Vanderbilt Journal of Entertainment & Technology Law

Volume 19
Issue 2 *Issue 2 - Winter 2016*

Article 1

2016

Health Information Ownership: Legal Theories and Policy Implications

Lara Cartwright Smith

Elizabeth Gray

Jane H. Thorpe

Health Information Ownership: Legal Theories and Policy Implications

*Lara Cartwright-Smith, Elizabeth Gray, and Jane Hyatt Thorpe**

ABSTRACT

This Article explores the nature and characteristics of health information that make it subject to federal and state laws and the existing legal framework that confers rights and responsibilities with respect to health information. There are numerous legal and policy considerations surrounding the question of who owns health information, including whether and how to confer specific ownership rights to health information. Ultimately, a legal framework is needed that reflects the rights of a broad group of stakeholders in the health information marketplace, from patients to providers to payers, as well as the public's interest in appropriate sharing of health information.

TABLE OF CONTENTS

* The authors thank Jennifer Ansberry, JD, MPH, Maanasa Kona, JD, LLM, and Resa Cascio, JD, LLM, for their valuable research contributions to this paper.

I. INTRODUCTION

The concept of owning information invokes thoughts of property and profit. Property ownership means that the owner may use the property as he or she wishes. The owner may modify it, destroy it, transfer it by sale or donation, and permit others to use it according to his or her terms, among other things. However, ownership of health information is less clear. In some cases, the law ascribes clear ownership rights over part or all of a health record, but in other cases, information may be used by a number of parties without clear ownership rights, even for the person who is the subject of the information. Stakeholders at the state and federal levels struggle with these issues as more uses for health information are developed, technological advancements enable greater mobility, and accessibility and ownership of health information becomes more significant, yet the answer to the ownership question remains unclear. Numerous potential solutions to the health information ownership question exist. One option would be to allow each person to own the information held in her personal medical records, even if another person created the record. Another might be to give ownership of the patient's information to the healthcare provider who recorded that information. Or perhaps the many rights surrounding health information amount to ownership or make ownership irrelevant in a highly regulated environment.

This Article will explore the existing laws that confer rights and responsibilities with respect to health information, discuss various legal theories of ownership that could apply to health information, and consider the implications of applying them in the current health information policy landscape. In Part I, the Article will explore the nature of health information and the various

characteristics that may make it subject to federal and state regulation. In Part II, the Article will explore the legal and policy landscape surrounding health information regulation, considering why ownership of health information is of particular relevance now. In Part III, the Article will discuss the various laws and legal theories that apply to health information, giving full ownership rights or rights to access, use, and control it. Finally, in Part IV, the Article will discuss policy considerations surrounding the question of health information ownership, including the implications of conferring specific ownership rights over health information. While there is no one solution to the question of health information ownership, given the complex bundle of overlapping rights under state and federal laws that apply, the Article highlights the policy considerations that weigh against treating health information exclusively as property. Ultimately, a legal framework is needed that reflects the rights of the many stakeholders in the health information marketplace, from patients to providers to payers, as well as the public's interest in the appropriate sharing of health information.

II. THE UNIQUE NATURE OF HEALTH INFORMATION

In some ways, health information is similar to other types of personal information: it contains unique details about a particular individual. Like financial information, it can be used improperly to discriminate against an individual and, like private photos or personal thoughts, it can be embarrassing if disclosed publicly. In other ways, health information is unique. For example, disclosing health information to others is necessary both for proper medical treatment of the person who is the subject of the information and also for the business purposes of potentially many different people or entities, such as doctors for treatment and billing purposes and health insurance companies for payment purposes. Health information may be relevant to third parties, as in the case of communicable diseases or inheritable genetic conditions. Before considering how laws apply to health information, it is important to define what health information is and explain what makes it subject to regulation.

A. Definitions of Health Information

The most basic definition of health information is any information concerning the health of at least one person.[1] When considering law and policy, however, the regulated information must be specifically defined. For example, the physical medical record, the content of the record, biological samples taken from a person, and data aggregated from many different people can all be considered "health information," but they may be treated differently under the law. Not all health information is subject to regulation, and information that is regulated may be subject to laws that overlap or directly contradict each other.[2]

1. Health Information Characteristics

There is no single legal framework governing "health information;" rather, information may be subject to one or more laws and/or regulations depending on the information's specific characteristics. For purposes of applying legal protections and restrictions, health information can be defined based on a variety of characteristics, such as its content, its source, and its form. These characteristics are not mutually exclusive, so that multiple overlapping rights and obligations may apply to a particular record or piece of information, complicating the question of ownership.

Content focuses on the substance of the information. The American Health Information Management Association (AHIMA) defines health information as "the data related to a person's medical history, including symptoms, diagnoses, procedures, and outcomes."[3] This content-based definition is perhaps the broadest possible way to describe health information, as there are no limitations related to its source, form, or subject. The Office for the National Coordinator for Health Information Technology (ONC) uses a slightly narrower definition, recognizing health information as information about an individual's medical condition or history where the information can be used to identify an individual.[4] Indeed, identifiability is a critical

---

1. *What Is Health Information?*, AM. HEALTH INFO. MGMT. ASS'N, http://www.ahima.org/careers/healthinfo [https://perma.cc/8NV9-5VL4] (last visited Oct. 27, 2016).

2. *See, e.g.*, Beverly Cohen, *Reconciling the HIPAA Privacy Rule with State Laws Regulating Ex Parte Interviews of Plaintiffs' Treating Physicians: A Guide to Performing HIPAA Preemption Analysis*, 43 HOUS. L. REV. 1091, 1105–07 (2006).

3. *What Is Health Information?*, *supra* note 1.

4. *What Is "Health Information" for Purposes of the Mobile Device Privacy and Security Subsection of HealthIT.gov?*, HEALTHIT.GOV, https://www.healthit.gov/providers-

component underlying most federal and state laws and regulations governing health information.[5]

Health information can also be categorized by its source, which refers to the person or the entity that initially collected the information, as well as the setting in which the information was generated or collected. Sometimes, the individual subject of the information or the individual's family members may be the information collector. Health information may also be collected by entities providing care, paying for care,[6] performing public health functions, conducting research, or delivering other services that may incidentally involve healthcare information, such as those provided by prisons, schools, or universities. Laws focusing on the source alone may protect information only in its collected form, meaning the information itself is not protected but the list, database, or other collected information format is protected, as in the case of a business record, such as a patient list. Moreover, these laws may only protect information held by a certain party, such as a substance abuse treatment facility.

Lastly, the form of medical information indicates the method by which information is collected and stored. Health information may be tangible, such as a tissue sample, or intangible, such as an individual's memory about his or her health or an individual's genetic information. Intangible health information becomes tangible once it is recorded or extracted from the individual. Tangible health information is stored digitally or on paper, or as preserved physical samples, such as those kept in biobanks. Some legal protections and restrictions apply to health information by virtue of its form or medium, such as laws granting ownership of a medical record to the healthcare provider that holds it.[7] In that case, the information is protected health information because it is contained in a medical record, but the protection may not follow the information once it leaves the medical record.

---

professionals/faqs/what-health-information-purposes-mobile-device-privacy-and-security-sub [https://perma.cc/72JC-NQT2] (last visited Oct. 27, 2016).

5. *See, e.g.*, Health Insurance Portability and Accountability Act (HIPAA) of 1996 § 1177, 42 U.S.C. § 1320d(6) (2012) (defining an "offense" by referring four times to "identifiable health information" or "health identifier").

6. Health insurers, for example, are entities that pay for care, though other entities may be involved in payment. This would include the federal government when it directly pays providers to deliver care to a specific population for which it has responsibility, such as veterans.

7. *E.g.*, S.C. CODE ANN. § 44-115-20 (West 2016) (a physician is the owner of medical records that were made in treating a patient and are in his or her possession, as well as the owner of records transferred to him or her concerning prior treatment of the patient); V.A. CODE ANN. § 54.1-2403.3 (West 2016) (medical records maintained by any healthcare provider are the property of the healthcare provider or the provider's employer).

2. Health Information Types

When considering ownership and regulation of health information, it is important to understand what may be owned or regulated. Laws may regulate only a certain type of health information, as in the case of state laws granting ownership of genetic information to the subject of the information,[8] which can complicate matters if a certain record contains multiple types of information. It is important to understand the terms used by policymakers and stakeholders to delineate different types of information because these definitions may determine what rights and responsibilities apply to that information.

The medical and health policy communities have adopted several commonly used terms to define certain types of health information. The term "clinical data," for example, refers to health information collected in a clinical setting by a provider from a patient.[9] Clinical data may include patient histories, lab results, x-rays, or provider notes.[10] Clinical data is stored in electronic health records (EHRs) and electronic medical records (EMRs), paper-based medical records, and clinical trial records.[11]

"Administrative data" is information collected from patients by healthcare stakeholders, such as providers and payers, in connection with the patient's care or payment for care.[12] Administrative data is used primarily for business purposes like record keeping or billing and may include patient demographic and insurance information.[13]

---

8. *E.g.*, ALASKA STAT. ANN. § 18.13.010 (West 2016) ("DNA sample and the results of a DNA analysis are the exclusive property of the person sampled or analyzed."); COLO. REV. STAT. ANN. §§ 10-3-1104.6, -1104.7 (West 2016) (indicating genetic information is the property of the individual); FLA. STAT. § 760.40 (2016) ("[R]esults of . . . DNA analysis, whether held by a public or private entity, are the exclusive property of the person tested."); GA. CODE ANN. § 33-54-1 (West 2016) ("Genetic information is the unique property of the individual tested . . . ."); LA. STAT. ANN. §§ 22:1023, 40:2210 (2016) ("[I]nsured's or enrollee's genetic information is the property of the insured or enrollee . . . .").

