and risks in different domains, and some legal and technological approaches towards privacy protection. Different values and legal considerations are discussed here together, instead of of focusing on privacy and only one or two other concerns, so that a more integrated and holistic approach may be developed.

Although the US is unusual in the mix of legal and social issues that come into play, considering the many different facets, both separately and together, can help illuminate more general significant issues. Different theory and justifications govern each domain, and viewing the issues through these different approaches can help highlight needed considerations both in the US and elsewhere. Considering how issues are framed from one domain to another, while sometimes illuminating, also can add to opaqueness, or worse, conflicting regulation.

Section V describes transparency, harmonization, and simplication needed so that patients, and then, in turn, policy makers and, where necessary, courts, can make wiser, more democratically based decisions. In light of rapidly changing technological and societal norms, principles may serve better than rigid rules.

I conclude that the public nor policy makers should be more aware of risks and possible ways to mitigate them through technological and legal developments and social

research. They also should be more aware of the current precarious balance of the variety of laws, regulations, public perceptions, and social values. Lack of awareness and transparency contribute to making current approaches and proposals neither sufficiently protective against privacy threats nor allow for beneficial uses of health-related data. In the current environment, patients, clinicians, insurers, hospitals, and other organizations have interests in controlling their data.[19] The combination of public concern, privacy laws, and economic interests in limiting data access and aggregation are a toxic combination that prevent integrating patient information and combining data to produce new value. Perversely, they also insufficiently protect both clinicians and patients.

II. Clinical Health Data Privacy Protection and Risks in the US Public Sector

Health data universally is seen to require special protection in order to maintain trust between clinician and patient in the interest of both social and public order as well as better care for the patient. Nowhere can this private data rightly be passed to a third party without the patient's permission. A patient's rights to confidentiality is recognized in all countries, but in ways that differ from place to place.[20]

In the United States, multiple laws govern health data privacy. The US Department of Health and Human Services recognized the need to "establish a single, consistent approach to address the privacy and security challenges related to electronic health information exchange through a network for all persons, regardless of the legal framework that may apply to a particular organization" in their 2008 Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health

[19] Mark A. Hall & Kevin A. Schulman, *Ownership of Medical Information*, 301 JAMA 1282(2009).
[20] TIMOTHY STOLTFUS JOST, READINGS IN COMPARATIVE HEALTH LAW AND BIOETHICS (Carolina Academic Press 2 ed. 2007).

Information.[21] Though specific to an information network, the point applies to the broader mix of federal laws, which, together with state laws, are rife with gaps and exceptions that vary with jurisdiction, intended use of data, and intended user. Such a hodge-podge increases risks and decreases transparency. Ironically, the Framework includes openness and transparency as one of its principles.[22]

I describe three primary laws that govern health data in clinical care. Data as part of clinical care and data from medical research and are governed differently. While research data governance is beyond the scope of this paper, the division creates frictions between regulations and hidden costs for research.[23] Separating research and clinical care data governance also adds to confusion. There is no clear division between the research and clinical aspects of treating a patient for conditions subject to research protocols. Neither treatment nor disease, and hence, data, divides so conveniently into these categories of "clinical" and "research."[24] Similarly, there is long-standing difficulty in distinguishing between public health practice and public health research, especially as it applies to individual data privacy and use.[25] These distinctions are expected to overlap in the environment enabled by health information technology.[26] Hence, the Institute of

[21] Department of Health and Human Services United States Government, Office of the National Coordinator, healthIT.gov, *Nationwide Privacy and Security Framework for Electronic Exchange*, *available at* http://www.healthit.gov/policy-researchers-implementers/nationwide-privacy-and-security-framework-electronic-exchange (last visited January 22, 2014).
[22] Department of Health and Human Services United States Government, Office of the National Coordinator, Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information pp. 2, 7(2008), *available at* http://www.healthit.gov/sites/default/files/nationwide-ps-framework-5.pdf (last visited January 22, 2014).
[23] Jane R. Bambauer, *Is Data Speech?*, 66 STANFORD LAW REVIEW 57 pp. 96, 114 (2014).
[24] Bonnie Kaplan, et al., Data Governance Dilemmas for Research and Clinical Care (American Medical Informatics Association ed., Annual Symposium Proceedings 2014).
[25] Barbara J. Evans, *Much Ado About Data Ownership*, 25 HARVARD JOURNAL OF LAW & TECHNOLOGY 70(2011).
[26] Melissa M. Goldstein, *Health Information Technology and the Idea of Informed Consent*, 38 JOURNAL OF LAW, MEDICINE AND ETHICS 27, p. 34 (2010).

Medicine has called for revising privacy rules to better enable research based on clinical data.[27]

A. The Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is widely believed to protect patient privacy. The HIPAA Privacy Rule set national standards for the first time that specified who is covered, what information is protected, and how protected health information can be used and disclosed.[28] According to the Department of Health and Human Services, the law is intended to protect individuals' health information while providing for sharing that information to ensure quality care. Examining HIPAA highlights a need to revisit this sort of legislation.[29]

Contrary to a common public perception that current laws and regulation protect health information privacy, HIPAA anecdotally is well-known among health care professionals to have little such privacy effect, and patients experience health care workers' creative variety in interpreting HIPAA requirements. Consensus in the heath care industry is that HIPAA has not been rigorously enforced.[30] The result: people who need the information cannot get it,[31] and others have access without patients' knowledge. The Institute of Medicine's Committee on Health Research and the Privacy of Health Information concluded "that the HIPAA Privacy Rule does not protect privacy as well as

[27] INSTITUTE OF MEDICINE, BEYOND THE HIPAA PRIVACY RULE: ENHANCING PRIVACY, IMPROVING HEALTH THROUGH RESEARCH (National Academies. 2009). Report Brief available at http://www.iom.edu/~/media/Files/Report%20Files/2009/Beyond-the-HIPAA-Privacy-Rule-Enhancing-Privacy-Improving-Health-Through-Research/HIPAA%20report%20brief%20FINAL.pdf.

[28] Department of Health and Human Services United States Government, Office for Civil Rights, *Summary of the HIPAA Privacy Rule*, *available at* http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/ (last visited June 30, 2013).

[29] Kaplan, CAMBRIDGE QUARTERLY OF HEALTHCARE ETHICS, (in press).

[30] Carlos Levya & Deborah Levya, *HITECH Act Summary*, *available at* http://www.hipaasurvivalguide.com/hitech-act-summary.php (last visited May 19, 2014).

[31] Koontz, What Is Privacy? p. xi. 2013.

it should, … impedes important health research, … [and that] organizations that collect and use health data vary greatly in how they interpret and follow the rule, and the rule does not apply uniformly to all health research." Consequently, their 2009 report makes the case for new approaches for research data.[32] The same, of course, applies to clinical data.

HIPAA governs what is involved in de-identification, reuse, and consent or authorization, and what responsibilities are required of different organizations and agencies. De-identifying data is a key part of HIPAA protection, yet de-identification, on which both the EU and US privacy protection is based, is increasingly untenable for this purpose.[33] The HIPAA Privacy Rule also requires that the minimum amount of data needed be collected or disclosed, and that organizations develop means to determine what that minimum is. It also introduced the idea of individual consent, but constrains it to "as appropriate."[34] There are special considerations and privacy expectations where minors are concerned.[35]

With the exceptions and complexity, patients, and even clinicians, may have little idea of what becomes of patient data, or just what HIPAA covers and what it does not. Lack of legal accountability for unauthorized re-identification and poor public transparency about de-identified data uses feed the public's privacy concerns.[36]

[32] INSTITUTE OF MEDICINE, Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research. 2009. Available at http://www.iom.edu/Reports/2009/beyond-the-HIPAA-Privacy-Rule-Enhancing-Privacy-Improving-Health-Through-Research.aspx, (last visited January 22, 2014). See also the press release at http://www8.nationalacademies.org/onpinews/newsitem.aspx?RecordID=158, (last visited January 22, 2014).

[33] Kaplan, CAMBRIDGE QUARTERLY OF HEALTHCARE ETHICS, (in press).

[34] Koontz, What Is Privacy? 2013.

[35] Fabienne C. Bourgeois, et al., *Whose Personal Control? Creating Private, Personally Controlled Health Records for Pediatric and Adolescent Patients*, 15 JAMIA (JOURNAL OF THE AMERICAN MEDICAL INFORMATICS ASSOCIATION) 737(2008).

[36] McGraw, JAMIA (JOURNAL OF THE AMERICAN MEDICAL INFORMATICS ASSOCIATION), (2013).

1. Legal Framework

Traditionally, doctor-patient confidentiality protected patient privacy. It was part of the original Hippocratic Oath, and further developed in the common law tort system, allowing for flexibility in interpretation on a case-by-base basis and for overriding in the public interest.[37] HIPAA, instead, takes a rule-based approach and attempts to anticipate disclosures needed for public policy and set rigid restrictions on other disclosures.[38] It is based on Fair Information Practices (FIPs).[39] FIPs also are the foundation for privacy laws and related policies in the European Union and in other countries, including Australia and New Zealand.[40] The FIPs are meant to maintain the same level of privacy when using information technology as when not.[41] The 2008 Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information, published by the US Department of Health and Human Services embodies many of the Organisation for Economic Cooperation and Development's FIPs, but it elevated individual choice and consent to a principle and gave greater emphasis to accountability and breach reporting.[42] This Framework, however, is not meant for

[37] The original oath includes: "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." This was changed in the modern version to be: "I will respect the privacy of my patients, for their problems are not disclosed to me that the world may know." http://www.pbs.org/wgbh/nova/body/hippocratic-oath-today.html, (last visited February 3, 2013; Bambauer, STANFORD LAW REVIEW, p. 114 (2014).

[38] Goldstein, JOURNAL OF LAW, MEDICINE AND ETHICS, p. 28 (2010).; Bambauer, STANFORD LAW REVIEW, p. 114 (2014).

[39] United States Government, Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information p. 3 2008.

[40] Koontz, What Is Privacy? 2013; United States Government, Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information p. 3 2008.

[41] Kelly Caine & Rima Hanania, *Patients Want Granular Privacy Control over Health Information in Electronic Medical Records*, 20 JAMIA (JOURNAL OF THE AMERICAN MEDICAL INFORMATICS ASSOCIATION) 7, p. 7 (2013).

[42] Koontz, What Is Privacy? 2013.

individuals with respect to their own individually identifiable information, but applies to health care-related individuals and organizations exchanging personally identifiable information.[43] Even so, the FIPs are broadly applicable. They inform other US and international privacy law, have been adapted by other agencies, and can serve as a good check-list to holistically assess privacy.[44]

2. De-Identification

Health and medical data is needed for research, public health, monitoring adverse reactions and safety of new pharmaceuticals and devices, and biosurveillance for tracking disease trends and possible bioterrorism. Most, but not all, of these purposes can be served by de-identified (data that has information that could identify an individual removed) aggregated data.

HIPAA specifies methods for de-identifying data to protect privacy. The most widely used de-identification method is to strip data of a pre-defined set of "identifiers" thought to indicate which individual is connected to that data. The standards have long been controversial and various organizations and task forces have issued recommendations for change.[45] The list of identifiers enumerated in the HIPAA Privacy

[43] United States Government, Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information p. 6 2008.

[44] Koontz, What Is Privacy? 2013.; The principles cover individual access, correction, and choice; openness and transparency; limitation on collection, use, and disclosure; data quality and integrity; safeguards; accountability, according to United States Government, Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information pp. 6-10 2008.

[45] McGraw, JAMIA (JOURNAL OF THE AMERICAN MEDICAL INFORMATICS ASSOCIATION), (2013) reports on a 2011 workshop of stakeholders convened by The Center for Democracy & Technology to explore policy ideas for HIPAA de-identification. INSTITUTE OF MEDICINE, Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research. 2009.