9. *Data Resources in the Health Sciences*, U. WASH., http://guides.lib.uw.edu/hsl/data/findclin [https://perma.cc/3TXB-EQT5] (last visited Nov. 2, 2016).

10. THE OFFICE OF THE NAT'L COORDINATOR FOR HEALTH INFO. TECH., COMMON CLINICAL DATA SET 2 (2015), https://www.healthit.gov/sites/default/files/commonclinicaldataset_ml_11-4-15.pdf [https://perma.cc/G37Q-LPP2]; *see also What Is Health Information?*, *supra* note 1.

11. *See, e.g.*, INST. OF MED., CLINICAL DATA AS THE BASIC STAPLE OF HEALTH LEARNING: CREATING AND PROTECTING A PUBLIC GOOD: WORKSHOP SUMMARY 45 (National Academies Press 2010), http://www.ncbi.nlm.nih.gov/books/NBK54296/ [https://perma.cc/9VDT-SPY9].

12. *Id.* at 100.

13. *Id.* at 126.

Administrative data may be found in EHRs and EMRs, paper-based medical records, and practice management systems.[14]

Finally, "patient-generated health data" (PGHD) is "health-related data created, recorded, or gathered by or from patients" or patients' family members or other caregivers in non-clinical settings.[15] PGHD may be generated or collected by mobile apps, personal health records (PHRs), and home health equipment that does not automatically transmit to a provider, such as a blood glucose monitor.[16]

Other common terms refer to the content of the information. "Biospecimens" are physical materials taken from an individual, including tissue, blood, urine, or other human-derived material,[17] as well as the information derived from the material, such as extracted DNA.[18] A biospecimen can comprise subcellular structures, cells, tissue, organs, blood, gametes (sperm and ova), buccal swabs, embryos, fetal tissue, exhaled breath condensate, and waste (urine, feces, sweat, hair and nail clippings, shed epithelial cells, and placenta).[19] "Genetic information" refers to information about an individual's genetic makeup and the genetic makeup of an individual's family members, as well as information about the manifestation of a disease or disorder in an individual's family members, such as a family medical history.[20] Both biospecimens and genetic information may be defined and regulated according to their form as well as content, as in the case of a rule applying only to the physical sample taken from a body.

---

14. *Id.* at 69.

15. *Patient-Generated Health Data*, HEALTHIT.GOV, https://www.healthit.gov/policy-researchers-implementers/patient-generated-health-data [https://perma.cc/6QHJ-T7MT] (last visited Oct. 27, 2016).

16. *Id.*

17. OFFICE OF BIOREPOSITORIES AND BIOSPECIMEN RESEARCH ET AL., NCI BEST PRACTICES FOR BIOSPECIMEN RESOURCES 59 (2011), http://biospecimens.cancer.gov/bestpractices/2011-NCIBestPractices.pdf [https://perma.cc/WAH2-3WQS] (last visited Oct. 27, 2016).

18. NAT'L INST. OF HEALTH, GUIDELINES FOR HUMAN BIOSPECIMEN STORAGE AND TRACKING WITHIN THE NIH INTRAMURAL RESEARCH PROGRAM 3 (2013), https://oir.nih.gov/sites/default/files/uploads/sourcebook/documents/ethical_conduct/guidelines-biospecimen.pdf [https://perma.cc/QU9E-CDR4] (last visited June 28, 2016).

19. OFFICE OF BIORESPOSITORIES AND BIOSPECIMEN RESEARCH ET AL., *supra* note 17, at 59; Jonathan S. Miller, *Can I Call You Back? A Sustained Interaction with Biospecimen Donors to Facilitate Advances in Research*, 22 RICH. J.L. & TECH. 1 (2015).

20. Adapted from the definition of "genetic information" set forth in GINA Title I. *See* Genetic Information Nondiscrimination Act of 2008 § 201, 42 U.S.C. § 2000ff (2012).

III. THE LEGAL AND POLICY LANDSCAPE FOR HEALTH INFORMATION

In recent years, evolving technology has made health information more accessible and more meaningful to individual consumers, providers, payers, and researchers. Value-based purchasing policies have created incentives for providers to collect, analyze, and report more data about individual patients.[21] Wearable devices collect and record health information such as activity, heart rate, and blood sugar level, enabling individuals to monitor, and thus better manage their own health.[22] These and other self-management tools, such as Consumer Health Informatics (CHI) applications, are particularly useful for patients with chronic conditions. For example, researchers have found that the use of such tools can positively affect health outcomes in the cases of breast cancer, alcohol abuse, smoking cessation, obesity, diabetes, mental health, and asthma.[23] CHI applications also include electronic PHRs and patient portals, some of which function as peer interaction systems by which users can communicate with others who have similar conditions.[24] Individuals may also choose to share personal health information freely online through websites specifically designed to aggregate information from patients, such as PatientsLikeMe,[25] as well as on social media.[26] Providers even share patient information on social media (with privacy protections in place), essentially crowdsourcing medical diagnosis and treatment.[27]

---

21. *See, e.g.*, *Linking Quality to Payment*, MEDICARE.GOV, https://www.medicare.gov/hospitalcompare/linking-quality-to-payment.html [https://perma.cc/D5FK-XVJQ] (last visited Oct. 27, 2016).

22. *See* John Comstock, *CES 2016: Running List of Health and Wellness Devices*, MOBIHEALTH NEWS (Jan. 6, 2016), http://mobihealthnews.com/content/ces-2016-running-list-health-and-wellness-devices [https://perma.cc/U4B3-WSJ2].

23. JOHNS HOPKINS UNIV. EVIDENCE-BASED PRACTICE CTR., IMPACT OF CONSUMER HEALTH INFORMATICS APPLICATIONS, at v (2009), http://www.ahrq.gov/downloads/pub/evidence/pdf/chiapp/impactchia.pdf [https://perma.cc/8H5Q-L9KR].

24. Bisk, *Defining the Concept of CHI, and Exploring How It Is Democratizing Healthcare for Patients*, USF HEALTH, http://www.usfhealthonline.com/resources/key-concepts/consumer-health-informatics/#.V2xi0jkrK2x [https://perma.cc/5TET-T7GU] (last visited Nov. 2, 2016).

25. *Live Better, Together!*, PATIENTSLIKEME, https://www.patientslikeme.com [https://perma.cc/R66M-K49F] (last visited Nov. 2, 2016).

26. *See* Patricia Sanchez Abril & Anita Cava, *Health Privacy in a Techno-Social World: A Cyber-Patient's Bill of Rights*, 6 NW. J. TECH. & INTELL. PROP. 244, 247–48 (2008).

27. *See, e.g.*, Alex Mohensi, *Doc APProvED: 'Instagram for Doctors,'* 36 EMERGENCY MED. NEWS 22 (2014), http://journals.lww.com/em-news/Fulltext/2014/04000/Doc_APProvED___Instagram_for_Doctors_.15.aspx [https://perma.cc/2B9P-GKDX]; *see also* Esther K. Choo et al., *Twitter as a Tool for*

Technology is also enabling the use of "big data" drawn from health records, which promises to improve the quality of healthcare, allow a greater understanding of patient and provider behaviors, and even find new treatments for conditions like cancer. "Big data" refers to very large datasets containing vast quantities of a variety of information types that arrive and must be processed quickly.[28] It also invites concern about commercial uses by information resellers and marketers, as well as nefarious uses like identity theft and discrimination.[29] Cybersecurity experts estimate that a stolen medical record is worth ten times more than stolen credit card information because of medical information's greater profit potential.[30] In the legal data market, health information is collected and sold to companies such as credit bureaus, advertisers, and investigators. An appendix to a 2013 Government Accountability Office (GAO) report on information resellers listed characteristics that the credit reporting company Experian used to identify individuals to include in marketing lists it created and provided to its clients.[31] The characteristics included an extensive list of heath conditions, including potentially sensitive conditions like Alzheimer's disease, cancer, clinical depression, diabetes, erectile dysfunction, epilepsy, irritable bowel syndrome, menopause, Parkinson's disease, and prostate problems.[32] The business of gathering health data for commercial purposes can be significant; for example, IMS Health, one of the leading providers of such intelligence, reported approximately $1.5 billion in annual revenue for its information segment in each of the last five years.[33] IMS Health draws information from a variety of sources, including over 500 million patient medical records and over fourteen million healthcare providers and organizations (Figure 1). These millions of

---

Communication and Knowledge Exchange in Academic Medicine: A Guide for Skeptics and Novices, 37 MED. TCHR. 411, 413 (2014).

28. Bernard Marr, *Big Data a Game Changer for Healthcare*, FORBES (May 24, 2016, 1:55 AM), http://www.forbes.com/sites/bernardmarr/2016/05/24/big-data-a-game-changer-in-healthcare/#28efa52f3c75 [https://perma.cc/UYA3-MJKC].

29. *Id.*

30. Caroline Humer & Jim Finkle, *Your Medical Record Is Worth More to Hackers Than Your Credit Card*, REUTERS (Sep. 24, 2014, 2:24 PM), http://www.reuters.com/article/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924 [https://perma.cc/X7QQ-4SVD].

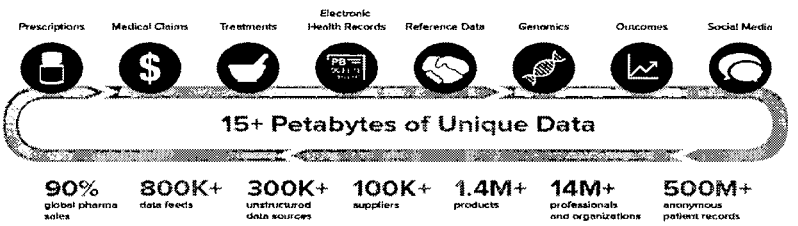
31. U.S. GOV'T ACCOUNTABILITY OFFICE, INFORMATION RESELLERS: CONSUMER PRIVACY FRAMEWORK NEEDS TO REFLECT CHANGES IN TECHNOLOGY AND THE MARKETPLACE 52–53 (2013), http://www.gao.gov/assets/660/658151.pdf [https://perma.cc/U8JQ-SZZZ].