Rule is based on the assumption that other data in a health record will not contribute to re-identification, even though it may when combined with rich outside information.[46]

Current de-identification methods are problematic. It is not clear that even stripping identifiers, as mandated by HIPAA, is sufficient to protect individual data or prevent uses individuals may experience as privacy violations or misuse of their data.[47] Whether this stripping of identifiers actually de-identifies health records is at question. It has been possible to re-identify enough HIPAA de-identified records that concerns remain.[48] These concerns are increasing, even though recent studies indicate that there is not as much chance of re-identification of properly de-identified data as feared.[49] Nevertheless, the new computer science specialty of re-identification science casts doubt on how effective de-identification is and requires reconsidering it as a basis for privacy protection law. Both US federal privacy statutes and the EU Data Protection Directive rely on de-identification for privacy protection. As Paul Ohm points out:

> In addition to HIPAA and the EU Data Protection Directive, *almost every single privacy statute and regulation ever written* in the U.S. and the EU embraces—implicitly or explicitly, pervasively or only incidentally—the assumption that anonymization protects privacy, most often by extending safe harbors from penalty to those who anonymize their data.[50] (emphasis added)

[46] Ohm, UCLA LAW REVIEW, pp. 1738,1740 (2010).
[47] Kaplan, CAMBRIDGE QUARTERLY OF HEALTHCARE ETHICS, (in press).
[48] Gregory D. Curfman, et al., *Prescriptions, Privacy, and the First Amendment*, 364 NEW ENGLAND JOURNAL OF MEDICINE 2053(2011);Lee Tien, Online Behavioral Tracking and the Identification of Internet Users (From Mad Men to Mad Bots: Advertising in the Digital Age, The Information Society Project at the Yale Law School, 2011), *available at* http://www.law.yale.edu/documents/pdf/ISP/Lee_Tien.pdf;Kathleen Benitez & Bradley A. Malin, *Evaluating Re-identification Risks with respect to the HIPAA Privacy Rule*, 17 JAMIA (JOURNAL OF THE AMERICAN MEDICAL INFORMATICS ASSOCIATION) 169(2010).
[49] McGraw, JAMIA (JOURNAL OF THE AMERICAN MEDICAL INFORMATICS ASSOCIATION), (2013).
[50] Ohm, UCLA LAW REVIEW, p. 1740 (2010).

He argues that it no longer is sufficient to view whether particular data fields are identifiable. Technological developments and re-identification science techniques that combine previously separate databases undermine this assumption, making HIPAA insufficient and the EU Data Protection Directive overbroad because "*any* element can be identifying in combination with others;" re-identification will win out in the race with de-identification.[51]

Regardless, once de-identified, HIPAA regulation no longer applies;[52] the data can be used for multiple purposes, including combining it with other data that may enable individuals to be identified. De-identification, too, applies only to patients, not to providers. Provider data is not privacy protected.[53]

Further, data sometimes needs to be identified, as, for example, when combining medical records for one individual treated in different locations, or to monitor dispensing of controlled substances to particular individuals. Meeting these different requirements without diminishing the value of both privacy and data collection is difficult.

3. Entities Covered and Exempt

HIPAA governs health care providers, health care plans and health insurance companies, and health care clearing houses that process health information received from other entities. However, providers like hospitals or pharmacies, are able to share identifiable information without patient authorization for treatment, billing, audit, and

[51] Id. at, p. 1761, p. 1741, n. 213 quoting Arvind Narayanan & Vitaly Shmatikov, De-Anonymizing Social Networks, http://userweb.cs.utexas.edu/~shmat/shmat_oak09.pdf, p. 1752 (emphasis added), p. 1741, n. 213 quoting Arvind Narayanan & Vitaly Shmatikov, *De-Anonymizing Social Networks*, http://userweb.cs.utexas.edu/~shmat/shmat_oak09.pdf, p. 1752

[52] McGraw, JAMIA (JOURNAL OF THE AMERICAN MEDICAL INFORMATICS ASSOCIATION), (2013).

[53] Carolyn Petersen, et al., *Sorrell v. IMS Health: Issues and Opportunities for Informaticians*, 20 JAMIA (JOURNAL OF THE AMERICAN MEDICAL INFORMATICS ASSOCIATION) 35(2013).

organ donation,[54] Therefore, while HIPAA generally applies to disclosures that one's health care provider may make, patients may not realize that it does not govern an employee's disclosures of health information an employer uses to administer sick leave, workers' compensation, wellness programs, or health insurance. These are not protected.[55] Also, HIPAA regulates only "covered entities" and their "business associates." Life and disability insurance companies, health-related web sites, social media, people who do blood pressure or other screenings at public places, welfare agencies, and mobile phone apps are among the entities not covered by HIPAA.[56] New and emerging organizations and actors are not ennumerated in HIPAA, so not covered.[57] HIPAA is based on the presumption that data is exchanged between one provider and another, between patient and one clinician, or among two parties to a contract; it is not well-suited to team-based care or distributed data-sharing networks.[58] Moreover, HIPAA

[54] See definitions of "business associate" and "covered entity" at 45 CFR 160.103; LifeNet Health Transplant Services Division, *HIPAA Provisions*, *available at* http://lifenethealthopo.org/healthcare_professionals/hipaa_provisions (last visited July 30, 2014).

[55] Department of Health and Human Services United States Government, Office for Civil Rights, *Health Information Privacy: Employers and Health Information in the Workplace*, *available at* http://www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/employers.html (last visited September 24, 2013).

[56] Privacy Rights Clearing House, *Fact Sheet 8a: HIPAA Basics: Medical Privacy in the Electronic Age*, *available at* https://www.privacyrights.org/fs/fs8a-hipaa.htm#3 (last visited September 24, 2013);Privacy Rights Clearing House, *Mobile Health and Fitness Apps: What Are the Privacy Risks?*, *available at* https://www.privacyrights.org/fs/fs39/mobile-apps (last visited September 24, 2013). The HITECH Act strengthened HIPAA protection by increasing penalties for business associates' violations and providing some additional options for patient choice, see Department of Health and Human Services United States Government, Press Office, *New Rule Protects Patient Privacy, Secures Health Information*(January 17, 2013), *available at* http://www.hhs.gov/news/press/2013pres/01/20130117b.html (last visited Septembe 24, 2014).

[57] Deven McGraw, *Privacy and Information Technology*(2009), *available at* http://www.law.georgetown.edu/oneillinstitute/research/legal-solutions-in-health-reform/Privacy.cfm Also available at http://scholarship.law.georgetown.edu/ois_papers/25, accessed July 17, 2014 (last visited Paper 25).

[58] Mark A. Rothstein, *The Hippocratic Bargain and Health Information Technology*, JOURNAL OF LAW, MEDICINE AND ETHICS 7(2010); Michael D. Greenberg, et al., *Crossed Wires: How Yesterday's Privacy Rules Might Undercut Tomorrow's Nationwide Health Information Network*, 28 HEALTH AFFAIRS 450(2009).

requirements are confusing, and clinicians may not be willing to share patient information for treatment, payment, and operations without patient authorization, though allowed by HIPAA.[59]

Neither government agencies, like the Centers for Medicare and Medicaid Services (CMS), nor state agencies are required to de-identify data. States may sell large volumes of hospital discharge data. Consequently, they collect and may provide identifiable data to those with a clear interest in not protecting privacy, albeit, as required by HIPAA, there is an understanding that they will do so. Secondary use of this data is common.

4. Secondary Use

"Secondary use" refers to taking advantage of existing data for purposes other than why it was collected. HIPAA permits secondary uses of data for research, public health, law enforcement, judicial proceedings, and other "public interest and benefit activities," without individual authorization.[60] For example, the Food and Drug Administration launched the Sentinel Initiative in 2008 to "complement existing systems that the Agency has in place to track reports of adverse events linked to the use of its regulated products" by accessing data routinely collected in electronic health record systems, administrative and insurance claims databases, and registries, "within pre-established privacy and security safeguards." These safeguards include eliminating direct identifiers "*whenever possible"*[emphasis added].[61]

[59] Susan D. Hosek & Susan G. Straus, Patient Privacy, Consent, and Identity Management in Health Information Exchange: Issues for the Military Health System, 3 RAND HEALTH QUARTERLY 9(Summer, 2013).

[60] See section on "Permitted Uses and Disclosures."

[61] Department of Health and Human Services United States Government, Office for Civil Rights, *Summary of the HIPAA Privacy Rule*, *available at* http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/

HIPAA thus allows disclosure for public health purposes. The usual consent and authorization processes also are not necessary for judicial or law enforcement purposes. HIPAA does not protect medical records from the National Security Agency and other intelligence activities.[62]

5. Research

Different de-identification requirements govern secondary use for research. Patients are supposed to give or withhold permission for their health records to be used for research, and researchers are supposed to strip what HIPAA specifies as identifying information when aggregating such data for analysis. Nevertheless, patients may not be asked their preferences about research uses of their data, especially if their permission is not required. Consent, therefore, becomes an issue.

HIPAA does not require patient consent to use de-identified patient information. In general, this also applies to research uses. However, de-identification is not required for research if an Institutional Review Board authorizes a waiver. Data collected specifically as part of research projects is governed by other laws which can be difficult to reconcile with HIPAA.[63]

(last visited June 30, 2013); Food and Drug Administration United States Government, *FDA's Sentinel Initiative*, *available at* http://www.fda.gov/Safety/FDAsSentinelInitiative/default.htm (last visited Food and Drug Administration United States Government, *Mini-Sentinel: About Us*, *available at* http://www.mini-sentinel.org/about_us/ (last visited January 18, 2014), emphasis added.

[62] Evans, HARVARD JOURNAL OF LAW & TECHNOLOGY, p. 82 (2011);Qmed Staff, *HIPAA vs. The NSA: Who Wins When Medical Devices Are Concerned?*(August 26, 2013), *available at* http://www.qmed.com/news/hipaa-vs-nsa-who-wins-when-medical-devices-are-concerned (last visited September 10, 2013).

[63] Evans, HARVARD JOURNAL OF LAW & TECHNOLOGY, p. 83 (2011). Research is governed by The Federal Policy for the Protection of Human Subjects (the "Common Rule"), the U.S. Food and Drug Administration (FDA)'s framework of human-subject protections. States, too, may require additional privacy and human-subject protections on research within their jurisdictions. Laura A. Mamo, et al., Patient Informed Governance of Distributed Research Networks: Results and Discussion from Six Patient Focus Groups (American Medical Informatics Association ed., Annual Symposium Proceedings 2013), available at http://knowledge.amia.org/amia-55142-a2013c-1.429499/annual2013-1.434519/f-001-1.434520/a-326-

The Privacy Rule distinguishes between informed consent, as required for human subject research, and patient authorization of disclosure of protected health information for research purposes.[64] Differences and compatibilities between "consent" and "authorization" can be opaque to patients, especially when different agencies and organizations use these terms differently,[65] and clinicians may find it difficult to divide clearly data related to care and to research. Confounding of "care" and "research" also is exacerbated by the movement towards a continually learning health care system, in which data from electronic patient records is analyzed as research data useful to improve quality of healthcare.[66] Privacy advocates, researchers, and public health officials thus may disagree about appropriate data uses. In the UK, for example, the National Health Service (NHS) has a mass database of citizens' health information. Together with a Wellcome Trust-lead coalition of leading medical research organizations, they oppose the EU's move towards greater health data protection that would make it illegal.[67] The database could be tremendously useful for public health, outcomes research, and patient safety. The care.data database was created, according to NHS England to improve NHS services and to "drive economic growth by making England the default location for

1.432775/ap-431-1.435247?qr=1, (last visited January 30, 2014); A press release about the INSTITUTE OF MEDICINE, Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research. 2009 stated: "…the HIPAA Privacy Rule is difficult to reconcile with other federal regulations governing research involving people and their personally identifiable information."(National Academies, HIPAA Privacy Rule Fails to Adequately Protect Patient Privacy and Hampers Health Research; A New Approach to Privacy Protection Is Needed in Research (February 4, 2009) available at http://www8.nationalacademies.org/onpinews/newsitem.aspx?RecordID=12458, (last visited January 22, 2014)).

[64] http://www.hhs.gov/hipaafaq/permitted/research/313.html, (last visited January 19, 2014).

[65] Goldstein, JOURNAL OF LAW, MEDICINE AND ETHICS, p. 31 (2010)..

[66] Kaplan, et al., Data Governance Dilemmas for Research and Clinical Care. 2014 forthcoming;Institute of Medicine, Best Care at Lower Cost: The Path to Continuously Learning Health Care in America: Recommendations. (2012), *available at* http://www.iom.edu/~/media/Files/Report%20Files/2012/Best-Care/Best%20Care%20at%20Lower%20Cost_Recs.pdf (last visited July 14, 2014).

[67]

world-class health services research."[68] The database also provokes privacy concerns, which delayed plans to include, for the first time, records from primary care practices.[69] Insurers, pharmaceutical companies, and other private commercial enterprises will receive "pseudoanonymized" records that the NHS claims "will not contain information that identifies you," but that instead include NHS numbers, date of birth, postcode, ethnicity and gender.[70] Individuals can opt-out of the new care.data program, but other rules allow greater third-party access to other NHS databases.[71]

Exacerbating the lack of clarity is that law may require protecting some data and disclosing other data. Federal and state regulation imposes more stringent protection than required by HIPAA for some sensitive data. Federal regulation requires consent to disclose substance and alcohol abuse information collected by federally assisted alcohol and drug abuse programs, and some states also require consent to disclose HIV/AIDS and mental health information.[72] On the other hand, identifiable data is required for vital statistics (such as births, deaths, and causes of death), controlled substance prescriptions, tumor registries, and reports of animal bites (because of the threat of rabies), gun shot

---

[68] *Your Records: Better Information Means Better Care*, *available at* http://www.nhs.uk/nhsengland/thenhs/records/healthrecords/pages/care-data.aspx (last visited July 24, 2014);Randeep Ramesh, *NHS Patient Data to Be Made Available for Sale to Drug and Insurance Firms*, THE GUARDIAN, January 19, 2014, *available at* http://www.theguardian.com/society/2014/jan/19/nhs-patient-data-available-companies-buy (last visited July 24, 2014).