32. *Id.* at 53.

33. IMS HEALTH HOLDINGS, INC., 2015 ANNUAL REPORT 38 (2015), http://s2.q4cdn.com/521378675/files/doc_downloads/2016/IMS_2015_Annual-Report_Final_Final.pdf [https://perma.cc/V35F-JGCT]. $1.5 billion per year is a lot of money to make just from aggregating and selling health data.

records and pieces of patient information are combined into a dataset that is sold as a product to a variety of users.[34] These practices illustrate how one's health information may be commodified—that is, turned into a product for someone else's profit. In this landscape, legal ownership of information becomes a critical question.

Figure 1: Data combined by IMS Health for its "Market Insights" health information business sector[35]



Courts are confronting these new data uses and considering where they fit in existing legal structures, such as intellectual property law. Two cases decided by the US Supreme Court in recent years illustrate the challenge of sorting out legal rights where corporate interests in personal information are concerned.[36] In 2013, in *Ass'n for Molecular Pathology v. Myriad Genetics, Inc.*, (*Myriad*), the Court considered a challenge to a patent held by Myriad Genetics on genetic tests for certain genes that increase the risk of breast and ovarian cancer.[37] The tests involved isolating natural DNA strands and creating synthetic complementary DNA that mirrored the original isolated strands with slight alterations.[38] The Court ruled that synthetically created complementary DNA is patentable, while isolated natural DNA is not.[39] Although the case appeared to be a relatively straightforward application of intellectual property law, granting corporations a protectable property interest in material derived from an individual's DNA could have far-reaching implications.[40] If a corporation can create a commodity from DNA, selling it and preventing others from making competing products,

34. *Id.*

35. *Global, National and Subnational Insights*, QUINTILESIMS, http://www.imshealth.com/en/solution-areas/market-insights [https://perma.cc/NG8J-YY56] (last visited Nov. 12, 2016).

36. *See generally* Ass'n for Molecular Pathology v. Myriad Genetics, Inc., 133 S. Ct. 2107 (2013); Sorrell v. IMS Health Inc., 564 U.S. 552 (2011).

37. *Myriad*, 133 S. Ct. at 2110–11.

38. *Id.* at 2111.

39. *Id.*

40. *Id.* at 2113, 2120.

other activities that amount to ownership of a person's biological material are not far off.

In 2011, the Court considered the constitutionality of legal restrictions on the use of collected personal information in *Sorrell v. IMS Health Inc.*[41] *Sorrell* dealt with a common marketing practice, wherein pharmacies collect prescriber-identifying information when processing prescriptions and sell this information to "data miners."[42] Data miners use this information to produce reports on prescriber behaviors, de-identified with respect to patients but identifying the prescribing physician, which they lease to pharmaceutical manufacturers.[43] Manufacturers then employ "detailers," commonly known as pharmaceutical sales representatives or "drug reps," who use the reports to strategically market and promote their drugs to physicians.[44]

The Vermont law in question prohibited pharmacies from selling or disclosing prescriber-identifying information for marketing purposes without the prescriber's consent and further prohibited pharmaceutical manufacturers and marketers from using prescriber-identifiable information for sales marketing and promotion practices.[45] The majority used a First Amendment free speech analysis to strike down the statute because it imposed a burden on the protected speech of the regulated pharmacies, manufacturers, and marketers, including plaintiff IMS Health, thereby restricting communication.[46]

The dissent, however, argued that Vermont's law regulated commercial activity rather than speech and thus imposed no significant burden on free speech.[47] Because the majority interpreted restrictions on the use of health information as a free speech violation rather than regulation of health information use and exchange for commercial purposes, the Court may have made it very difficult for legislators to regulate the activity of collecting and disseminating personal information, including health information, for profit. With respect to ownership of health information, it may not be possible after *Sorrel* to give ownership rights over health information to a particular individual or entity through statute, regulation, or common

41. *Sorrell*, 564 U.S. at 557.

42. *Id.* at 558.

43. *Id.*

44. *Id.*

45. VT. STAT. ANN. tit. 18, § 4631(d) (West 2010), *invalidated by* Sorrell v. IMS Health, Inc., 564 U.S. 552 (2011).

46. *Sorrell*, 564 U.S. at 563–65.

47. *Id.* at 591–92.

law because another party may be able to claim a constitutional right to use the information for their own purposes.

The legal status of health information is the subject of robust debate and the legal landscape is in flux. Scholars debate what legal framework—whether property law, tort law, or constitutional protections of free speech—should apply to health information.[48] Members of the public debate the ethics of using personal health information without consent, as in the case of Henrietta Lacks, whose cancer cells were taken, replicated, and later commodified for valuable research for decades without her consent and without her family's knowledge.[49] Policymakers debate the proper balance between the potential benefits of data derived from personal information and the need to protect privacy and other rights.[50]

At the federal level, ONC is leading efforts to define the rules of the road for the use and exchange of health information. For example, ONC released a set of guiding principles related to health information exchange governance in 2013, which were designed to serve as a common framework for organizations engaging in the data exchange for healthcare purposes.[51] In 2015, ONC released the Federal Health IT [Information Technology] Strategic Plan 2015–2020,[52] which highlights the importance of protecting health information privacy and security in order to support and advance "widespread use of all forms of health IT."[53] According to the Plan, clarifying federal and state laws governing the privacy and security of health information is a key component of promoting greater adoption of health information technology.[54]

---

48. *See, e.g.*, Barbara J. Evans, *Much Ado About Data Ownership*, 25 HARV. J.L. & TECH. 70, 74 (2011) (arguing against propertization of health data); Bonnie Kaplan, *Selling Health Data: De-Identification, Privacy, and Speech*, 24 CAMBRIDGE Q. HEALTHCARE ETHICS 256 (2015) (comparing property and free speech framework and suggesting tort law as alternative); Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2056 (2004) (criticizing tort law as comprehensive framework and suggesting property law as proper framework).

49. *See generally* REBECCA SKLOOT, THE IMMORTAL LIFE OF HENRIETTA LACKS (Random House 2010).

50. *See, e.g.*, Marc A. Rodwin, *Patient Data: Property, Privacy & the Public Interest*, 36 AM. J.L. & MED. 586, 617 (2010).

51. THE OFFICE OF THE NAT'L COORDINATOR FOR HEALTH INFO. TECH., GOVERNANCE FRAMEWORK FOR TRUSTED ELECTRONIC HEALTH INFORMATION EXCHANGE 1 (2013), https://www.healthit.gov/sites/default/files/GovernanceFrameworkTrustedEHIE_Final.pdf [https://perma.cc/8WX9-DBFT].

52. THE OFFICE OF THE NAT'L COORDINATOR FOR HEALTH INFO. TECH., FEDERAL HEALTH IT STRATEGIC PLAN 2015–2020, at 4 (2015), https://www.healthit.gov/sites/default/files/9-5-federalhealthitstratplanfinal_0.pdf [https://perma.cc/BSG4-943T].

53. *Id.*

54. *Id.* at 43.

IV. LEGAL THEORIES OF INFORMATION OWNERSHIP

In law, ownership generally means legal title to something combined with the exclusive right to possess it.[55] Legal title gives the owner a variety of rights, including rights to control, use, profit from, dispose of, and prevent others from using the thing that is owned.[56] This concept is straightforward in the case of an object or piece of real estate. In the case of health information, ownership is usually less clear. A patchwork of laws grants various rights and obligations with respect to health information and medical records, including privacy, confidentiality, and the rights to access, amend, and direct the transfer of one's health information.[57] Some rights come from specific laws and regulations, while others are derived from broader principles of law, like privacy and property.[58]

Some states have laws granting specific ownership over medical records or health information either to the healthcare provider or, in New Hampshire, to the individual who is the subject of the information.[59] Some of these state laws use the term "own" or "owner," while others use the term "property."[60] In Wyoming, the law refers to the physical conveyance for the information, giving the provider ownership of "the paper, microfilm, or data storage unit upon which the patient's information is maintained [and stating that patients] do not have a right to possess the physical means by which the information is stored," although they must be given access to "pertinent information."[61] In New Hampshire, the state's Patients' Bill of Rights law states: "[m]edical information contained in the medical records at any facility licensed under this chapter shall be deemed to be the property of the patient."[62] This law is unique among states and, since providers retain a property interest in their business records, it is not clear how the conflicting property rights of patients and providers would be resolved in case of a dispute. There are also cases finding that medical records are the property of the healthcare

55. *Ownership*, BLACK'S LAW DICTIONARY (10th ed. 2014).

56. *E.g.*, Jane B. Baron, *Property as Control: Case of Information*, 18 MICH. TELECOMM. & TECH. L. REV. 367, 384 (2012).

57. *E.g.*, Mark A. Hall, *Property, Privacy, and the Pursuit of Interconnected Electronic Medical Records*, 95 IOWA L. REV. 631, 649–50 (2010).

58. *See id.*

59. *Who Owns Medical Records: 50 State Comparison*, HEALTH INFO. & L., http://www.healthinfolaw.org/comparative-analysis/who-owns-medical-records-50-state-comparison [https://perma.cc/3H2N-XNF5] (last visited Nov. 12, 2016).

60. *See id.*

61. 024-052 WYO. CODE R. § 003 (LexisNexis 2016).