[69] Laura Donnelly, *Hospital Records of All NHS Patients Sold to Insurers*, THE TELEGRAPH, February 23, 2014, *available at* http://www.telegraph.co.uk/health/healthnews/10656893/Hospital-records-of-all-NHS-patients-sold-to-insurers.html (last visited July 24, 2014).

[70] Your Records: Better Information Means Better Care.

[71] Donnelly, THE TELEGRAPH, February 23, 2014.

[72] Confidentiality of Alcohol and Drug Abuse Patient Records, 2000; NORC, Evaluation of the State Health Information Exchange Cooperative Agreement Program: Early Findings from a Review of Twenty-Seven States, January 2012,NORC, University of Chicago, Contract Number: HHSP2337010T/OS33547 prepared for The Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services, Washington, D.C., p. 19. Available at http://www.healthit.gov/sites/default/files/pdf/state-health-info-exchange-coop-program-evaluation.pdf, (last visited January 19, 2014).

wounds, drunk driving, and sexually transmitted diseases. Individuals may be required by law to disclose personal health information for such purposes as attending school or obtaining licenses for marriage, gun purchases, and driving. The public generally is not aware of what becomes of this data or to what uses it may be put.

B. The Health Information Technology for Economic and Clinical Health (HITECH) Act

A subsequent law, The Health Information Technology for Economic and Clinical Health, or HITECH, Act of 2009, part of the American Recovery and Reinvestment Act of 2009 (ARRA), affects health data privacy as well. It mandated, first incentives, and later penalties, to promote electronic medical record adoption by clinicians and organizations treating Medicare patients. Not surprisingly, electronic health and medical records are becoming more common, as are their benefits and risks.

Sharing individual patient data among everyone involved in that patient's care is one of the many benefits of electronic medical record (EMR) adoption. Vendors of these systems are understood to be business associates of covered entities under HIPAA.[73] The law did not require that funded systems be interoperable so as to enable interconnecting of records for an individual patient. However, a provision for exceptions to restrictions on remuneration for health data lays groundwork that can create incentives to facilitate commercial data sharing for research and for public health.[74]

The law also mandated electronic prescribing and the development of state Health Information Exchanges (HIE), ultimately intended to be linked into a national health

[73] Levya & Levya, HITECH Act Summary.
[74] Evans, HARVARD JOURNAL OF LAW & TECHNOLOGY, pp. 108-109 (2011).

information network (NHIN) so that each person's medical data and history theoretically will be available at the point of care when needed, as well as for research and biosurveillance. ONC recognizes that HIEs create an environment that HIPAA was not meant to address. The 2008 ONC National Privacy and Security Framework was intended to address this by articulating clear uniform principles for a consistent approach to privacy and security.[75]

States need approval for their HIE plans in order to receive funding from ONC.[76] These plans include policy on data sharing, data privacy, data access privileges, and similar concerns. As with HIPAA, HIE policies are difficult to unravel; determining what is protected data and what is not is a challenge, as is finding a state's policy clearly articulated in one easily accessible document. The Health Information Security and Privacy Collaboration (HISPC), established in 2006 by the Department of Health and Human Services, completed the last of its phases in 2008. HISPC highlighted different state policies and developed toolkits for harmonizing them.[77]

The need for simplicity remains. HIE policies differ by state. However, all reflect the growing consensus in the US and abroad that patients should decide when and with whom to share health data. In some states, patients may opt in and in other states, they may opt out; some states have a hybrid model and some allow the partners involved to determine their own consent model; some states require permission for sharing some

[75] United States Government, Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information pp. 3, 1 2008.
[76] The HITECH Act strengthened HIPAA protection by increasing penalties for business associates' violations and providing some additional options for patient choice. See United States Government, New Rule Protects Patient Privacy, Secures Health Information. January 17, 2013.
[77] United States Government, Federal-State Privacy & Security Collaboration (HISPC);United States Government, Health Information Security & Privacy Collaboration (HISPC).

data but not other data; while some do not require patient consent to be part of the HIE at all. A health care provider who accesses patient information from another state must adhere to the disclosure requirements of that state.[78] This can make it especially confusing for patients and clinicians near state borders, or patients who seek healthcare out-of-state. Data concerning a patient who is treated at a military, veterans, Indian Health Service, or county hospital and also treated at a non-government facility; or a patient treated in a foreign facility and also treated domestically; are subject to a multiplicity of policies. State policies govern only data in the HIE and do not necessarily concern patient permissions for sharing data within a clinical practice or hospital network, or permission to create electronic medical records.[79]

These different laws and policies may conflict and certainly confound; the multiplicity creates complexity and lack of transparency for both patients and providers.[80] Consequently, the US Department of Health and Human Services established the Health Information Security and Privacy Collaborative (HISPC) in 2006 to address the complex legalities of patient data privacy and harmonizing HIE data privacy regulation. HISPC divided their work into three phases, the first two of which involved summarizing the

[78] NORC, Evaluation of the State Health Information Exchange Cooperative Agreement Program: Early Findings from a Review of Twenty-Seven States, January 2012,NORC, University of Chicago, Contract Number: HHSP2337010T/OS33547 prepared for The Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services, Washington, D.C., p. 19. Available at http://www.healthit.gov/sites/default/files/pdf/state-health-info-exchange-coop-program-evaluation.pdf, (last visited January 19, 2014). Goldstein, JOURNAL OF LAW, MEDICINE AND ETHICS, p. 32, 34 (2010).;Hosek & Straus, RAND HEALTH QUARTERLY, (Summer, 2013).

[79] Goldstein, JOURNAL OF LAW, MEDICINE AND ETHICS, pp. 31-32 (2010).

[80] Mamo, et al., Patient Informed Governance of Distributed Research Networks: Results and Discussion from Six Patient Focus Groups. 2013; Frank Pasquale, *Grand Bargains for Big Data: The Emerging Law of Health Information*, 72 MARYLAND LAW REVIEW 682(2013); Department of Health and Human Services United States Government, Centers for Medicare & Medicaid Services, HealthCare.gov, *Who's Eligible to Use the Marketplace*, *available at* https://www.healthcare.gov/am-i-eligible-for-coverage-in-the-marketplace/ (last visited September 27, 2013).

legal landscape. Their final report, issued 2009, included tools summarizing data release requirements in different states and recommendations for standardized consent options. The HISPC website links to these reports and also to information for patients and families on privacy protection.[81] Whether patients and families know about this resource, or would find it adequately describes risks and benefits of data sharing, is an open question.[82] That clinicians and patients needed it at all suggests how opaque and inaccessible the information is.

C. Patient Protection and Affordable Care Act (ACA)

Despite considerable discussion of the Patient Protection and Affordable Care Act (ACA) of 2009, which mandates everyone have medical insurance or face tax penalties,[83] few are aware of the potential privacy risks in this law. To make insurance more readily available, Health Insurance Exchanges (HIX) (now also known as Health Insurance Marketplace) in participating states help insure those with limited income. The HIX Program includes state agencies administering Medicaid, Children's Health Insurance Program (CHIP) and the Basic Health Plan (BHP).

---

[81] Goldstein, JOURNAL OF LAW, MEDICINE AND ETHICS, p. 28 (2010); United States Government, Health Information Security & Privacy Collaboration (HISPC).

[82] For example, Jeanne McGee & Mark Evers, *Oregon HISPC Consumer Engagement Project," Oregon Health Information Security and Privacy Collaborative (HISPC)*(October, 2007), *available at* http://www.oregon.gov/oha/OHPR/hispc/docs/or_20hiconsumerengagementprojectfinalreportspc_20consumer_20project_20rpt_202007.pdf (last visited January 22, 2014) reports "People knew very little about the multiple ways in which their health information is now being stored and routinely shared, sometimes with their knowledge and permission and sometimes not." Ann F. Chou & Robn Green, Interstate Disclosure and Patient Consent Requirements: HISPC and Advancing E-Health (Health Information Security and Privacy Collaboration (HISPC) ed., National Conference March 5, 2009) *availble at* http://www.rti.org/files/hispc/OK_State_Pres.pdf lists "Lack of knowledge of HIPAA and other privacy and security laws" as a "barrier" to HIEs.

[83] 111th Congress Public Law 148, *available at* http://www.gpo.gov/fdsys/pkg/PLAW-111publ148/html/PLAW-111publ148.htm, (last visited January 30, 2014). A more user-friendly version is available at http://www.hhs.gov/healthcare/rights/law/, (last visited January 30, 2014).

No matter how people enroll, all applications ultimately go through a federal Data Services Hub that connects federal, state, and private data bases to determine eligibility. Eligibility depends on citizenship or immigration, residence, income, and incarceration status.[84] The Centers for Medicare and Medicaid Services (CMS) Data Services Hub involves data sharing agreements with the Internal Revenue Service (IRS), Social Security Administration (SSA), Department of Homeland Security (DHS), Department of Veterans Affairs (VA), Department of Defense (DoD), Peace Corps, and Office of Personnel Management (OPM) to validate eligibility for benefits.[85] Employment and income information is verified against IRS and SSA data.

The hub is hosted by the cloud service of Terremark Federal Group, a wholly-owned subsidiary of Verizon Communications Inc. In order to get more current information, verification will be supplemented by real-time, "instant" information about applicant's income supplied by another private service, Equifax Workforce Solutions, a wholly owned subsidiary of the credit bureau Equifax, Inc. Equifax data indicates whether the applicant has employer-sponsored coverage. Meanwhile, states with insurance exchanges are planning access to similar data using other private services in case of shutdowns in the federal/Equifax service. Provider and employer information is not protected. Employers are being pitched Equifax products and services.[86]

---

[84] United States Government, Who's Eligible to Use the Marketplace.
[85] 78 FR 49525, Number 25 (Wednesday, February 6, 2013), p. 8539, *available at* http://www.gpo.gov/fdsys/pkg/FR-2013-02-06/html/2013-02666.htm, (last visited September 9, 2013).
[86] [Joel S. Winston], *States' Hospital Data for Sale Puts Patient Privacy in Jeopardy*(June 7, 2013), *available at* https://www.annualmedicalreport.com/states-hospital-data-for-sale-puts-patient-privacy-in-jeopardy/ (last visited January 19, 2014).

The Data Services Hub will contain identifiable information about employers who want to provide insurance coverage for qualified employees through a Small Business Health Options Program (SHOP), and officers, and employees or contractors of the Exchange, CMS, and various organizations, agencies, and individuals involved with recruitment and enrollment.[87] Lack of transparency about the Data Services Hub creates suspicion; IRS linkages to individually identifiable medical data leads to concerns related to potentially targeting citizens for political reasons.[88] Intelligence services and law enforcement agencies, too, may well be interested in health data for foreigners being treated in the US, for US citizens being treated out of country, for telehealth services across national boundaries, and for other transmission of health or medical data as part of the widespread collection of telephone and internet records.[89] CMS already has a sophisticated data matching procedure for detecting fraud,[90] raising questions of why all the other agencies' data is needed again.

III. NEW TECHNOLOGIES, NEW RISKS, NEW SOLUTIONS

As new technologies develop, so do accompanying risks. But new technological developments also have potential for new approaches to risk mitigation. Big data is an example of each of these possibilities. More and more collection and aggregation of medical record information, together with growing sophistication of data storage and data

[87] 78 FR 49525, Number 25 (Wednesday, February 6, 2013), p. 8539, available at http://www.gpo.gov/fdsys/pkg/FR-2013-02-06/html/2013-02666.htm, (last visited September 9, 2013).
[88] Adrian Gropper, The Federal Health Data Services Hub Hubbub.;Gottlieb, FORBES. May 15, 2013
[89] Greenwald, GUARDIAN WEEKLY, 2013 revealed: how US and UK spy agencies defeat internet privacy and security. Guardian Weekly, 5 September 2013, available at , http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security, (last visited Sept 10, 2013).
[90] Pasquale, MARYLAND LAW REVIEW, (2013).

analysis techniques, provide new opportunities for privacy violation and for privacy protection. Data sets that were meant to be kept apart now easily are combined and used for re-identying individuals even if the original data was stripped of identifiers.[91] For other new technologies, it may be too soon to predict what threats and protections they portend. Considering technological protections illuminates tensions that they are intended to address. Technological approaches may enhance or obviate the need for legal tools that address these tensions, or point towards a combination of technological and legal remedies that both protect privacy and achieve other significant goals.