62. N.H. REV. STAT. ANN. § 151:21 (2016).

provider who created them, even where there is no statute or regulation to that effect.[63]

While ownership is significant, it may not determine who can do what with health information. Patients may have rights with respect to their medical records under some federal privacy laws and regulations.[64] Many states have specific laws addressing how providers must maintain, protect, and dispose of records, as well as laws giving patients, providers, and others access to medical records, regardless of ownership status.[65] The following discussion addresses the legal theories that could potentially serve as the basis for ownership of health information, including property law, intellectual property law, and privacy law.

A. Property law

In the United States, there is no recognized property interest in one's own personal information.[66] There may be property interests in specific types of information, as in the case of medical information under the New Hampshire law[67] referenced above, or in the physical container that houses the information, such as a computer or diary.[68] When information about individuals is compiled from public data or by an entity with legal access to the information, such as a credit card company, it can be sold without the permission of the subjects of the information, who are not entitled to any compensation.[69] Information about customers, such as mailing lists, can be distributed alongside real property when a business is transferred.[70]

Property can be defined broadly as "any interest in an object, whether tangible or intangible, that is enforceable against the

63. *See, e.g.*, Holtkamp Trucking Co. v. David J. Fletcher, M.D., L.L.C., 932 N.E.2d 34, 43 (Ill. 2010) (holding that medical records were physician's property); McGarry v. J.A. Mercier Co., 262 N.W. 296, 297–98 (Mich. 1935) (holding that x-ray negatives were the property of the physician who made them, not the patient).

64. Hall, *supra* note 57, at 649–50.

65. *See States*, HEALTH INFO. & L., http://www.healthinfolaw.org/state [https://perma.cc/6DWF-FVSR] (last visited Nov. 13, 2016).

66. Vera Bergelson, *It's Personal but Is It Mine? Toward Property Rights in Personal Information*, 37 U.C. DAVIS L. REV. 379, 403 (2003).

67. N.H. REV. STAT. ANN. § 151:21 (2016).

68. Hall, *supra* note 57, at 646–47.

69. Dwyer v. Am. Express Co., 652 N.E.2d 1351, 1352–53 (Ill. App. Ct. 1995).

70. *E-7.04 Sale of a Medical Practice*, AM. MED. ASS'N, https://www.denbar.org/docs/AMA%20(Professionalism)%20E-7.pdf?ID=2373 [https://perma.cc/5P5Y-WBAT] (last updated Sept. 26, 2005).

world."[71] As explained by the California Supreme Court, applying a broad definition, "[t]he term 'property' is sufficiently comprehensive to include every species of estate, real and personal, and everything which one person can own and transfer to another. It extends to every species of right and interest capable of being enjoyed as such upon which it is practicable to place a money value."[72] Others have limited the definition of property to the specific set of "legally sanctioned property forms" defined by legislatures.[73] This Article uses a broad definition, modified to apply to health information. Thus, a property interest in health information may be defined as any interest in the health information that is enforceable against the world. Property rights under this definition are distinguished from the more limited rights that apply under the terms of a contract, where rights are enforceable only against a party to the contract, or rights that only apply in certain settings or for certain users, such as health information privacy and security regulations. When considering property rights in personal information, courts have historically held that such information belongs to no one until it is collected, at which point it belongs to the collector.[74] Thus, when a company collects the names, addresses, phone numbers, and shopping histories of its customers, that information may become a protected piece of property that can be transferred along with other corporate property when the business is sold or sold outright as a product itself.[75]

In the healthcare context, medical records typically belong to the physician, hospital, or another provider that created them.[76] Thinking of healthcare like any other service industry, the medical record is a record of the service provided to the customer. For the healthcare provider, the information in a medical record is necessary for a number of purposes other than patient care. These include receiving payment for the service from an insurance company, complying with state and federal reporting requirements, supporting business functions such as profit-sharing among partners and paying taxes, and defending the provider in case of any claim of malpractice.[77]

---

71. Schwartz, *supra* note 48, at 2058.

72. Yuba River Power Co. v. Nevada Irrigation Dist., 207 Cal. 521, 524 (1929).

73. Thomas W. Merrill & Henry E. Smith, *Optimal Standardization in the Law of Property: The Numerus Clausus Principle*, 110 YALE L.J. 1, 10 (2000).

74. Bergelson, *supra* note 66, at 403.

75. *E.g.*, Julia N. Mehlman, *If You Give a Mouse a Cookie, It's Going to Ask for Your Personally Identifiable Information: A Look at the Data-Collection Industry and a Proposal for Recognizing the Value of Consumer Information*, 81 BROOK. L. REV. 329, 331 (2015).

76. *E.g.*, Hall, *supra* note 57, at 646–47.

77. Stanley J. Reiser, *The Clinical Record in Medicine Part 2: Reforming Content and Purpose*, 114 ANNALS INTERNAL MED. 980, 984 (1991).

As business records, medical records and the information they contain can be transferred when, for example, a partner leaves a medical practice or a practice merges with another institution.[78] Custody of medical records may be made part of an employment contract between a practice and an individual physician or part of a contract for the sale of a practice.[79] Patients cannot take the original medical record away from the provider who created it, as it remains a vital business record of the service provided.

On the other hand, the property interest in medical records is not exclusive to the individual or entity that created them.[80] Because of the many rights held by individual patients with respect to their medical records, records may not be disposed of in the same manner as other property.[81] Medical records cannot be destroyed or given to others without following the procedures prescribed by federal and state laws.[82] Providers cannot prevent individuals from taking the information in their records and giving it to a competing provider.[83] The property interest a physician has in medical records is fundamentally different than the property interest he or she has in an x-ray machine or stethoscope.[84] Thus, while medical records are certainly property, they are a unique type of property.

Turning to the information contained in the medical record, it may be the property of the person or entity that collected it. In general, the collected form of the information may be "property," which courts have recognized,[85] rather than the individual pieces of the information itself. In the case of a customer list, for example, the list may be considered property in its collected form. However, when the names of some of the individuals from that customer list are available elsewhere, such as in a phone book, it cannot be said that the phone book contains the property of the company that collected the customer list. In other words, the fact that health information may be

78. WILLIAM H. ROACH JR. ET AL., MEDICAL RECORDS AND THE LAW 333 (Jones and Bartlett Publishers 4th ed. 2006).

79. *Id.* at 339.

80. Mark A. Hall & Kevin A. Schulman, *Ownership of Medical Information*, 301 J. AM. MED. ASS'N. 1282, 1282–84 (2009).

81. *See generally id.*

82. *E.g.*, Christine L. Glover, *To Retain or Destroy? That Is the Health Care Records Question*, 103 W. VA. L. REV. 619, 625–26 (2001).

83. *See* Hall & Schulman, *supra* note 80, at 1282–84.

84. *Id.*

85. *E.g.*, In re Nw. Airlines Privacy Litig., No. CIV.04-126(PAM/JSM), 2004 WL 1278459, at *4 (D. Minn. June 6, 2004) (where airline passengers' personal information was compiled and combined with other information to form a record, and the record itself became the airline's property).

the property of one party in its collected form does not mean that the information itself is the property of the collector wherever it exists.

Whether or not the collected health information, like that in a medical record, could be the property of the person who is the subject of the information remains in question. In general, courts have refused to recognize property rights in information about oneself, even as they recognize causes of action where personal information is misused, as in the case of identity theft or misappropriation of an individual's name or likeness for profit.[86] Individuals have been unable to prevent the distribution of information about them by investigators, credit companies, and magazine publishers.[87] Certainly, health information cannot be the exclusive property of the subject, since the information itself is contained in business records of the health providers who recorded the information and must be exchanged with others, such as regulators, insurance companies, and other providers, in order to do business.

What about genetic information, which is even more closely tied to an individual than a name or photograph? Does genetic information, such as a DNA sequence, have a special status as property even where other health information does not? In the famous *Moore v. Regents of the University of California*,[88] a physician at UCLA Medical Center isolated a cell line from the patient Moore's T-lymphocytes, extracted from biological samples taken during his treatment.[89] The physician made agreements to profit from commercial development of the cell line and resulting products. Moore sued, claiming, among other causes of action, that the biological samples that yielded the cell line were his property that was illegally converted by the physician.[90] To prove the tort of conversion, the "plaintiff must establish an actual interference with his ownership or right of possession . . . [w]here plaintiff neither has title to the property alleged to have been converted, nor possession thereof, he cannot maintain an action for conversion."[91] In *Moore*, the California Supreme Court held that Moore did not have an enforceable property interest in his cells under existing law, partly because he did not

86. I.J. Schiffres, Annotation, *Invasion of Privacy by Use of Plaintiff's Name or Likeness in Advertising*, 23 A.L.R.3d 865 § 4 (1969).

87. *E.g.*, Dwyer v. Am. Express Co., 652 N.E.2d 1351, 1351 (Ill. App. Ct. 1995); Shibley v. Time, Inc., 341 N.E.2d 337, 340 (Ohio Ct. App. 1975); U.S. News & World Report, Inc. v. Avrahami, No. 95-1318, 1996 WL 1065557, at *6 (Va. Cir. Ct. June 13, 1996).

88. Moore v. Regents of Univ. of Cal., 793 P.2d 479, 487 (Cal. 1990) (rejecting individual's claim of property right in his genetic information).

89. *Id.* at 481.

90. *Id.* at 482.

91. *Id.* at 488.

expect to retain possession of them after they were taken from his body.[92] The court declined to extend conversion to the facts in *Moore*, noting the chilling effect on medical research and development of treatments that would result from giving every patient a property interest in their biological samples taken in the course of treatment and any resulting research or innovation.[93] Interestingly, genetic information is one type of health information where states have given individuals a property interest under the law. In Alaska,[94] Colorado,[95] Florida,[96] Georgia,[97] and Louisiana,[98] state statutes declare genetic information, DNA samples, or the results of DNA analysis to be the property of the individuals who are the subject of the information. Likewise, reproductive material has been deemed property after it has been removed from the body.[99] In general, reproductive material itself is not sold but "donated," although the donor may receive substantial compensation in exchange for her "donor services."[100] Indeed, egg donation is an $80 million market.[101] Largely self regulated, there are industry guidelines limiting the amount of compensation an egg donor may receive, though no limits apply to sperm donation. These limits were challenged in a class action[102] brought by egg donors that was settled in early 2016.[103] Thus, given this history of treating reproductive material as property or allowing the sale of reproductive material using contracts in the same way other goods are sold, there is potentially a greater degree of ownership that applies to reproductive material than to other biological material or, more broadly, to health information.