A. Big Data and Health Records

The mandated implementation of electronic medical records involves collecting data on a scale that is qualitatively different from paper records. This makes possible many potential beneficent uses of the data. Data sharing among health care providers, for research purposes, and for patient safety can improve quality of care. Increasingly sophisticated methods of data mining and analytics take advantage of large-scale data collection and aggregation, which may be distributed rather than stored in a centralized database. Data mining can help generate new knowledge. This development has led to promising research based on what has come to be called "big data."

Simultaneously, these advances also create new opportunities for nefarious data uses, both legal and illegal. Individuals concerned about the release of their data may withhold information that could benefit their care,[92] as well as skew the data on which quality improvements and research are based. Privacy risks are exacerbated by newer

[91] Ohm, UCLA LAW REVIEW, (2010).
[92] Petersen, et al., JAMIA (JOURNAL OF THE AMERICAN MEDICAL INFORMATICS ASSOCIATION), (2013).

technologies and the increased abilities to collect, aggregate, and mine data. On the other hand, research may be enhanced, but only if the data is sufficiently complete and reliable. Some examples follow.

1. Technological Protection: Personalized Granular Control, Strengthening De-Identification

Privacy enhancing technologies can counterbalance privacy erosions made easier by other technological advances. Just as medicine is becoming more personalized, posing threats to privacy if genomic, social, and behavioral data, as recommended by the Institute of Medicine,[93] is included in otherwise de-identifed records, it also is becoming possible to personalize privacy protections. Sequestering specified categories of health data (known as "segmenting," "separate management," "e-consent", or "sequestration"), as recommended by the National Center for Vital Health Statistics, and granular consent methods are in their infancy and face considerable obstacles.[94] Granular control would mark each data field to indicate whether it is sequestered or individual disclosure preferences, so computer programs can control release of data accordingly. External privacy threats have been more of a focus than patient preferences, yet patients may well prefer granular level control over their data, though they and their health care provider may find it burdensome to manage their consent data.[95]

---

[93] INSTITUTE OF MEDICINE, CAPTURING SOCIAL AND BEHAVIORAL DOMAINS IN ELECTRONIC HEALTH RECORDS: PHASE 1 (The National Academies Press. 2014). Summary of Selected Domains *available at* http://iom.edu/~/media/Files/Report%20Files/2014/EHR-Phase-1/EHRdomains.pdf, (last visited July 3, 2014).

[94] Rothstein, JOURNAL OF LAW, MEDICINE AND ETHICS, (2010);Mark A. Rothstein, *Access to Information in Segmented Electronic Health Records*, JOURNAL OF LAW, MEDICINE AND ETHICS 394(2012; Hosek & Straus, RAND HEALTH QUARTERLY, (Summer, 2013).

[95] Maja van der Velden & Khaled El Eman, *"Not All My Friends Need to Know": A Qualitative Study of Teenage Patients, Privacy, and Social Media*, 20 JAMIA (JOURNAL OF THE AMERICAN MEDICAL INFORMATICS ASSOCIATION) 16, p. 17 (2013). Kelly Caine & Rima Hanania, *Patients Want Granular*

This approach may be implemented automatically. Big data makes it possible to analyze large databases to predict someone's preferences by identifying cohorts of individuals likely to be similarly inclined in their data protection proclivities and to personalize disclosure default, and then to disclose accordingly. These big data profiles could be used in court to personalize, for example, inheritance in the absence of a will.[96] A similar approach could be extended to automatically release or block access to data according to a calculated preference profile, much as personalized customer recommendations are automatically generated for targeted advertising. In another approach, patients can use a patient portal to control "access keys" in a central registry. These keys, in turn, determine whether requesting organizations may obtain record information from unaffiliated facilities.[97]

Advances in how data is stored, accessed, linked, and analyzed also can serve to protect data better. A flurry of on-going research activity is developing better methods for securely storing and transmitting data. These efforts are being supplemented with better methods of access authorization, encryption, auditing, linking records while masking identity, redacting identifying information in free-text health data, and other means of de-identifying or otherwise protecting patient identities.[98]

Privacy Control over Health Information in Electronic Medical Records, id.|◊at, Cited Pages 7;Hosek & Straus, RAND HEALTH QUARTERLY, (Summer, 2013).

[96] Porat & Strahilevitz, MICHIGAN LAW REVIEW, pp. 3-4, 53 (2014).

[97] Yaorong Ge, et al., *Patient-Controlled Sharing of Medical Imaging Data across Unaffiliated Healthcare Organizations*, 20 JAMIA (JOURNAL OF THE AMERICAN MEDICAL INFORMATICS ASSOCIATION) 157(2013).

[98] Bradley A. Malin, et al., *Biomedical Data Privacy: Problems, Perspectives, and Recent Advances*, 20 JAMIA (JOURNAL OF THE AMERICAN MEDICAL INFORMATICS ASSOCIATION) 2(2013).

2. *Unique Patient Identifiers*

There is no unique identifier for each patient in the US due to privacy concerns. Public outcry and federal regulations prevented HIPAA's 1996 mandate for one from being implemented.[99] However, the advent of electronic health records and their potential to coordinate individual care across delivery settings are motivating urgent calls for national Unique Patient Identifiers. Discussion over Unique Patient Identifiers illustrates the tensions between privacy and the many beneficial uses of patient record information.[100] Advocates of Unique Patient Identifiers believe, as the American Health Information Management Association (AHIMA) put it, "the unique health identifier now can be addressed with technology and sound business practices underpinned by federal and state regulation." They note that, de facto, Social Security Numbers are being used as identifiers, which is more problematic for privacy because of the direct link with financial information.[101] Consequently, a variety of professional and governmental institutions have been working on standards and guidelines.[102]

According to the US government's National Committee on Vital and Health Statistics, Unique Patient identifiers would allow for positive identification of each patient so that an individual's records over his or her lifetime could be linked. Each

[99] Dean F. Sittig & Hardeep Singh, *Legal, Ethical, and Financial Dilemmas in Electronic Health Record Adoption and Use*, 127 PEDIATRICS (April 2011).

[100] Despite the original HIPAA requirement for unique identifiers, political and privacy concerns prevented the Department of Health and Human Services from developing them when Congress prohibited funding for doing so in the Omnibus Appropriations Act of 1998. See http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_049016.hcsp?dDocName=bok1_049016 (last visited September 23, 2013).

[101] American Health Information Management Association, *Limiting the Use of the Social Security Number in Healthcare*, 82 JOURNAL OF AHIMA 52(2011) *available at* http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_049016.hcsp?dDocName=bok1_049016 (last visited September 23, 2013).

[102] These efforts date at least since the 1990s, before HIPAA required implementing identifiers.

person named "John Smith" or "Jane Jones" would have a different identifier. That way, it is claimed:

> Through improved access to information, the Unique Patient Identifier: a) enables the prompt delivery of care during the current encounter, b) facilitates continuity of care, c) supports quality of care, d) reduces cost of integration and e) promotes optimum use of information technology.[103]

Clinicians would be able to obtain information about a patient's previous care, thereby preventing unnecessary duplication of procedures or potential for adverse events due to incomplete information. Patient identification could be verified more easily for insurance and other administrative purposes. Patient data could more easily be aggregated properly so that payers, researchers, policy makers, managers of health systems, and public health officials could do studies based on different cohorts and populations of patients.

Advocates in the National Center on Vital and Health Statistics argue that these identifiers would protect privacy by ensuring authorized access to each patient's information.[104] Nevertheless, many remain concerned that privacy would be compromised, even if the identifiers are cryptologically or biometrically based. People could share their identifiers, just as they now share Social Security Numbers. Identifiers could be stolen. Though use of another's identifier would be more difficult if biometrics are used, some would not want records to follow them, even if it meant possibly

[103] Solomon I. Appavu for the Department of Health and Human Services for the United States Government, National Committee on Vital and Health Statistics, *Part Three: Unique Patient Identifier*(November 27, 1997), *available at* http://www.ncvhs.hhs.gov/app3.htm (last visited September 23, 2013).
[104] Id.

adversely affecting their care. Regardless of technology and HIPAA requirements to remove biometric data when de-identifying records, including biometrics in patient records might make them more difficult to protect. Also, master indices linking an identifier to the individual identified cannot be 100% secure. Algorithms to match patient information with identifiers still need testing and validation in real world situations.[105]

For years, researchers have been proposing privacy-protecting technological alternatives to unique identifiers.[106] One suggested non-technological compromise is for patients to choose if they want a unique patient identifier to link their records. Patients could get Voluntary Universal Healthcare Identifiers (VUHID) at low cost through their HIE, thanks to Global Patient Identifiers, Inc. (GPII), a private-sector organization established in 2008.[107] VUHID is designed so there is no central data base, thus addressing fears of a national centralized patient data base that helped derail the National Patient Identifier. Moreover, the VUHID allows patients to control who has access to what information and who can identify the person associated with clinically sensitive information.[108] This ability to segment data would address the problem of identifying categories of sensitive health information, as also mandated by the HITECH Act by simply having patients make their own decisions about it.[109] However, having some data

[105] Hosek & Straus, RAND HEALTH QUARTERLY, (Summer, 2013).
[106] Peter Szolovits & Isaac Kohane, *Against Simple University Health-care Identifiers*, 1 JAMIA (JOURNAL OF THE AMERICAN MEDICAL INFORMATICS ASSOCIATION) 316(July/August, 1993).
[107] About GPII, http://gpii.info/about.php, (last visited September 23, 2013).
[108] http://gpii.info/system.php, (last visited September 23, 2013).
[109] The HITECH Act directed the Health Information Technology Policy Committee (HITPC, an advisory committee to the Office of the National Coordinator for Health Information Technology) to make these recommendations, and the NCVHS, too, provided initial definitions of categories of sensitive information Justine N. Carr for the National Committee on Vital and Health Statistics, *Recommendations Regarding Sensitive Health Information: Letter to the Honorable Kathleen Sibelius, Secretary, Deparment of Health and Human Services*(November 10, 2010), *available at* http://www.ncvhs.hhs.gov/101110lt.pdf (last

present and some not could lead to questions of data integrity and completeness. Clinicians and researchers may well question whether significant data is missing.

B. Technologies Other than Medical Records

The growing use of new electronic devices for collecting, storing, and transmitting data related to health care lead to increased privacy risks. Even before confirmation that internet and telephone traffic is monitored and the data collected by government agencies such as the National Security Administration (NSA),[110] it was apparent that data transmission is vulnerable. Many health-related applications for smart phones are available commercially, via health care providers, or as part of research projects. As more people get implantable devices (such as pace makers) with radiofrequency identification (RFID) chips that transmit and receive data, this too, presents possibilities for privacy violations, or more alarming, remote tampering with settings on such devices. The UK is undertaking a trial of swallowable transmitters that are embedded in pills. They will monitor whether patients take their medicines and their effects on patients physical activity, heart rate and other health measures. Patients, their doctors, and their relatives can monitor the information using their smartphones or other apps. These kinds of new technologies can help save billions by helping patients remember to take their medicines, helping doctors monitor treatment effectiveness, and reassuring relatives.[111]

visited September 23, 2013).

[110] Greenwald, GUARDIAN WEEKLY, 2013.

[111] Denise Roland, *UK to Get 200 High-Tech Factory Jobs Making 'Swallowable Sensors'.* THE TELEGRAPH, March 10, 2014. 2014, *available at* http://www.telegraph.co.uk/finance/10687395/UK-to-get-200-high-tech-factory-jobs-making-swallowable-sensors.html (last visited July 17. 2014).

They also can pose frightening privacy and autonomy threats.[112] Data transmitted by medical and hospital devices, and by implantable or wearable technologies are vulnerable to surveillance,[113] malware, and hacking.[114] Aging in place projects involve home sensors that monitor individual movement, food use and consumption, etc., while home monitoring equipment sends vital signs and other health information to remote locations. These technologies track information that many consider private.[115] Telehealth consultations, some to services in foreign countries (such as teleradiology or telecardiology services between the US and, for example, India), electronic mail and other messaging between clinicians and patients, even e-ICU set-ups in which images and data from intensive care units are transmitted to a central location for monitoring by clinical specialists, involve use of services that could be hacked, bugged, or swept up in broad-based collection of telephone and internet traffic.

Additional concerns surround the growing use of personal health records or computer-based disease management records maintained by insurance companies, employers, or private services. Regardless of individual intent, or even knowledge, that data *is* made available to others, people willingly enter data they may or may not wish to make available to unknown others at popular web sites such as PatientsLikeMe, or

---

[112] JB Bardot, *Forget Personal Privacy - UK to Microchip Prescription Medicines with New Smart Pill*(February 2, 2012), *available at* http://www.naturalnews.com/034843_medicines_microchipping_smart_pill.html (last visited April 26, 2014).

[113] Qmed Staff, HIPAA vs. The NSA: Who Wins When Medical Devices Are Concerned? August 26, 2013.

[114] Shams Zawoad & Ragib Hasan, *The Enemy Within: The Emerging Threats to Healthcare from Malicious Mobile Devices*, *in* WIRELESS MOBILE COMMUNICATION AND HEALTHCARE: THIRD INTERNATIONAL CONFERENCE, MOBIHEALTH 2012 (Balwant Godara & Konstantina S. Nikita eds., 2013). Tang & Zimmerman, COMMUNICATIONS OF THE ACM, (2013). Kevin Fu & James Blum, *Controlling for Cybersecurity Risks of Medical Device Software*, 56 COMUNICATIONS OF THE ACM 35(2013).

[115] Bonnie Kaplan & Sergio Litewka, *Ethical Challenges of Telemedicine and Telehealth*, 17 CAMBRIDGE QUARTERLY OF HEALTHCARE ETHICS 401(2008).

23andme, where personally identifiable health, illness, and genetic information is stored and shared.[116] One innovative approach for data sharing with attention to privacy preferences is the new international Open Humans Network, which "attempts to break down health data silos through an online portal that will connect participants willing to share data about themselves publicly with researchers who are interested in using that public data and contributing their analyses and insight to it."[117] People also share such information via personal health records (which may be provided by health care organizations, insurers, or commercial vendors), blogs, on-line support groups, listservs, tweets, etc. Public health trends can be detected by data mining information from such activities, including e-mail, Facebook and Twitter.[118] Neither some e-mail services nor data entered into sites such as PatientsLikeMe or Facebook is private, but may be sold to pharmaceutical and other companies.[119] Data from these kinds of sources and from devices also is being incorporated into patient records, sometimes supplied by the patient, but sometimes without the patient's knowledge, and without clarity over who owns the data.[120]

With increasing sophistication of biometric identification, such as identifying individuals from photographs and tagging them with location data, privacy may be even

[116] Some individuals bring their 23&me reports to their physicians to discuss prophylactic treatment. Consequently, their genomic information may be added to their records.
[117] Open Humans Network, *Open Humans Network Wins Knight News Challenge: Health Award*, *available at* http://openhumans.org/ (last visited July 1, 2014).
[118] Nicholas A. Christakis & James H. Fowler, *Social Network Vsualization in Epidemiology*, 19 NORWEGIAN JOURNAL OF EPIDEMIOLOGY 5(2009); Nicholas A. Christakis & James H. Fowler, *Social Network Sensors for Early Detection of Contagious Outbreaks*, 5 PLOS ONE e12948(2010); Edward Velasco, et al., *Social Media and Internet-Based Data in Global Systems for Public Health Surveillance: A Systematic Review*, 93 THE MILBANK QUARTERLY, 7 pp. 13, 23, 25 (2014).
[119] JULIA ANGWIN, DRAGNET NATION: A QUEST FOR PRIVACY, SECURITY, AND FREEDOM IN A WORLD OF RELENTLESS SURVEILLANCE p. 2 (Times Books, Henry Holt and Company. 2014).
[120] John Moore & Rob Tholemeier, Whose Data Is It Anyway? (November 20, 2013).

more compromised. Such data can be collected by government agencies and private companies. Some electronic record systems include patients' photographs and projects are under way to link virtual reality and Google Glass capabilities with electronic health records.[121] The push to include genomic data in electronic medical records raises additional concerns.[122] As of 2012, the Department of Health and Human Services, had not clarified whether genetic or genomic information falls under one of the HIPAA identifiers.[123] Already, genomic data, when combined with other metadata, has been used to identify surnames,[124] raising the usual problem of balancing vs individual good.[125] Pilot projects funded by the National Human Genome Research Institute (NHGRI)[126] and the Eunice Kennedy Shriver National Institute of Child Health and Human Development (NICHD)[127] investigate genome sequencing for screening newborns and how to incorporate genomic data into official medical records, such projects make it questionable whether stripping other identifiers is sufficient. Despite targeted legislative mandates, as numerous recommendations make clear, further policy is needed concerning what genomic information should be release to whom, and what should become part of

[121] See, for example, Jennifer Bresnick, *Google Glass is Making A Convincing Case For Healthcare*, EHR Intelligence(March 21, 2014), *available at* http://ehrintelligence.com/2014/03/21/google-glass-is-making-a-convincing-case-for-healthcare/ (last visited July 15, 2014). and Bernie Monagain, *Google Glass Links to EHR*(June 19, 2014), *available at* http://www.healthcareitnews.com/news/drchronos-bright-ideas-google-glass (last visited July 15, 2014).

[122] Presidential Commission for the Study of Bioethical Issues, Privacy and Progress in Whole Gene Sequencing (Presidential Commission for the Study of Bioethical Issues ed., October 2012).

[123] Id. at, pp. 62-63.

[124] Melissa Gymrek, et al., *Identifying Personal Genomes by Surname Inference*, 339 SCIENCE 321(2013).

[125] Amy Gutmann & James W. Wagner, *Found Your DNA on the Web: Reconciling Privacy and Progress*, 43 HASTINGS CENTER REPORT 15-18(2013).

[126] Department of Health and Human Services United States Government, National Institutes of Health, National Human Genome Research Institute, genome.gov, *Clinical Sequencing Exploratory Research (CSER)*, *available at* http://www.genome.gov/27546194 (last visited September 23, 2013).

[127] Department of Health and Human Services United States Government, National Institutes of Health, *NIH Program Explores the Use of Genomic Sequencing in Newborn Healthcare*(September 4, 2013), *available at* http://www.nih.gov/news/health/sep2013/nhgri-04.htm (last visited September 23, 2013).

medical and biobanking records,[128] [129] whether results are obtained from individual clinical or commercial testing, part of a research project, or in other ways.[130] Although the proposal has not received as much attention, the Institute of Medicine's recommendation that electronic records include behavioral and social data believed to be determinants of health[131] will contribute to compromising privacy.

IV. LEGAL REMEDIES and BALANCING VALUES

This section discusses how data ownership, informed consent, and free speech relate to health data privacy. Each is one way to address health privacy issues, yet none of these approaches is adequate by itself. Divergent analyses and recommendations highlight how complex the issue is.[132]

A. Aggregating and Selling Data

As discussed, big data analytics are valuable for business, public health, and research. Provider data and de-identified patient data can be sold without requiring individual permission. A recent Supreme Court case upheld selling prescription data on free speech grounds. In *Sorrell v IMS Health Inc., et al.*, decided June 23, 2011, the Court struck down a Vermont law that restricted selling identifiable prescriber data for use in marketing prescription drugs.[133] Vermont made this restriction, in part, to protect

[128] Gymrek, et al., SCIENCE, (2013).
[129] Presidential Commission for the Study of Bioethical Issues, Privacy and Progress in Whole Gene Sequencing. October 2012.
[130] Kimberly Shoenbill, et al., *Genetic Data and Electronic Health Records: A Discussion of Ethical, Logistical and Technological Considerations*, 21 JAMIA (JOURNAL OF THE AMERICAN MEDICAL INFORMATICS ASSOCIATION) 171(2014).
[131] INSTITUTE OF MEDICINE, Capturing Social and Behavioral Domains in Electronic Health Records: Phase 1. 2014. Summary of Selected Domains *available at* http://iom.edu/~/media/Files/Report%20Files/2014/EHR-Phase-1/EHRdomains.pdf.
[132] Patricia Sanchez Abril, *Selling Privacy*, *in* BEYOND INTELLECTUAL PROPERTY: THE FUTURE OF PRIVACY (Shlomit Yanisky-Ravid ed. this volume).
[133] Sorrell v. IMS Health, Inc. et al, 131 S. Ct. 2653 (2011).

privacy and physician confidentiality, but the Court did not consider potential privacy threats to prescribers sufficient to uphold the law, nor did they consider privacy threats to patients because the data ultimately is HIPAA de-identified. The case illustrates how various legal doctrines may conflict. It was framed as a free speech First Amendment issue rather than one of privacy. Nevertheless, the United Kingdom's Court of Appeal reached a similar conclusion on privacy grounds in *R v. Department of Health, Ex Parte Source Informatics Ltd*. The Court considered that selling de-identified prescription data for pharmaceutical marketing did not violate pharmacists' duty to confidentialy because the data was de-identified.[134] Both the *Source* and *Sorrell* decisions are problematic on privacy and other ethical grounds.[135]

1. Data Aggregators: Privacy Risks vs Data Value

Companies, government agencies, and professional organizations specialize in data aggregation and analytics. The data is used for research, public health, health insurance, administering health care organizations and meeting regulatory requirements, professionals. Concerns about communications to patients encouraging them to purchase or use a healthcare-related product or service led Congress to expand limitations on the sale of medical information to third parties for marketing purposes.[136], [137]

---

[134] R v. Department of Health, Ex Parte Source Informatics Ltd., [C.A. 2000] 1 All ER 786.. See also *R v. Department of Health, Ex Parte Source Informatics Ltd*, 4 EUROPEAN LAW REPORT 397(2000).
[135] Kaplan, CAMBRIDGE QUARTERLY OF HEALTHCARE ETHICS, (in press);Kaplan, CAMBRIDGE QUARTERLY OF HEALTHCARE ETHICS, (in review).
[136] Koontz, What Is Privacy? 2013.
[137] Department of Health and Human Services United States Government, Office for Civil Rights, *Standards for Privacy of Individually Identifiable Health Information*, *available at* http://aspe.hhs.gov/admnsimp/final/pvcguide1.htm (last visited January 19, 2014), describes the limitations set forth under HIPAA § 164.506.

Anonymity can make data useless.[138] Data is far more valuable when it can be linked to other data about the same person. It is unclear whether data aggregators receive patient-identifible data.[139],[140] Even if they do,[141] or if they strip the identifiers as HIPAA requires, data aggregators add a unique patient ID that enables patient tracking over time and, some have argued, could be used to link this data with data in public records (including hospital discharge databases) and commercial databases to re-identify patients,[142] especially in sparsely populated rural areas.[143]

Data brokers obtain, share, and sell information on nearly every consumer in the US. The provide a valuable service in collecting, cleaning, aggregating, and storing data,

[138] Ohm, UCLA LAW REVIEW, p. 1752 (2010).
[139]Gordon Atherley, *The Public-Private Partnership Between IMS Health and the Canada Pension Plan*, FRASER FORUM 2011.
[140] Curfman, et al., NEW ENGLAND JOURNAL OF MEDICINE, (2011).
[141] IMS Health makes clear on their web site that they work with identified patient data, but that they will obtain patient permission and use the data only for the purposes for which it was collected. Further, they state that they "employ a combination of privacy, compliance, legal and other resources, together with a combination of technical, physical and administrative safeguards, to ensure that privacy and data protection are core competencies." http://www.imshealth.com/portal/site/ims/menuitem.5ad1c081663fdf9b41d84b903208c22a/?vgnextoid=534bc9e28f44f210VgnVCM10000071812ca2RCRD&vgnextfmt=default, (last visited September 24, 2013). Aggregators, such as RPC Health Data Store, sell a wide variety of both national and state health care data, customizable reports, and analytics based on combining this with "specialized databases, such as mapping systems, population estimates, economic forecast information, and physical supply and demand projection trends." (http://www.healthdatastore.com/About.aspx\ (last visited Sept 13, 2013.) The Centers for Medicare and Medicaid Services (CMS) collects and releases data for all U.S. hospital inpatient stays for Medicare beneficiaries. This data is released annually in the CMS Medicare Provider Analysis and Review (MedPAR) file. Each record in the MedPAR file represents an inpatient stay during the calendar year of the file and has information on diagnosis, procedure, charge, payment, provider and patient for the claim. The health data store created a data dictionary PDF for the file, which lists and describes the data elements and the file layout. Another company, Crimson Market Services seem to have created a patient identifier that can track patients across providers and systems. Though in their presentations they describe combining third party payer data with internal data at organizations to track patients as they move through the system from primary care to hospital, there is no indication of this capability on their website, http://www.advisory.com/Technology/Crimson-Market-Advantage, (last visited September 24, 2014
[142] Joint Appendix, Volume 1 at 155, William H. Sorrell et al. v. IMS Health Inc. et al., 2010 U.S. Briefs 779 (2nd Cir. 2011) (No. 10-779).
[143] Brief for the New England Journal of Medicine, the Massachusetts Medical Society, the National Physicians Alliance, and the American Medical Students Association as Amici Curiae Supporting Petitioners, William H. Sorrell v. IMS Health, Inc. et al., 2010 U.S. Briefs 779 (No. 10-779), 2011 U.S. S. Ct. Briefs LEXIS 299.

and in combining it in ways that make it more valuable than the separate records and databases involved. The combination, too, is more revealing, as even seemingly innocuous data may threaten privacy when used in a new context or linked to other data. Nevertheless, they operate with what the Federal Trade Commission calls "a fundamental lack of transparency," raising significant privacy concerns.[144]

Data aggregators get data from multiple extensive online and offline sources, including health data. The Centers for Medicare and Medicaid Services (CMS) for example, sell patient data. Though their data use agreements prohibit individual identification, the data CMS provides is not de-identified as to patient or provider.[145] They collect and release data for Medicare beneficiaries for each inpatient stay at all US hospitals during each calendar year, including information on diagnosis, procedure, charge, payment, provider and patient for the claim. State public health agencies have been selling patient hospital data for years to both researchers and to data aggregators.[146] Though de-identified, it can be relinked to individuals using public information.[147] Arizona, California, Florida, Illinois, Maryland, Massachusetts, New Jersey, New York, Pennsylvania, Tennessee, Texas, and Washington sell medical records that can be used to

[144] Federal Trade Commission United States Government, *FTC Recommends Congress Require the Data Broker Industry to be More Transparent and Give Consumers Greater Control Over Their Personal Information*(May 27, 2014), *available at* http://www.ftc.gov/news-events/press-releases/2014/05/ftc-recommends-congress-require-data-broker-industry-be-more (last visited July 14, 2014).