In contrast, the status of preserved embryos is much less clear. Some courts have held that as potential persons, embryos cannot be

92. *Id.* at 488–89.

93. *Id.* at 494.

94. ALASKA STAT. ANN. §§ 18.13.010–.030, .100 (West 2016).

95. COLO. REV. STAT. ANN. §§ 10-3-1104.6, 1104.7 (West 2016).

96. FLA. STAT. § 760.40 (2016).

97. GA. CODE ANN. §§ 33-54-1 to -8 (West 2016).

98. LA. STAT. ANN. § 22:1023 (2016).

99. *E.g.*, Kurchner v. State Farm Fire & Cas. Co., 858 So. 2d 1220, 1221 (Fla. Dist. Ct. App. 2003) (holding that sperm outside of the body is property for purposes of insurance claim).

100. Kamakahi v. Am. Soc'y for Reprod. Med., No. C 11-01781 SBA, 2013 WL 1768706, at *3 (N.D. Cal. Mar. 29, 2013).

101. *Id.*

102. Kamakahi v. Am. Soc'y for Reprod. Med., No. 11-CV-01781-JCS, 2015 WL 1926312, at *1 (N.D. Cal. Apr. 27, 2015).

103. Jacob Gershman, *Fertility Industry Group Settles Lawsuit over Egg Donor Price Caps*, WALL ST. J. (Feb. 3, 2016, 11:01 AM), http://blogs.wsj.com/law/2016/02/03/fertility-industry-group-settles-lawsuit-over-egg-donor-price-caps/ [https://perma.cc/989S-CHXF].

property to be transferred like other marital property,[104] while others have freely enforced contracts that determine how embryos are to be used or disposed of in the case of a separation.[105] As the practice of assisted reproduction continues to become more common, the legal approach to the disposition of embryos may be informative for the question of health information ownership. At least two people have simultaneous and valid legal interests in a frozen embryo, created from their biological material, which is somewhat analogous to multiple parties having valid interests in a piece of health information.

As these examples illustrate, the practice of treating health information as property under the law has an uneven history. There are some forms of health information, such as medical records created by a healthcare provider in the course of doing business, that the law is comfortable treating as property. Other forms, such as biological materials and genetic information, have been treated differently. Because an ownership interest may be claimed in intangible information rather than the physical form of the record, some have proposed that health information be protected under intellectual property law.[106]

B. Intellectual Property Law

Intellectual property laws (which include trademark, copyright, and patent mechanisms) confer the rights of property on creations of the mind, such as scientific discoveries, artwork, designs, and written work, which one could not otherwise have an exclusive interest.[107] The term "[i]ntellectual property relates to items of information or knowledge, which can be incorporated in tangible objects at the same time in an unlimited number of copies at different locations anywhere in the world."[108] In order to be protected by a patent, which is the mechanism that would apply to most healthcare-related intellectual property, the discovery in question cannot be simply a "consequence of the body's natural processes."[109] Even if the natural phenomenon in question is not identical across every person, if "the genetic

104. Davis v. Davis, 842 S.W.2d 588, 593, 604 (Tenn. 1992).

105. *E.g.*, Litowitz v. Litowitz, 48 P.3d 261, 274 (Wash. 2002).

106. *See* Schwartz, *supra* note 48, at 2076.

107. *See What Is Intellectual Property?*, WORLD INTELL. PROP. ORG., http://www.wipo.int/about-ip/en/ [https://perma.cc/HS98-PTZU] (last visited Nov. 14, 2016).

108. SRIKANTH VENKATRAMAN, UNDERSTANDING DESIGNS ACT 115 (2010).

109. Genetic Techs. Ltd. v. Bristol-Myers Squibb Co., 72 F. Supp. 3d 521, 530 (D. Del. 2014).

correlations . . . exist apart from any human action," the discovery is unpatentable.[110] Most of the health information about an individual that is collected in medical records and databases is merely reporting on the observed biological state and processes of the individual who is the subject of the information. As such, it could not be protected by intellectual property law, even if a human made the observation.

Courts in the United States have rejected attempts to patent diagnostic procedures and medical treatments.[111] However, it is possible for a physician to use a very specialized technique for evaluating or treating a patient and for that technique to be protected by copyright or patent laws.[112] The US Patent and Trademark Office (USPTO) issued guidance to illustrate what considerations may allow a procedure for evaluating or treating a natural process to be protectable.[113] If such protection is granted, the physician may be able to shield the protected part of the evaluation from disclosure. Thus, there is some capacity for health information to be protected by intellectual property law, but it is limited under current standards.

C. Federal Privacy Law

1. Constitutional Law

The US Constitution does not explicitly enumerate a right to privacy.[114] However, various amendments to the Constitution grant rights that relate to personal autonomy, an aspect of privacy insofar as individuals can choose whether or not to participate in certain activities or be subject to certain experiences, such as "the right to be left alone."[115] The US Supreme Court has also identified a right to privacy under the Fourteenth Amendment.[116] Under the Fourteenth

110. *Id.* (citing Genetic Techs. Ltd. v. Agilent Techs., Inc., 24 F. Supp. 3d 922, 927 (N.D. Cal. 2014) (stating correlations between variation in non-coding and coding regions alone are unpatentable natural laws despite not being "universal" or "immutable scientific truths")).

111. *E.g.*, Mayo Collaborative Servs. v. Prometheus Labs., Inc., 132 S. Ct. 1289, 1298 (2012); PerkinElmer, Inc. v. Intema Ltd., 496 Fed. Appx. 65 (Fed. Cir. 2012). In Australia, by contrast, medical treatments are considered patentable. *Apotex Pty Ltd v Sanofi-Aventis Australia Pty Ltd* [2013] HCA 50.

112. *See* Memorandum from Andrew H. Hirshfeld, Deputy Comm'r for Patent Examination Policy, U.S. Patent and Trademark Office, to the Patent Examining Corps (Mar. 4, 2014), http://www.uspto.gov/patents/law/exam/myriad-mayo_guidance.pdf [https://perma.cc/3T4R-Z8C6].

113. *Id.*

114. Julie K. Freeman, *Medical Records and the U.S. and Pennsylvania Constitutions' Right to Privacy*, 70 Pa. B.A. Q. 93, 95 (1999).

115. Robert E. Mensel, *The Antiprogressive Origins and Uses of the Right to Privacy in the Federal Courts 1860–1937*, 3 FED. CTS. L. REV. 109, 124 (2009).

116. *See, e.g.*, Roe v. Wade, 410 U.S. 113, 164 (1973).

Amendment, a law is unconstitutional if it infringes upon the exercise of a fundamental right, such as the right to privacy, without a "compelling" state interest.[117] The right to privacy is defined and determined on a case-by-case basis; for example, the Court has identified a specific right to privacy with respect to decisions about "family, marriage, motherhood, procreation, and child rearing."[118]

One aspect of the privacy concept is the ability to control one's own information.[119] However, existing Supreme Court case law does not recognize within the right to privacy a right to control information, though it has specifically declined to foreclose that possibility for the future.[120] As it currently stands, the right to control one's information, health-related or otherwise, is not considered a fundamental right, and thus any law infringing upon that ability need only be rationally related to a legitimate government purpose.[121] Ten states explicitly recognize an individual's right to privacy in their constitutions.[122] These states prohibit unreasonable or unwarranted invasions of privacy, though none specifically include the right to control one's personal information as an aspect of "privacy."[123] In general, however, the right to information privacy has been conferred primarily by statute and regulation rather than by courts' application of a constitutional right.[124]

There is no comprehensive federal statutory framework governing health information privacy and security,[125] rather a patchwork of federal laws that often overlap or even contradict each other. The primary function of these laws and regulations is to limit the ways in which lawful holders of the information may use and share it with or without the subject of the information's consent.[126] Although federal privacy laws and regulations do not explicitly confer an ownership interest in health information, they do grant information holders some ability to direct and control how the

---

117. *Id.* at 155–56.

118. Paris Adult Theater v. Slaton, 413 U.S. 49, 65 (1973).

119. *See* Hall & Schulman, *supra* note 80, at 1282–84.

120. ERWIN CHEMERINSKY, CONSTITUTIONAL LAW: PRINCIPLES AND POLICIES 856 (3d ed. 2006).

121. *See id.*

122. *Privacy Protections in State Constitutions*, NAT'L CONF. ST. LEGISLATURES (Dec. 3, 2015), http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-constitutions.aspx [https://perma.cc/VG3R-Q6MY].

123. *See id.*

124. *See id.*

125. Jane Hyatt Thorpe & Elizabeth A. Gray, *Big Data and Public Health: Navigating Privacy Laws to Maximize Potential*, PUB. HEALTH REP. 130(2):171–75 (2015).