[145] Department of Health and Human Services United States Government, Centers for Medicare & Medicaid Services, *Agreement for Use of Centers for Medicare & Medicaid Services (CMS) Data Containing Unique Identifiers, Form CMS-R-0235, OMB No. 0938-0734*, *available at* http://www.cms.gov/Medicare/CMS-Forms/CMS-Forms/downloads//cms-r-0235.pdf, (last visited September 13, 2013).

[146] Jordan Robertson, *States Review Rules After Patients Identified Via Health Records*, BUSINESS WEEK 2013, *available at* http://www.businessweek.com/news/2013-07-22/states-review-rules-after-patients-identified-via-health-records\ (last visited July 22, 2013).

[147] Jordan Roberston, *States' Hospital Data for Sale Puts Privacy in Jeopardy*(2013), *available at* http://www.healthleadersmedia.com/content/QUA-292963/States-hospital-data-for-sale-puts-privacy-in-jeopardy (last visited June 14, 2013).

link a person's identity to medical conditions via public information.[148] Arizona, New York, New Jersey, Tennessee, and Washington records include some combination of age, zip codes and admission and discharge dates, making the data particularly vulnerable to re-identification.[149]

Many US organizations can use and legally sell health information,[150] some for purposes patients and clinicians would not anticipate. Aggregators purchase and combine data from the states as well as from pharmacies.[151] Credit reporting agencies were the most frequent buyers of multi-state health profiles, but IMS Health, Inc. also purchases data from the states.[152] This public-private data linking was even more evident when the Canadian Pension Plan Investment Board and TPG Capital purchased IMS Health in 2010. IMS Health owns of one of the world's deepest pools of medical information. It has prescription-drug dossiers on 260 million people; about 85% of its revenues come from reselling this data to pharmaceutical companies for designing drug sales pitches.[153] As noted above, the company has gone to court to protect its business. Services such as the RPC Health Data Store create and sell a data dictionary which lists and describes the data elements and the file layout, as well as "custom reports, graphs and maps using this data file and combining it with other health care and demographic files."[154]

---

[148] [Winston], States' Hospital Data for Sale Puts Patient Privacy in Jeopardy. June 7, 2013..
[149] Roberston, States' Hospital Data for Sale Puts Privacy in Jeopardy. 2013.
[150] Yaron F. Dunkel, *Medical Privacy Rights in Anonymous Data: Discussion of Rights in the United Kingdom and the United State in Light of the Source Informatics Cases*, 23 LOYOLA OF LOS ANGELES INTERNATIONAL AND COMPARATIVE LAW REVIEW (2001).
[151] RPC Health Data Store, *CMS MedPAR Hospital Data File*, *available at* http://www.healthdatastore.com/cms-medpar-hospital-data-file.aspx (last visited September 13, 2013).
[152] {Winston], States' Hospital Data for Sale Puts Patient Privacy in Jeopardy. June 7, 2013.
[153] Id.
[154] RPC Health Data Store, CMS MedPAR Hospital Data File.

Clinician privacy also is not protected. Just as IMS sells individually identified prescriber data, the American Medical Association[155] and health information exchanges (HIEs)[156] and CMS sell provider data.[157] Insurance companies or health information technology vendors might aggregate and sell provider-identified data on performance and quality measures, number of procedures performed, meaningful use criteria, data security breaches, etc. It is easier to link (even de-identified) patient data to clinician data if identifiable clinician data is readily available.

If such sales were restricted, some fear, the data would not be collected at all, which could compromise research and new drug development.[158] Others note that stripping identifiers such as age, zip code, and hospitalization dates, as required of non-state actors, would make it useless for epidemiological tracking.[159]

B. Data Ownership

Property rights in information are evolving as compilations of facts are being recognized as proprietary information.[160] Data aggregation and dissemination is becoming increasingly valuable, and increasingly protected through case law and contract as property rights in information expand.[161]

Selling patient data raise the question of who owns and controls that data. Patients, after all, lose control over their pharmacy data once they fill a prescription or

[155] Curfman, et al., NEW ENGLAND JOURNAL OF MEDICINE, (2011).
[156] TONI HEBDA & PATRICIA CZAR, HANDBOOK OF INFORMATICS FOR NURSES AND HEALTHCARE PROFESSIONALS p. 321 (Pearson/Prentice Hall 4th ed. 2009).
[157] United States Government, Agreement for Use of Centers for Medicare & Medicaid Services (CMS) Data Containing Unique Identifiers, Form CMS-R-0235, OMB No. 0938-0734.
[158] Brief for the Association of Clinical Research Organizations as Amici Curiae Supporting Respondents, William H. Sorrell v. IMS Health, Inc. et al, 2011 WL 2647130 (2011) (No. 10-779), (2011).
[159] Roberston, States' Hospital Data for Sale Puts Privacy in Jeopardy. 2013.
[160] Abril, Selling Privacy. this volume.
[161] RENÉE MARLIN-BENNETT, KNOWLEDGE POWER: INTELLECTUAL PROPERTY, INFORMATION, AND PRIVACY pp. 7-12 (Lynne Reinner Publishers. 2004).

provide information to various web sites and insurance companies. They lose control over medical information generated in the course of treatment once it is recorded in a medical record. Clarity is needed over what health data can be owned, who can own what data, and what may be done with it. As Renée Marlin-Bennett argues in connecting intellectual property and privacy rights:

> Rules, again often in the form of laws, establish the conditions under which an individual can control that flow of personal information. If I cannot stop information about myself from being transmitted against my will, my privacy has been breached.[162]

It generally is considered that clinicians and insurers own the tangible form of a patient record. Patients own the data itself, but not the record; they have rights of privacy and access, and may obtain copies of their records if they pay "reasonable, cost-based" fees,[163] but cannot destroy or claim sole possession of the record, as they might with objects they own. This was more clear when records were kept on paper, but the advent of electronic records makes ownership confusing to both patients and clinicians.[164] Ownership will become even more muddled as data from medical devices, personal health records, social networking, home monitors, sensors, and other patient generated data gets incorporated into patient records. Who owns that data is debatable.[165]

[162] Id. at, p. 17

[163] Department of Health and Human Services United States Government, Office for Civil Rights, *Health Information Privacy: If patients request copies of their medical records as permitted by the Privacy Rule, are they required to pay for the copies?*(March 14, 2006 (created December 20, 2002)), *available at* http://www.hhs.gov/ocr/privacy/hipaa/faq/right_to_access_medical_records/353.html (last visited January 19, 2014).

[164] Hall & Schulman, JAMA, (2009).

[165] Moore & Tholemeier, Whose Data Is It Anyway? November 20, 2013.

Medical records are property, but medical information is not.[166] The distinction between owning data and owning the tangible vessel in which data is kept is lost on most people. Such distinctions are even more murky when data about a patient may be stored in multiple archives that can be linked through a distributed architecture that involves the patient, the care provider, the organization where care is provided, and services to store, link data, and aggregate data. Who, and under what circumstances, should coordinate and determine whether and how data may be tapped for individual or public benefit?[167]

Organizations and HIEs,[168] too, need consider ownership and rights to records. Some propose that healthcare organizations not sell data without patient consent, and only after reviewing the ethics of how that data will be used. This approach also suggests a similar review of HIPAA-allowed secondary data uses for compatibility with the organization's goals and its ethical principles.[169]

Law and common ethical practice prevent conveying medical information without a patient's permission, but legally, nothing prevents selling or transferring rights to records. Health care providers and organizations, where patient data necessarily is first obtained, act as the data (as opposed to the record) is their private property and often sell it.[170] Contractual agreements governing data ownership and sale are made easier when records are electronic. Computer or software vendors, trusted intermediaries, or newly

[166] Mark A. Hall, *Property, Privacy, and the Pursuit of Interconnected Electronic Health Records*, 95 IOWA LAW REVIEW p. 646 631(2010).
[167] Evans, HARVARD JOURNAL OF LAW & TECHNOLOGY, pp. 102, 105 (2011).
[168] HEBDA & CZAR, Handbook of Informatics for Nurses and Healthcare Professionals p. 323. 2009.
[169] Larry Ozeran, *Considering Ethics in Privacy*, *in* INFORMATION PRIVACY IN THE EVOLVING HEALTHCARE ENVIRONMENT (Linda Koontz ed. 2013).
[170] Mark A. Rodwin, *Patient Data: Property, Privacy, & the Public Interest*, 36 AMERICAN JOURNAL OF LAW AND MEDICINE 586, p. 588 (2010).

created organizations theoretically can bundle and sell rights and data.[171] Well-known electronic health record vendors have sold de-identified copies of their patient databases to pharmaceutical companies, medical device makers, and health services researchers.[172] Patient data is becoming the private property of commercial interests.[173] Contracts between health care organizations and electronic record vendors specify that the patient data becomes the vendor's property. This is an unusual arrangement; businesses and financial institutions do not give up their data to their software vendors.[174] Some indicate that once the relationship ends, patient data will be destroyed or returned "if feasible" but also can continue to be aggregated and shared by the vendor with others.[175] It is not clear from vendor web sites where or how data they sell was obtained or to what purpose it might be put. For example,[176] Fair Isaac Corporation, which provides the FICO® Score,

[171] Hall & Schulman, JAMA, (2009).
[172] Sittig & Singh, PEDIATRICS, (April 2011).
[173] Rodwin, AMERICAN JOURNAL OF LAW AND MEDICINE, p. 589 (2010).
[174] Moore & Tholemeier, Whose Data Is It Anyway? November 20, 2013.
[175] Marlene Durben Hirsch, *5 Unique EHR Contract Stipulations: Scary, Odd and Even Fun Provisions from Vendor Agreements*(June 17, 2014), *available at* http://www.fierceemr.com/story/5-unique-ehr-contract-stipulations/2014-06-17?page=full (last visited June 19, 2014).
[176] RPC Health Data Store referenced in notes 141, 151, 154, is one other example. Two other examples: (1) GE Data Visualization uses information "based on 7.2 million patient records from GE's proprietary database" http://visualization.geblogs.com/visualization/network/ (last visited September 27, 2013), and GE Healthcare's Healthcare IT solutions include patient records and patient portals. See http://www3.gehealthcare.com/en/Products/Categories/Healthcare_IT?gclid=CIKQ4Z6P7LkCFcE7OgodTDIAPQ and http://www3.gehealthcare.com/en/Products/Categories/Healthcare_IT/Knowledge_Center. (last visited September 27, 2013). (2) On the other hand, Optum, for example, describes services based on patient claims data and medical record data but gives no indication of the source of the data. http://www.optuminsight.com/physicians/solutions/cost-clinical-and-quality-management-phy/optum-care-suite/overview/, (last visited September 24, 2013). The data is patient-specific: "Optum Care Pathways allow for the development of customized, multi-provider care plans for patients based on patient's individual needs; Optum Care Coordination provides tools that closely track and document patient care across settings and providers, thus enhancing visibility into diagnoses and treatments and facilitating team-based approaches to patient care." See http://www.optuminsight.com/physicians/solutions/cost-clinical-and-quality-management-phy/optum-care-suite/features/, (last visited September 24, 2014). They "identif[y] patients with chronic conditions and health risks, alerting physicians to gaps in care. http://www.optuminsight.com/about/focus/, (last visited September 23, 2013). They also "create secure, interoperable networks that enable the exchange of information among communities" without identifying what kinds of communities are being networked. See

"the standard measure of consumer credit risk in the United States,"[177] launched a Medication Adherence Score. Their website claims that:

> leveraging multiple, rich third-party data sources, the Medication Adherence Score can predict each patient's adherence over the next year. [It] use[s] a patient's prescription claims history when available and pull[s] on other publicly available third-party data sources when no other information is present.[178]

Consumer advocates were alarmed when FICO announced this tool even though FICO officials claimed this information could not be used by insurers to adjust risk.[179] Nevertheless, private insurers use prescription and other claims data to deny insurance, charge differential premiums, or exclude some conditions.[180] According to the Federal Trade Commission, the MIB Group (Medical Information Bureau) Inc., which operates in the US and Canada, and whose member insurance companies account for 99% of the individual life insurance policies and 80% of all health and disability policies issued in the United States, collects underwriting information from member insurance companies. It then provides reports of medical conditions, potentially dangerous hobbies, adverse driving records, and possibly criminal activity[181] "to assess an individual's risk and eligibility during the underwriting of life, health, disability income, critical illness, and long-term care insurance policies," while its subsidiaries offer other services to members

---

http://www.optuminsight.com/about/businesses/, (last visited September 24, 2013).