126. *E.g.*, Hall, *supra* note 57, at 657.

information is used.[127] Some laws and regulations give individuals explicit rights with respect to their health information when it is in the possession of certain lawful holders of that information.[128] These laws vary considerably in terms of the health information they protect and the entities they govern, though all of these laws apply only to identifiable information.[129]

2. HIPAA

The most widely referenced federal framework related to health information are the Health Insurance Portability and Accountability Act of 1996 (HIPAA)'s[130] Administrative Simplification provisions[131] and their enabling regulations—the Privacy, Security, Breach Notification, and Enforcement Rules, known collectively as "the HIPAA Rules." Under HIPAA, individually identifiable health information is oral or recorded information created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse that identifies or could be used to identify an individual, and relates to the individual's care or to his past, present, or future mental or physical health condition or payment for care.[132] The HIPAA Rules do not apply to individually identifiable health information held in certain types of records, such as education records, or about individuals deceased for over fifty years.[133] The information subject to HIPAA is referred to as "protected health information" (PHI). Much health-related information exists outside of HIPAA's protections, including PGHD,[134] consumer and sentiment data describing patient activities and preferences (i.e., exhaust data),[135]

---

127. *See id.*

128. *See id.* at 646.

129. *Id.* at 659.

130. Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191, 110 Stat. 139 (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C.).

131. *See, e.g., id.* at §§ 261–62.

132. 45 C.F.R. § 160.103 (2016) ("Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual . . . .").

133. *Id.*

134. *Patient-Generated Health Data, supra* note 15.

135. Nicolas P. Terry, *Big Data Proxies and Health Privacy Exceptionalism*, 24 HEALTH MATRIX 65, 85 (2014), http://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?article=1005&context=healthmatrix [https://perma.cc/RR4R-Z4Y4].

and de-identified information—though these types of information may be subject to other laws and regulations.[136]

The HIPAA Rules only regulate the use, disclosure, and management of PHI when it is in the possession of certain entities.[137] These are Covered Entities (health plans, healthcare clearinghouses, and most healthcare providers)[138] and their Business Associates (entities that have access to PHI in the course of performing certain services for or functions on behalf of a Covered Entity);[139] HIPAA does not govern individually identifiable health information when it is in the possession of non-regulated entities (i.e., neither Covered Entity nor Business Associate), even if the information meets the definition of PHI.[140]

The HIPAA Rules collectively serve as the federal floor for identifiable health information privacy and security.[141] The HIPAA Privacy Rule, as its name suggests, governs the privacy and confidentiality of PHI.[142] It dictates when and to whom a Regulated Entity is permitted to disclose PHI, which can be grouped into three broad categories:

1. Required Disclosures: a Regulated Entity *must* disclose PHI to the individual subject of the information upon request[143] and

136. *See generally What Is "Health Information" for Purposes of the Mobile Device Privacy and Security Subsection of HealthIT.gov?*, *supra* note 4.

137. 45 C.F.R. § 160.102(a), (b) (2016).

138. 45 C.F.R. § 160.103 (defining "covered entity" to include "[a] health plan," "[a] health care clearinghouse," and "[a] health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter"); *see also* § 160.103 (defining "health care clearinghouses" to include businesses or agencies that process nonstandard health information they receive from other entities into a standard format); § 160.103 (where "health information"—information (identifiable or not) that is created by a healthcare provider, health plan, public health authority, employer, life insurer, school or university, or healthcare clearinghouse and that relates to an individual's healthcare or an individual's past, present, or future physical or mental health or condition or payment for care—has a broader definition than "protected health information"); 45 C.F.R. § 162 (2016) (defining "covered health care provider" as one who electronically transmits health information in connection with "covered" transactions, which include, but are not limited to, benefit eligibility inquiries and claims).

139. 45 C.F.R. § 160.103 (defining "business associate" to include those who provide "legal, actuarial, accounting, consultation, data aggregation . . ., management, administrative, accreditation, or financial services").

140. *See, e.g.*, 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, 78 Fed. Reg. 5566 (Jan. 25, 2013) (codified at C.F.R. pts. 160, 164).

141. *See* 45 C.F.R. § 160 (2016); *see also* 45 C.F.R. § 160.203 (2016); 45 C.F.R. § 164.502 (2016).

142. *See generally* 45 C.F.R. §§ 164.500–.534 (2016).

143. 45 C.F.R. § 164.502(a)(2)(i), (4)(ii) (2016).

to the Secretary of the US Department of Health and Human Services (HHS) for enforcement and compliance purposes;[144]

2. Prohibited or Limited Disclosures: a Regulated Entity *may not* disclose PHI for certain purposes[145] (e.g., most sales of PHI[146]) and must obtain an individual's authorization to disclose certain types of PHI (e.g., psychotherapy notes[147]) in almost all circumstances;[148] and

3. Permissive Disclosures: a Covered Entity[149] *may* disclose [most] PHI *without first obtaining the subject's authorization* for a variety of purposes (though some of these purposes require that, where practicable, the individual be given the opportunity to informally object to the disclosure[150]).[151]

Any disclosures not required, permitted, or prohibited by the Privacy Rule require written authorization from the individual subject of the PHI.[152] The "permissive disclosure" exceptions were designed to permit Covered Entities to engage in fundamental healthcare activities without being burdened by authorization requirements.[153] Permissive exceptions include disclosures for purposes of treatment, payment, and healthcare operations,[154] as well as a variety of purposes that benefit the public good, such as disease surveillance, national security, and law enforcement activities.[155] These exceptions are so broad that Covered Entities essentially retain greater control over PHI than the actual subject of the information.[156] However, in an

144. 45 C.F.R. § 164.502(a)(2)(ii), (4)(i).

145. *See* 45 C.F.R. § 164.502(a)(5).

146. 45 C.F.R. § 164.502(a)(5)(ii).

147. 45 C.F.R. § 164.508(a) (2016).

148. 45 C.F.R. § 164.508(a)(2).

149. *See* 45 C.F.R. § 164.502(a)(1); *see also* 45 C.F.R. § 164.502(a)(3) (stating that a business associate may only disclose PHI as required by its business associate contract or the law).

150. 45 C.F.R. § 164.510 (2016).

151. 45 C.F.R. § 164.512 (2016); *see also* OFFICE FOR CIVIL RIGHTS, PERMITTED USES AND DISCLOSURES: EXCHANGE FOR TREATMENT 1 (2016), http://www.hhs.gov/sites/default/files/exchange_treatment.pdf [https://perma.cc/8WK6-F6D5]; OFFICE FOR CIVIL RIGHTS, PERMITTED USES AND DISCLOSURES: EXCHANGE FOR HEALTH CARE OPERATIONS 1 (2016), http://www.hhs.gov/sites/default/files/exchange_health_care_ops.pdf [https://perma.cc/22LV-LN9M].

152. 45 C.F.R. § 164.502(a)(1).

153. *See, e.g.*, Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 14776 (proposed Mar. 27, 2002) (to be codified at C.F.R. pts. 160, 164).

154. 45 C.F.R. § 164.506 (2016).

155. 45 C.F.R. § 164, §§ 510, 512 (2016).

156. *See infra* notes 168–73.

effort to balance an individual's interest in his or her own information with the need to enable proper functioning of the healthcare system, the Privacy Rule establishes six rights individuals have with respect to their PHI:

1. To be notified of uses and disclosures a Covered Entity may make;[157]

2. To request restrictions on some uses and disclosures, though a Covered Entity is only required to comply with such a request in very limited circumstances;[158]

3. To request that a health plan or a covered provider communicate PHI confidentially (i.e., by alternative means or at alternative locations), though a health plan is only required to comply in specific circumstances;[159]

4. To inspect and obtain a copy of PHI or have the Covered Entity transmit a copy of PHI to a designated third party;[160]

5. To amend PHI in certain circumstances;[161] and

6. To receive an accounting of disclosures of PHI made in the preceding six years, though many types of disclosures are exempt from the accounting requirement.[162]

While the HIPAA Privacy Rule grants an individual substantial rights, including access to and some measure of control over their health information, because of the many exceptions to and limitations on these rights, they do not equate to the full control that ownership under a property theory would convey.[163]

3. Other Federal and State Statutes and Regulations Protecting Health Information Privacy

Some other federal statutes and regulations protect health information primarily based on its content. These include: 42 C.F.R. Part 2 (Part 2),[164] which protects identifying information about

157. 45 C.F.R. § 164.520(a)(1) (2016).
158. 45 C.F.R. § 164.522(a) (2016).
159. 45 C.F.R. § 164.522(b).
160. 45 C.F.R. § 164.524 (2016).
161. 45 C.F.R. § 164.526 (2016).
162. 45 C.F.R. § 164.528 (2016).
163. Hall, *supra* note 57, at 649.
164. 42 C.F.R. § 2 (2016).

substance abuse treatment patients, the Genetic Information Non-Disclosure Act of 2008 (GINA),[165] which protects individuals' genetic information, and the Patient Safety and Quality Improvement Act of 2005 (PSQIA),[166] which protects identifiable patient safety work product. Other laws protect health information primarily based on its source. These include: the Fair Credit Reporting Act (FCRA),[167] which protects medical information in consumer reports, the Privacy Act of 1974,[168] which protects individually identifiable information—including health information—held by the federal government, the Family Educational Records Privacy Act (FERPA),[169] which protects identifiable information—including health information—in education records, and the Public Health Services Act's Title X,[170] which protects health information collected by Community Health Centers.

a. The Genetic Information Non-Disclosure Act of 2008 (GINA)

GINA protects individuals' genetic information[171] from being used for certain purposes.[172] Under Title I of GINA, health plans and health insurance issuers may not use genetic information to make coverage-related decisions about beneficiaries.[173] Health plans and issuers generally may not even request that a beneficiary undergo genetic testing or provide genetic information, though there are limited exceptions.[174]

Title II of GINA prohibits employers from using genetic information to discriminate against employees or applicants and from using genetic information in employment decisions.[175] Employers are generally prohibited from acquiring genetic information about an

165. Genetic Information Nondiscrimination Act (GINA) of 2008, Pub. L. No. 110-233, 122 Stat. 881 (tit. II codified at 42 U.S.C. § 2000ff).

166. Patient Safety and Quality Improvement Act (PSQIA) of 2005, Pub. L. No. 109-41, 119 Stat. 424 (codified in scattered sections of 42 U.S.C.).