[177] FICO, *About Us*, *available at* http://www.fico.com/en/about-us/ (last visited January 8, 2014).

[178] FICO, *FICO® Medication Adherence Score*, *available at* http://www.fico.com/en/products/fico-medication-adherence-score/ (last visited January 8, 2014).

[179] McGraw, JAMIA (JOURNAL OF THE AMERICAN MEDICAL INFORMATICS ASSOCIATION), (2013).

[180] Brief for the New England Journal of Medicine, the Massachusetts Medical Society, the National Physicians Alliance, and the American Medical Students Association as Amici Curiae Supporting Petitioners, William H. Sorrell v. IMS Health, Inc. et al., U.S. Briefs 779 (No. 10-779), 2011 U.S. S. Ct. Briefs LEXIS 299.

[181] [Winston], States' Hospital Data for Sale Puts Patient Privacy in Jeopardy. June 7, 2013.

and customers.[182] Businesses, too, often check job applicants' MIB data.[183] The same is happening in the UK. The Institute of Faculty and Actuaries NHS data on all hospital stays from 1997-2010 with "socio-economic profiles" like credit ratings to advise insurance companies how to revise their premiums.[184]

1. Ownership Limbo

[182] MIB, *The Facts About MIB*, *available at* http://www.mib.com/facts_about_mib.html (last visited May 3, 2014).
[183] DAVID H. HOLTZMAN, PRIVACY LOST: HOW TECHNOLOGY IS ENDANGERING YOUR PRIVACY p. 195 (Jossey-Bass. 2006).
[184] Donnelly, THE TELEGRAPH, February 23, 2014.

Mark A. Hall considers "no legal question … more critical, more contested, or more poorly understood" than whether the patient, provider, or insurer owns a patient's medical information.[185] As in other countries, current US law does not address ownership clearly. If patients owned their data, they would have more control over what happens with it. Some propose just that, suggesting that if patients could license use of their data, economic incentives would be added to individual health care benefits. The result would more strongly encourage linking and integrate records, thereby enabling a network of longitudinally linked records that would be clinically useful.[186] Expanding this idea of economic value to patient-controlled health records also would be useful for creating databases for research, marketing, public health, and other unforeseen purposes. Ownership limbo, though, stymies any development along these or other productive directions, and prevents those who would be burdened by sharing data from reaping benefits. Although the issue is not as acute for integrated comprehensive systems, such as in the US Veteran's Administration and the large private Kaiser-Permanente network, effectively linking electronic medical records runs up against legal uncertainties over ownership and control and economic disincentives to link data.[187]

This is not only an issue in the US. Data ownership needs to be resolved clearly elsewhere, though again, where there are integrated networks, as in Europe, the problem is not so severe. The law needs to specify medical information ownership, control, and commercialization.[188]

---

[185] Hall, IOWA LAW REVIEW, p. 631 (2010).
[186] Hall & Schulman, JAMA, (2009).
[187] Hall, IOWA LAW REVIEW, pp. 637-640 (2010).
[188] Id. , at p. 642.

2. Personal Data Ownership and Control

Some propose principles for monetizing control over medical information intended to address these concerns, but scholars in this area disagree over who the owner should be, or whether ownership is better than the current approach.[189]

One suggested approach is for patients to own their data so they could license using it, thereby adding economic incentives to individual health care benefits. Proponents argue that this economic value of patient-controlled health records also would be useful for creating databases for research, marketing, public health, and other unforeseen purposes. Currently, effectively linking electronic medical records runs up against economic disincentives and legal uncertainties over ownership and control.[190] Ownership, it is argued would encourage linking and integrating records, thereby enabling a network of longitudinally linked records that would be clinically useful.[191] Others propose government ownership instead, while other legal scholars consider property rights in data, at best, unnecessary, and potentially worrisome.[192] Additionally, if data is a form of communication, as discussed next, perhaps health data can be protected as intellectual property. However, property protection of pharmaceuticals, devices, and health information technologies, also can impede access to the information or products being protected.

[189] Id. at, pp.660-663;Evans, HARVARD JOURNAL OF LAW & TECHNOLOGY, p. 87 (2011);Abril, Selling Privacy. this volume.
[190] H all, IOWA LAW REVIEW, pp. 637-640 (2010).
[191] Hall & Schulman, JAMA, (2009).
[192] Evans, HARVARD JOURNAL OF LAW & TECHNOLOGY, p. 74 (2011).

Marketplace norms can be anathema to professional values and the special relationship between doctor and patient.[193] Moreover, the idea of medical information as property subject to commercial practices is disturbing to those who see it as commodifying the self and sullying ideas of personhood. Allowing patients to license use of their data assumes they will be able to anticipate potential uses, risk, and benefits. They may restrict access for research or for public health, or otherwise limit the public-goods value of medical information.[194] Research approaches requiring large, broadly inclusive data sets would be undermined by patients' refusal to allow their data to be included. Others are concerned that the price of data may make it more difficult for researchers than for the commercial sector to obtain data.[195] This complex balance between individual preference, professional norms, and public good is not resolvable by current regulation.[196]

[193] Hall, IOWA LAW REVIEW, p. 656 (2010).
[194] Id. at, pp. 657, 659.
[195] Frank Pasquale, *Restoring Transparency to Automated Authority*, 9 JOURNAL ON TELECOMMICATIONS AND HIGH TECHNOLOGY LAW 235(2011).
[196] Evans, HARVARD JOURNAL OF LAW & TECHNOLOGY, p. 76 (2011).

Privacy scholar Mark A. Hall claims that "no legal question is more critical, more contested, or more poorly understood" than whether the patient, provider, or insurer owns a patient's medical information. The law needs to specify medical information ownership, control, and commercialization.[197] This is not only an issue in the US. Data ownership needs to be resolved clearly elsewhere, though where there are integrated healthcare networks, as in Europe, ownership is less problematic. Additionally, whether control over data is a sufficient view of privacy needs further consideration, although control and data protection are the basis of privacy in both the US and EU. These divergent analyses and recommendations highlight how complex the issue is.[198]

C. Free Speech, Free Choice

The balance between making data available for research and public health and protecting individual privacy is complicated in the US by considerations of free speech protection, which now covers marketing based on prescription data.[199] The *Sorrell* decision[200] that permitted this is one of few cases that have challenged data privacy law on First Amendment grounds. In those few cases, lower courts have treated communicating raw data as speech. However, the common assumption underlying privacy law is that speech and data are different.[201] For legal scholars of commercial speech, like Tamara R. Piety, it seems that it is stretching to extend First Amendment "free speech" rights to corporations, and that selling prescription data that will be used by

---

[197] Hall, IOWA LAW REVIEW, pp. 631, 642 (2010).

[198] Abril, Selling Privacy. this volume.

[199] Kaplan, CAMBRIDGE QUARTERLY OF HEALTHCARE ETHICS, (in press).

[200] Sorrell v. IMS Health, Inc. et al, S. Ct.

[201] Bambauer, STANFORD LAW REVIEW, (2014), from Arizona Legal Studies Discussion Paper No. 13-19, pp. 71-72, 57. Available at http://www.stanfordlawreview.org/print/article/data-speech, (last visited February 3, 2014).

other corporations to sell pharmaceuticals to prescribers and patients is hardly speech that should be protected. Others, like Joan R. Bambauer, argue instead that treating data as speech enables access to information.[202]

In addition to tensions between privacy and free speech, both First Amendment protections, the issue is complicated in that no one has a choice when it comes to prescription medication. Prescribers and patients must be identified on prescriptions. Thus, marketing interests benefit from these legal requirements of required information collection.[203]

Similarly, there is little choice involved with mandates for electronic health records and health information exchanges. Medical records will be created, maintained, stored, and transmitted electronically, making them subject to further privacy threats from government and private sector alike. These threats are exacerbated by the concommitant integration and consolidation of health care providers.[204] There also is little choice in the Affordable Care Act's health insurance mandate. The very people the act is most intended to help, the uninsured, will be most vulnerable in having their personal information open to numerous agencies and individuals. Will they consider access to care (or rather, access to insurance) worth the privacy threats? Will they even know? Will they have a choice?

---

[202] TAMARA R. PIETY, BRANDISHING THE FIRST AMENDMENT: COMMERCIAL EXPRESSION IN AMERICA (University of Michigan Press. 2012);Bambauer, STANFORD LAW REVIEW, (2014). from Arizona Legal Studies Discussion Paper No. 13-19, pp. 71-72, 1. Available at http://www.stanfordlawreview.org/print/article/data-speech, (last visited February 3, 2014).

[203] Kaplan, CAMBRIDGE QUARTERLY OF HEALTHCARE ETHICS, (in press).

[204] Mark A. Rothstein, *The Latest Challenge to Health Privacy: Health Care Consolidation*, The Hastings Center(May 13, 2014), *available at* http://thehastingscenter.org/Bioethicsforum/Post.aspx?id=6907&blogid=140 (last visited June 27, 2014).

D. Informed Patients/Informed Consent

The principle of patient autonomy,[205] as institutionalized in informed consent, is fundamental for both care and research. Just as the regulations discussed in Section I are less protective than they appear, so too are concepts like "informed consent." The 2008 Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information includes the principle of individual choice:

> "Individuals should be provided a reasonable opportunity and capability to make informed decisions about the collection, use, and disclosure of their individually identifiable health information….The degree of choice made available may vary with the type of information being exchanged, the purpose of the exchange, and the recipient of the information. Applicable law, population health needs, medical necessity, ethical principles, and technology, among other factors, may affect options for expressing choice."[206]

In HIPAA terms, though, this is called "authorization," which refers to disclosing personal health information; "consent" is reserved for human subjects research.[207] This discussion of "consent" therefore includes "authorization."

"Informed consent" has two components, "informed" and "consent."

---

[205] The principle of autonomy, on which "informed consent" is based, stems from what is known as "The Belmont Report," *t* http://www.hhs.gov/ohrp/humansubjects/guidance/belmont.html (last visited January 30, 2014). The principles articulated there are developed in the well-known TOM L. BEAUCHAMP & JAMES F. CHILDRESS, PRINCIPLES OF BIOMEDICAL ETHICS (Oxford University Press now in its 5th (2001) ed. 1985)..

[206] United States Government, Standards for Privacy of Individually Identifiable Health Information p. 8.

[207] http://www.hhs.gov/hipaafaq/permitted/research/313.html, (last visited January 19, 2014; Goldstein, JOURNAL OF LAW, MEDICINE AND ETHICS, p. 31 (2010).

1. Consent

Discussion here is limited to competent adults, which is complicated enough. "Consent" for persons presumed incompetent, or for pediatric patients, is more problematic. Minors can consent to some kinds of health care and they may be able to protect their privacy without parent permissions, especially where reproductive, psychiatric, and substance abuse services are involved. Likewise, parents may prevent disclosure of health information about a child to that child.[208]

The law emphasizes complying with rules, what Melissa M. Goldstein calls "rule-based consent."[209] For example, The HIPAA Privacy Rule requires most doctors, hospitals, other health care providers, pharmacies, etc. to obtain a patient's written consent before using or disclosing the patient's personal health information to carry out treatment, payment, or health care operations. They routinely obtain each patient's consent to disclose information to insurance companies or for other purposes according to a uniform standard set by the HIPAA Privacy Rule for certain health care providers.[210] Consent, then, is more manufactured than freely provided[211] as HIPAA provisions are circumvented by contract. A 2007 study estimated that employers, insurers, the criminal justice system, and other parties obtain some 25 million authorizations for patient records

[208] Bourgeois, et al., JAMIA (JOURNAL OF THE AMERICAN MEDICAL INFORMATICS ASSOCIATION), (2008).
[209] Goldstein, JOURNAL OF LAW, MEDICINE AND ETHICS, p. 28 (2010).
[210] Department of Health and Human Services United States Government, Office of the Secretary, 45 CFR Parts 160 and 164: Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule § 78 (January 25, 2013) section on "Consent" [45 CFR § 164.506]
[211] ANGWIN, Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance p. 217. 2014.

as a condition of employment, insurance, or public benefits. Usually the entire record is sent, leading to proposals to limit disclosure.[212]

2. *Informed*

Fundamental to the legal doctrine of informed consent internationally, including in the US, is that significant risks should be disclosed and understood before patients voluntarily consent to an intervention, and that permission should be obtained without coercion.[213]

Becoming informed is very difficult, even for professionals and experts. The many different laws, regulations, jurisdictions, agencies, institutional policies, and security practices involved with health data privacy are confusing, complex, and opaque. Moreover, information about them is scattered among various sources that are neither conveniently accessible nor easily intelligible. Yet patients need to be better informed to be able to make wise decisions about what they may wish to keep private, what they may wish to release, to whom and how they release it, and for what purposes. *Informed* consent requires being informed. As Laura A. Mamo, Dennis K. Brown, Holly C. Logan, and Katherine K. Kim pointed out at the 2013 Annual Symposium of the American Medical Informatics Association:

> Effective and transparent governance policies are needed to ensure public protection, build public trust and encourage patients to allow their health information to be aggregated and shared in [health information] networks.[214]

[212] Mark A. Rothstein & Meghan Talbot, *Compelled Authorizations for Disclosure of Health Records: Magnitude and Implications*, 7 AMERICAN JOURNAL OF BIOETHICS 38(March 2007).
[213] Goldstein, JOURNAL OF LAW, MEDICINE AND ETHICS, p. 28 (2010).
[214] Mamo, et al., Patient Informed Governance of Distributed Research Networks: Results and Discussion from Six Patient Focus Groups. 2013.

They also indicated the need to involve patients and members of the public so that patient perspectives are incorporated into governance practices. However, siloing various privacy considerations and regulations precludes an integrated view of health data policy governance in its entirety. Patients, practitioners, and policy makers need a more comprehensive holistic view. Creating or obtaining such a view places added burden on everyone: legislators, regulators, patients, practitioners, administrators, patient advocates, and those responsible for educating patients.

Whether or not individual patients choose a voluntary identifier or segment their health information according to sensitivity and accessibility, they should be aware of their options and consequences. They may reveal intimate personal information for one purpose without realizing that it then becomes available elsewhere and for other purposes or merged with other data about them to become even more potentially injurious.[215] Patients should know what can happen with data about them, what they can do to protect it, what the implications are for their care (e.g., restricting access to data may compromise care), for research, and for social benefit. They should know what the law does and does not allow. Laws, rules, regulations, institutional policies, and practices need to be streamlined, harmonized, and readily available and accessible, transparent, and easily understood. Governance, too, needs to be revisited in light of experience, so that it evolves as technologies, practices, and ethical considerations evolve.[216]

Within a hospital, in addition to the variety of clinical personnel caring for a patient, among the personnel with legitimate access to each person's records are

[215] Layman, HEALTH CARE MANAGER, (2003).
[216] Mamo, et al., Patient Informed Governance of Distributed Research Networks: Results and Discussion from Six Patient Focus Groups. 2013.

schedulers, clinic clerical personnel, and those who do the billing. Individuals also should know who has and has had access to data about them, but in a much more useful and accessible form than currently occurs by providing a voluminous audit trail of every access by each of these categories of personnel for every purpose related to a patient hospital stay.

Patients also need to know what is in their records, and have the ability to correct erroneous information. Though this might seem straightforward, experience with billing and credit errors suggests that it is not, even when needed corrections can be substantiated factually.[217] Here, though, there also is a matter of knowledge and interpretation. Patients may not understand the clinical language and notation in their records. Even if they do, it can be difficult to reconcile evaluations of what is and is not "erroneous." Further, clinicians may want to inform other clinicians about the patient, but may not want the patient to have access to that information, believing that it could be misinterpreted, unduly contested, or deleterious to the patient (for example, a poor prognosis that may affect a patient's attitude and hence response to treatment). Knowing that patients will see their records can compromise their care if such information is omitted. Record information already may be circumscribed in order to avoid litigation, or adjusted for reimbursement purposes. Having records be even more open can lead to their being less informative for good care. This also can reduce the value of patient record data for secondary uses.

[217] Layman, HEALTH CARE MANAGER, (2003).

V. CONCLUSION

Many different aspects of law are relevant to health data privacy. The context for health data privacy involves various values, norms, and legal considerations and issues range from privacy to speech to ownership and property to public good to professional values and practice. Possible approaches to mitigating privacy threats also can enhance ethical behavior, patient autonomy, and informed consent while allowing for individual liberties, and both private and public benefits of access to health data and information. Some proposals to address privacy threats may block these benefits. Some, like the *Sorrell* decision, do not balance important values adequately. Some, such as "informed consent" and de-identification, may be believed to protect privacy when they do not.

Potential solutions are not clear-cut. Privacy laws like HIPAA are thought simultaneously to hinder access to data and allow too much access. Repeated initiatives, rule-making revisions, and calls for new legislation suggest the difficulty of achieving a satisfactory balance.[218] Transparency and consistency also have been elusive. Like the ONC 2008 Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information's call for transparency and consistency,[219] the American Medical Informatics Association, too, issued recommendations calling for increased transparency and public awareness of benefits, challenges, and policies pertaining to secondary use, as well as a focus on data control and uses rather than ownership. Internationally, the International Medical Informatics Association built on this work when over 100 delegates from governments, academia, industry, and patient

[218] Evans, HARVARD JOURNAL OF LAW & TECHNOLOGY, pp. 70, 113, 72-73 (2011).
[219] United States Government, Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information pp. 2, 7 2008.

groups met in 2012 for the European Summit on Trustworthy Reuse of Health Data. Delegates from the 21 countries represented also called for regulation, oversight, harmonizing policy across the EU, and fully informed patients.[220]

A. Transparency, Harmonization, and Simplicity Needed

Yet opaqueness and misconception abound, exacerbated by multiple laws and regulations in multiple jurisdications, and obscure proposed frameworks and recommendations. In the US, the Health Information Security and Privacy Collaboration (HISPC), established in 2006 by the Department of Health and Human Services, completed the last of its phases in 2008. HISPC highlighted different state policies and developed toolkits for harmonizing them,[221] but the task remains. The US, too, is unusual in its regulatory mix of privacy, property, free speech, and public good. Perhaps new insights can be gained by examining each of these legal doctrines in light of the others through the lens of health care data privacy. Here, though, the main point is that the mix also is generally confusing, sometimes at cross-purposes, and so complex as to make piecemeal policy approaches likely ineffective at best. Changing any one part may have unforeseen consequences on the entire system, making it difficult to adequately assess risks and benefits of technological or policy fixes. It is difficult to adequately allow for release of data for public good and beneficent purposes while sufficiently protecting privacy. It is harder still to balance these two values with a mish-mosh of professional

[220] Charles Safran, et al., *Toward a National Framework for the Secondary Use of Health Data: An American Medical Informatics Association White Paper* 14 JAMIA (JOURNAL OF THE AMERICAN MEDICAL INFORMATICS ASSOCIATION) 1(2007);A. Geissbuhler, et al., *Trustworthy Reuse of Health Data: A Transnational Perspective*, 83 INTERNATIONAL JOURNAL OF MEDICAL INFORMATICS 1(2013).
[221] United States Government, Federal-State Privacy & Security Collaboration (HISPC);United States Government, Health Information Security & Privacy Collaboration (HISPC).

norms, free speech protections and exceptions, public health reporting requirements, and common understanding of various laws, regulations, and practices.

That balance is precarious. Taken together, various policy initiatives and technological advances point towards increasing data collection, sharing, and use for multiple purposes, often without permission, knowledge, or public understanding. Many patients do not know what can be done with their data, but keeping them ignorant is not the way to address this concern. The current intricate, fragmented state of health data governance requires dedicated expertise to understand and apply. Regulators and legislators may well lack expertise in the entire landscape; certainly patients and clinicians do. Yet, patients and clinicians *are* the public. Transparency, clarity, and public discussion is needed, for good and for ill, so that policy can better reflect a democratic balancing of the values involved.

This review begins to explicate the intricate interconnections to make them more transparent. The goal is to increase transparency and understanding of the current state of affairs so as to stimulate broader and more holistic thinking and encourage democratic deliberation. This can result in more integrated new legal tools to balance the important values that come into play when considering health data privacy.

B. Flexibility, Not Rigid Rules, Needed

Consensus is growing that US privacy law has not caught up with communicating medical information through national health information networks, social networking, mobile health, big data for research and innovation, genomics and biobanking, re-

identification science,[222] and minors' access to electronic records and health applications. Law likely cannot catch up with burgeoning data collection, data aggregation, and data mining activities, nor with technological advance, let alone adequately anticipate it. Until recently, the Hippocratic Oath and common law tort system governed health privacy. Although common law tort does not adequately address health data privacy,[223] the room it builds in for interpretation on a case-by-case basis is suggestive. Principles that can be applied in ways that evolve with changing norms and technologies could better serve than rigid rules. Rule-based requirements can provide a floor for proper behavior, but compliance may too easily turn into a ceiling for ethical behavior. Rigid rules also can thwart good policy and wise legal decisions that take account of the kind of data, the uses to which it is put, the balancing of values involved, social norms, individual rights, and broad ramifications for public welfare. Some data uses are more beneficial than others, and some data users more in line with public expectations for good than others.

Various privacy experts and legal scholars have proposed privacy bills of rights and guiding principles to protect privacy.[224] They overlap with frameworks and recommendations designed to promote secondary health data use in recognizing that

[222] Greenberg, et al., HEALTH AFFAIRS, (2009);Patricia Sanchez Abril & Anita Cava, *Health Privacy in a Techno-Social World: A Cyber-Patient's Bill of Rights*, 6 NORTHWESTERN JOURNAL OF TECHNOLOGY AND INTELLECTUAL PROPERTY 244(2008);Reid Cushman, et al., *Ethical, Legal and Social Issues for Personal Health Records and Applications*, 43 JOURNAL OF BIOMEDICAL INFORMATICS S51(2010);INSTITUTE OF MEDICINE, Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research. 2009;Presidential Commission for the Study of Bioethical Issues, Privacy and Progress in Whole Gene Sequencing. October 2012;Ohm, UCLA LAW REVIEW, (2010).

[223] Abril & Cava, NORTHWESTERN JOURNAL OF TECHNOLOGY AND INTELLECTUAL PROPERTY (2008).

[224] Abril, Selling Privacy. this volume;LORI ANDREWS, I KNOW WHO YOU ARE AND I SAW WHAT YOU DID: SOCIAL NETWORKS AND THE DEATH OF DATA PRIVACY (Free Press. 2011);ANGWIN, Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance. 2014;HOLTZMAN, Privacy Lost: How Technology is Endangering Your Privacy. 2006.

individuals should be aware of how data about them is collected and used and have a say in it.

C. Technological Solutions and Social Research Needed

While law and technology may not keep pace with each other, technological advances also offer approaches that can enhance individuals' knowledge and consent about data use so that those closest to providing and generating data know, and agree to, its use, and, in some way, benefit or are compensated for it. Better alternatives to identification and de-identification; means of tracking data through not just secondary, but tertiary and subsequent aggregation and use; granular level control; improved data security; and returning benefit to data originators all are under development.

Health data universally is treated as special.[225] It is different from other data in that individuals reveal it for intimate purposes, and it then can be used in unexpected ways. It is subject to legal requirements for disclosure to intermediaries with fiduciary duties, including confidentiality and privacy protection, as well as obligations for public good.

Yet "privacy" and "public welfare" are dynamic ideas.[226] Privacy is not simply a matter of identity and control. Nor are big data, data mining, and secondary use merely a matter of unconstrained market forces. Neither technological nor legal research should focus solely on the data per se. Weighing privacy and numerous beneficial uses for data requires understanding ideas of privacy, proper data use, and value of data aggregation products as they vary over time and place. Empirical social research, including

[225] Kaplan, CAMBRIDGE QUARTERLY OF HEALTHCARE ETHICS, (in review).
[226] Daniel J. Solove, *A Taxonomy of Privacy*, 154 UNIVERSITY OF PENNSYLVANIA LAW REVIEW (2006).

ethnographic study of personal and societal norms for balancing different values, can contribute to wiser policy and open public debate based on messy, human and humane interconnected social, psychological, institutional, legal, and ethical considerations.[227]

Harms and benefits can be judged best through transparency and accountability leading to individual awareness, public discussion, and considered judgment. That way, personal as well as societal decisions can be made on more informed and thoughtful grounds.

[227] Ohm, UCLA LAW REVIEW, p. 1761 (2010).