167. Fair Credit Reporting Act (FCRA), 15 U.S.C. §§ 1681–1681x (2012).

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

169. Family Educational Records Privacy Act (FERPA) of 1974, 20 U.S.C. § 1232g (2012) (implementing regulations at 34 C.F.R. § 99).

170. 42 C.F.R. § 51c.110 (2016).

171. "Genetic information" includes family medical history, information from genetic tests and services, requests for and receipt of genetic services, and participation in clinical research that includes genetic services. *See, e.g.*, Genetic Information Nondiscrimination Act (GINA) of 2008, Pub. L. No. 110-233, tit. I, § 101(d), 122 Stat. 881, 883 (2008).

172. Note that GINA does not apply to life insurance plans, long-term care plan issuers, or disability insurers. *Genetic Discrimination*, NAT'L HUM. GENOME RES. INST., https://www.genome.gov/10002077/ [https://perma.cc/CF84-PPR3] (last updated May 2, 2016).

173. *See, e.g.*, GINA tit. I, § 102(a)(4).

174. *See, e.g.*, GINA § 101(b).

175. *See, e.g.*, GINA tit. II, § 202(a).

employee or applicant for any reason,[176] with some exceptions where the acquisition is unintentional or for certain legitimate business purposes. Title II also requires that employers keep [legally acquired] genetic information confidential,[177] and lists several purposes for such information may be disclosed without the individual subject's consent.[178] GINA permits, but does not require, employers to disclose genetic information to the employee upon written request.[179]

GINA mandated amendments to HIPAA to ensure that "genetic information" is included within the definition of PHI, and that Title I's prohibition on the use of genetic information by health insurers for underwriting purposes is also explicitly prohibited under HIPAA.[180] GINA's protections give individuals some control over their genetic information by limiting not just how that information can be used, but whether it can be obtained at all.[181] GINA was enacted to ensure that individuals were not discouraged from utilizing genetic testing, technologies, research, and related therapies out of fear of discrimination.[182]

b. Privacy Act and FOIA

The Privacy Act of 1974 protects identifiable information about individuals, including health information, held or collected by the federal government.[183] Generally, a federal agency may not release individually identifiable information to anyone without the subject of the information's written consent.[184] There are multiple exceptions to this prohibition, including for several legitimate governmental purposes, statistical research, and as required by the US Freedom of Information Act (FOIA).[185] The Privacy Act does provide individuals certain rights with respect to their information, including the right to receive an accounting of certain disclosures made within the last five years,[186] the right to review and obtain a copy of the information upon request,[187] and the right to request an amendment to the information,

176. GINA § 203(b).
177. GINA § 206(a).
178. GINA § 206(b).
179. *Id.*
180. GINA tit. I, § 105(a).
181. GINA § 101(d).
182. GINA § 2(5).
183. 5 U.S.C. § 552a (2012).
184. § 552a(b).
185. *Id.*
186. § 552a(c)(3).
187. § 552a(d)(1).

though the agency is not required to comply with such a request.[188] While the Privacy Act does give individuals some control over their information, it does not limit the information that may be collected or stored by a federal agency, though such limitations may exist in other laws or regulations.[189] An individual cannot restrict, or even request that an agency restrict, how information is used or disclosed.[190] Thus, the Privacy Act is quite broad, though its reach is limited by its relationship to FOIA.[191]

Under FOIA, any person may access any information contained in federal agency records,[192] including individually identifiable information otherwise protected by the Privacy Act, unless the information is specifically exempted from disclosure.[193] Generally, these exemptions prevent disclosure of information that is considered sensitive or of a personal nature; the most pertinent of these is exemption 6, which protects "personnel, medical, and similar files" where disclosure "would constitute a clearly unwarranted invasion of personal privacy."[194] Exemption 6 essentially closes the privacy gap created by the Privacy Act's exception for FOIA-related disclosures.[195] While exemption 6 does not give an individual more control over his or her health information in the possession of the federal government, the opportunities for such information to be shared without the individual's consent is limited almost entirely to governmental and law enforcement functions.[196]

c. 42 C.F.R. Part 2

42 C.F.R. Part 2 protects identifying information, recorded or not, that could or does reveal that an individual received substance abuse treatment;[197] Part 2 applies to all federally-assisted programs[198] providing substance abuse diagnosis, treatment, or

188. § 552a(d)(2).

189. § 552a(b)(1).

190. *Id.*

191. U.S. GOV'T GEN. SERVS. ADMIN., YOUR RIGHT TO FEDERAL RECORDS: QUESTIONS AND ANSWERS ON THE FREEDOM OF INFORMATION ACT AND THE PRIVACY ACT 16 (2009), https://www.justice.gov/sites/default/files/oip/legacy/2014/07/23/right_to_federal_records09.pdf [https://perma.cc/2V3V-R7BF].

192. 5 U.S.C. § 552(a)(6)(A) (2012).

193. § 552(b).

194. § 552(b)(6).

195. *See id.*

196. *See id.*

197. 42 CFR § 2.12(a)(1)(ii), (a)(2) (2016).

198. A program is "federally assisted" if it is conducted by any federal department or agency (directly or under contract), is carried out under any federal license, certification,

referral.[199] While Part 2 information is also protected health information (PHI) and Part 2 programs are almost always Covered Entities, Part 2's protection for patient identifying information provides much greater control to patients than HIPAA would otherwise provide.[200] In general, Part 2-covered information may not be disclosed without the patient's written consent,[201] with limited exceptions. Part 2 also prohibits recipients of covered information from further disclosing the information without written consent or unless otherwise permitted by Part 2.[202] Part 2 grants individuals some rights with respect to their covered information, though these are limited to the right to be informed of Part 2's confidentiality protections[203] and the right to access, inspect, and obtain a copy of his or her own records.[204] Part 2's provisions grant individuals the near-exclusive ability to control when and to whom their covered information is disclosed.[205] Similar to GINA's intended purpose, Part 2 was enacted to ensure that individuals were not discouraged from seeking substance abuse treatment due to privacy-related fears.[206]

Federal Privacy Law has been crafted to meet certain needs but is not a comprehensive regulatory scheme covering all types or uses of health information. It does not confer comprehensive ownership rights but does extend a number of rights and obligations over health information that may have the same effect as ownership under the law, in some circumstances, for those types and uses of information that are covered.

D. Contract Law

Contracts are a way to confer rights where they may or may not be granted by other legal authorities.[207] Ownership can be

registration, or authorization (e.g., Medicare/Medicaid providers, providers with a DEA number), or receives any federal financial assistance (e.g., grants, federal tax-exempt status). § 2.12(b).

199. § 2.12(e)(2).

200. *See, e.g.*, U.S. DEP'T OF HEALTH & HUMAN SERVS., THE CONFIDENTIALITY OF ALCOHOL AND DRUG ABUSE PATIENT RECORDS REGULATION AND THE HIPAA PRIVACY RULE: IMPLICATIONS FOR ALCOHOL AND SUBSTANCE ABUSE PROGRAMS 4 (2004), http://archive.samhsa.gov/HealthPrivacy/docs/SAMHSAPart2-HIPAAComparison2004.pdf [https://perma.cc/FSH9-E35P].

201. 42 C.F.R. § 2.1(a) (2016).

202. 42 C.F.R. § 2.12(d)(2)(iii).

203. 42 C.F.R. § 2.22(a) (2016).

204. 42 C.F.R. § 2.23(a) (2016).

205. *See* § 2.12.

206. 42 C.F.R. § 2.3(b)(2) (2016).

207. *See* RESTATEMENT (SECOND) OF CONTRACTS § 1 (AM. LAW INST. 2016).

granted, transferred, or revoked through the use of contracts.[208] Regardless of ownership, any number of rights and responsibilities with respect to information can be delineated in a contract and enforceable in court with penalties for any breach.[209] The limitation of a contract is, of course, that it is only enforceable against the parties to the contract.[210] Thus, any protections granted to information by a contract will not follow the information if it is transferred to another person who, or entity that, is not a party to the contract.[211]

Contracts may be used to limit or expand rights and responsibilities over information even where the information in question is already regulated, as in the case of Business Associate Agreements (BAAs) that regulate how Business Associates of Covered Entities must manage protected health information in order to comply with HIPAA.[212] Even though the health information held by a Covered Entity is already regulated under HIPAA, the BAA can be used to extend the HIPAA's protections and liability for any breach to another entity.[213]

Contracts are a powerful way for parties to establish rights and responsibilities under the law, but they are limited because they only bind the parties to the contract. The privacy of people who are the subject of the information may be protected or left vulnerable by the terms of contracts to which they are not a party and which they cannot enforce.

E. State Law

States have wide latitude to define their own privacy framework, and as a result, state privacy laws vary considerably in terms of scope and application.[214] State health information laws may mirror federal requirements, be more protective than federal law, or govern health information that is not specifically protected by federal law.[215] In general, governed entities must comply with any state laws

208. *See id.*

209. *See, e.g.*, DAVID R. MELLOH, HIPAA PRIVACY AND MANAGED CARE ORGANIZATIONS IN THE ELECTRONIC ENVIRONMENT, at I (2000).

210. *See, e.g.*, Winterbottom v. Wright (1842) 152 Eng. Rep. 402, 405 (holding breach of contract not available as remedy for injured mail-coach passenger because there was no "privity").

211. *See id.*

212. 45 C.F.R § 164.504(e) (2016).

213. *See id.*

214. *See States*, *supra* note 65.

215. For more information about state laws governing health information, see *id.*

that are more protective of patients' rights,[216] as well as any state laws governing data, patients, or entities not regulated by existing federal law.[217] More protective state laws are generally content-based and focus specifically on highly sensitive information, such as HIV/AIDS test results,[218] STD treatment information, and mental health information,[219] and information about vulnerable populations, such as minors, incarcerated adults, and those declared legally incompetent.[220] States also generally have laws governing state-based registries, compulsory health information reporting, health insurers, public health entities, and provider licensure—all of which may contain requirements related to data sharing and confidentiality.[221]

V. POLICY CONSIDERATIONS

As is evident from the discussion above, individuals in the United States have a patchwork of rights, sometimes overlapping, with respect to information about them held by others and the use of that information. These rights are more or less enforceable depending on their source and the jurisdiction in question. What happens when these rights conflict? For example, suppose one person has a property interest in information about a second person, such as ownership of a database containing health information, and the second person has a privacy interest in keeping his or her information from being sold to other entities. Whose rights prevail? Historically, individuals have needed to prove a tort violation with damages to enforce privacy rights, such as appropriation of one's likeness, identity theft, or egregious invasion of privacy.[222] The HIPAA Privacy Rule confers some specific rights but enforcement is limited for aggrieved

---

216. JOY PRITTS ET AL., PRIVACY AND SECURITY SOLUTIONS FOR INTEROPERABLE HEALTH INFORMATION EXCHANGE: REPORT ON STATE LAW REQUIREMENTS FOR PATIENT PERMISSION TO DISCLOSE HEALTH INFORMATION, at 1-2 to 1-3 (2009), https://www.healthit.gov/sites/default/files/290-05-0015-state-law-access-report-1.pdf [https://perma.cc/D48S-A2JY].

217. *Id.*

218. *State HIV Laws*, CTRS. DISEASE CONTROL & PREVENTION, http://www.cdc.gov/hiv/policies/law/states [https://perma.cc/DWU5-KRG4] (last updated Aug. 29, 2016).

219. *See generally* INST. OF MED., IMPROVING THE QUALITY OF HEALTH CARE FOR MENTAL AND SUBSTANCE-USE CONDITIONS: QUALITY CHASM SERIES (National Academics Press 2006).

220. *See, e.g.*, Carol A. Ford & Abigail English, *Limiting Confidentiality of Adolescent Health Services*, 288 J. AM. MED. ASSN. 752, 752 (2002).

221. *See States*, *supra* note 65.

222. Vera Bergelson, *It's Personal but Is It Mine? Toward Property Rights in Personal Information*, 37 U.C. DAVIS L. REV. 379, 405 (2003).

individuals because there is no private right of action to enforce HIPAA.[223]

The European Union (EU) recently adopted a regulation for the protection of personal data across the EU that gives individuals broad rights to control the use of personal information about them.[224] Adopted April 27, 2016, the EU General Data Protection Regulation includes a number of rights for individuals who are the subject of personal information and obligations of member states to protect that information, though as with other EU regulations, there are many ways in which member states' application of the regulation will vary.[225] Among the most significant aspects of the Regulation are the designation of "the right to the protection of personal data" as a fundamental right[226] and the codification of a "right to be forgotten," where individuals have the right to withdraw consent at any point and have their data erased by any data holder.[227] Some have argued that this Regulation amounts to a property regime because it gives individuals substantial rights over their personal information akin to property rights.[228] For example, the protections created by the Regulation run with the information and bind third parties with whom the individual subject of the information may have no relationship.[229] The Regulation includes many exceptions, such as data processing necessary for public health, scientific research, and the provision of social services, and there will be substantial variation in how EU member states put the Regulation's broad principles into effect in their individual jurisdictions.[230] However, it creates a general right of access and control for the subject of the information, across all types of personal information, that is far more comprehensive than current US policies.

In contrast to the patchwork of rights that currently apply to health information in the US and even the more comprehensive EU regulation, ownership is a more concrete legal theory for enforcing rights in information that would give more certainty to the field.

---

223. *See* In re Nw. Airlines Privacy Litig., No. 04 Civ. 126 (PAM/JSM), 2004 WL 1278459, at *4 (D. Minn. June 6, 2004).

224. Council Regulation 2016/679, 2016 O.J. (119) (EU), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC [https://perma.cc/W6KN-CRFV].

225. *See generally id.*

226. *Id.* at 1.

227. *Id.* at 12–13.

228. Jacob M. Victor, *The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy*, 123 YALE L.J. 513, 515 (2013).

229. Council Regulation 2016/679, *supra* note 224, at ch.III, art. 17.

230. *See, e.g., id.* at ch.IX, art. 88.

However, having enforceable ownership of personal information depends on the law recognizing the information as property or intellectual property.[231] As discussed above, health information does not fit neatly under these legal constructs, though policymakers and courts may expand the definitions for the two types of protected information to grant ownership rights over health information. It may be, however, that information can never be "owned" the way a piece of real estate is owned because so many people have access to that information, by consent or by necessity, that one cannot be considered to be the exclusive owner of it.

Does it even matter whether an individual "owns" his or her health information? Where there are specific rights conferred with respect to my health information, such as under the HIPAA Privacy Rule, one maintains the right to access and share one's information even where one's healthcare provider owns the medical record.[232] It may be that comprehensive privacy laws can grant enough rights to the individual and impose enough responsibilities on holders and users of personal health information that ownership becomes irrelevant because it would convey no additional benefit than already exists.

The legal structures governing privacy have not yet reached this ideal, but using a property approach that assigns ownership of information to the individual subject of the information may not be good public policy. Ownership implies that the thing that is owned can be taken away and potentially disposed of whenever desired by the owner. But such exclusive rights may conflict with other interests. In the case of medical records, those records exist also as business records documenting the healthcare provider's services. The information may be valuable to the public, as information about the quality of care provided at a healthcare institution, data for scientific research, or evidence of a communicable disease, for example.

On the other hand, as health information is increasingly being commodified, profit-seeking by individuals and organizations—either traditional healthcare entities, such as providers and insurers, or third parties whose function is simply collecting and selling information—may call for increased protection for the subjects of the information. In the case of healthcare providers, ethical and practical considerations provide some protections for individuals. Providers

231. *E.g.*, Hall, *supra* note 57, at 645.

232. For example, rights to request privacy protection for protected health information. *See, e.g.*, 45 C.F.R. § 164.524 (2016).

have a duty to avoid harm, to ensure informed consent, and to provide a certain standard of care regardless of their financial interest, in addition to complying with laws that protect patient privacy and govern medical research.[233] However, other entities, such as data brokers, may have no such duties. If the law were to convey an ownership interest to the subject of the data being bought and sold, that individual would have an enforceable right not only to control the use of his or her information, but also the potential to profit directly from it or claim a share in any profit that results from its use by others. If patients were granted ownership interests over their information, it would be important to ensure that such rights did not inhibit important medical innovation and public health activities. These essential activities could be preserved through careful regulation because the law allows the restriction of property interests for the public good, as in the case of zoning laws and other regulatory takings.

In the healthcare setting, the potential for conflicting profit motives between patient and provider could chill a relationship that depends on honest exchange of information. If an individual can potentially profit from the sale of his or her information, that individual may wish to withhold it to prevent its disclosure through another route. Alternatively, a patient may simply wish to prevent his or her provider from making additional profit off of his or her information, which is certainly a disconcerting thought for many patients. While there have always been financial incentives in the US healthcare system, they have generally been limited to fees and reimbursements received for the provision of services.[234] But it may be that, in addition to these usual sources of income, a provider will create a product from the personal information gathered about his or her patients and sell that for a profit. As research and technology venture further into the realm of personalized medicine, it may be that details about individual patients become more valuable, such as for use in creating treatments or tools to support diagnosis. We may see more cases similar to *Moore*,[235] based on the use of specific information about patients to develop profitable products, perhaps revisiting the question of the use of genetic material.

---

233. Marc A. Rodwin, *Financial Incentives for Doctors*, 328 BMJ 1328, 1328–29 (2004), http://www.ncbi.nlm.nih.gov/pmc/articles/PMC420273/pdf/bmj32801328.pdf [https://perma.cc/2FTA-32S3].

234. *See, e.g.*, Mark Hagland, *How Does Your Doctor Get Paid?*, FRONTLINE, http://www.pbs.org/wgbh/pages/frontline/shows/doctor/care/capitation.html [https://perma.cc/7J4T-UJ9N] (last visited Nov. 14, 2016).

235. Moore v. Regents of Univ. of Cal., 793 P.2d 479 (Cal. 1990).

VI. CONCLUSION

The legal environment surrounding health information is dynamic and varied. Because of the expanse of rights at issue and the fact that many of them are subject to regulation by all fifty states in addition to the federal government, there's no single solution to address the issue of health information ownership. As illustrated, a variety of different laws and legal theories can be applied, potentially causing confusion for users of health information and the individuals who are the subject of the information. Valid rights and responsibilities can conflict. Unregulated activities appear that use health information in unanticipated ways, which may be threatening to the individual subjects of the information. Ownership is a familiar concept that some see as a simple way to clarify legal rights; indeed, many healthcare consumers may be surprised to discover that they don't already own their health information. However, conferring ownership to one party may interfere with legitimate claims of another party or important public goals. For example, vesting full ownership of health information in patients under a property scheme may harm research, hinder performance measurement, and limit important public health activities like disease surveillance. On the other hand, vesting full ownership with healthcare providers may prevent oversight, inhibit quality improvement, reduce patient autonomy, and limit patients' willingness to share information necessary for proper medical treatment. Given the balance of rights that must be struck to protect important public goals, we suggest that rights over health information should be resolved by new policies rather than under existing legal structures. As technology evolves to enable greater capability to digest health information and make it meaningful while the market responds to greater, more expansive uses of health information for a wider variety of stakeholders, policymakers at the federal and state levels should work to develop a legal framework to govern the many uses for and users of health information. It is important that this framework be as consistent as possible across settings and jurisdictions so that the many stakeholders in the health information marketplace know their rights and responsibilities and the public's interest in appropriate sharing of health information is protected.