1

In the Medical Privacy of One's Own Home

Four Faces of Privacy in Digital Home Health Care[*]

Barbara J. Evans

I INTRODUCTION

Digital tools to diagnose and treat patients in the home: The phrase hits several tripwires, each sounding its own privacy alarm. Invading the "castle" of a person's home is one privacy tripwire.[1] Sustained digital surveillance of the individual is another. Anything to do with personal health information is still another. Each alarm calls attention to a different strand of privacy law, each with its own account of why privacy matters and how to protect it. No overarching conception of privacy leaps out, which calls to mind Daniel Solove's remark that "the law has attempted to adhere to overarching conceptions of privacy that do not work for all problems. Not all privacy problems are the same."[2]

This chapter explores four faces of privacy: (1) Privacy of the home, which links privacy to the location where information is created or captured; (2) privacy as individual control over personal information, without regard to location, in an age of pervasive digital surveillance; (3) contextual privacy frameworks, such as medical privacy laws addressing the use and sharing of data in a specific context: clinical health care; and (4) content-based privacy, unmoored from location or context and, instead, tied to inherent data characteristics (e.g., sensitive data about health, sexual behavior, or paternity, versus nonsensitive data about food preferences). The hope here is to find a workable way to express what is special (or not) about digital tools for diagnosis and treatment in the home.

[*] The author thanks the Health Policy and Bioethics Consortium of Harvard Medical School and the Harvard Law School Petrie-Flom Center for the opportunity to receive feedback on an early draft of this chapter at the February 11, 2022 virtual meeting entitled, "Diagnosing Alzheimer's with Alexa?" The author has no conflicts to disclose.

[1] See Eric R. Claeys, Kelo, the Castle, and Natural Property Rights, in *Private Property, Community Development, and Eminent Domain* 35, 35–36 (Robin Paul Malloy ed., 2008) (discussing the metaphor of the home as one's castle).

[2] Daniel J. Solove, Conceptualizing Privacy, 90 Calif. L. Rev. 1087, 1147 (2002).

II THE PRIVACY OF THE HOME

An "interest in spatial privacy" feels violated as the home – the "quintessential place of privacy" – becomes a site of digital medical observation and surveillance.[3] Yet electronic home health monitoring originated decades ago, which invites the question of what has sparked sudden concern about digital home health privacy now.

Past experience with home diagnostics clarifies the privacy challenge today. In 1957, Dr. Norman J. Holter and his team developed an ambulatory electrocardiograph system, building on the 1890s string galvanometer for which Willem Einthoven won the 1924 Nobel Prize.[4] The resulting wearable device, known as a Holter monitor, records electrocardiographic signals as heart patients go about their routine activities at home and, since 1961, has been the backbone of cardiac rhythm detection and analysis outside the hospital.[5] Six decades of at-home use of this and similar devices have passed without notable privacy incidents.

There is a distinction that explains why traditional home diagnostics like Holter monitors were not controversial from a privacy standpoint, while today's digital home health tools potentially are. Jack Balkin stresses that "certain kinds of information constitute matters of private concern" not because of details like the content or location, "but because of the *social relationships* that produce them."[6] For example, an injured driver receiving care from an ambulance crew at the side of a road should not be filmed and displayed on the evening news – not because the person is in a private location (which a public highway is not), but because the person is in a medical treatment relationship at the time.[7] It is "*relationships* – relationships of trust and confidence – that governments may regulate in the interests of privacy."[8]

Traditional devices like Holter monitors are prescribed in a treatment relationship by a physician who refers the patient to a laboratory that fits the device and instructs the patient how to use it. After a set period of observation, the patient returns the device to the laboratory, which downloads and analyzes the data stored on the device and conveys the results to the ordering physician. Everyone touching the data is in a health care relationship, bound by a web of general health care laws and norms that place those who handle people's health information under duties of confidentiality.[9]

[3] Julie Cohen, Privacy, Visibility, Transparency, and Exposure, 75 U. Chi. L. Rev. 181, 190–91 (2008); Solove, supra note 2, at 1137.

[4] Ateeq Mubarik & Arshad Muhammad Iqbal, Holter Monitor, *StatPearls* (2022), www.ncbi.nlm.nih.gov/books/NBK538203/. See also Moises Rivera-Ruiz et al., Einthoven's String Galvanometer: The First Electrocardiograph, 35 Tex. Heart Inst. J. 174 (2008).

[5] Mubarik & Iqbal, supra note 4.

[6] Jack M. Balkin, Information Fiduciaries and the First Amendment, 49 UC Davis L. Rev. 1183, 1205 (2016).

[7] *Shulman* v. *Group W Prods., Inc.*, 955 P.2d 469 (Cal. 1998).

[8] Balkin, supra note 6, at 1187.

[9] Barry R. Furrow et al., *Health Law: Cases, Materials and Problems* (8th edn.) 117 (2018).

https://doi.org/10.1017/9781009373234.003 Published online by Cambridge University Press

These duties flow less from privacy law than from general health care laws and norms predating modern concerns about information privacy. For example, state licensing statutes for health care professionals focus mainly on their competence but also set norms of confidentiality, enforceable through disciplinary sanctions and the potential loss of licensure.[10] Professional ethics standards, such as those of the American Medical Association, amplify the legally enforceable duties of confidentiality.[11] State medical records laws govern the collection, use, and retention of data from medical treatment encounters and specify procedures for sharing the records and disposing of or transferring them when a care relationship ends.[12] State courts enforce common law duties for health care providers to protect the confidential information they hold.[13]

Jack Balkin's first law of fair governance in an algorithmic society is that those who deploy data-dependent algorithms should be "information fiduciaries" with respect to their clients, customers, and end-users.[14] Traditional health care providers meet this requirement. The same is not always (or perhaps ever) true of the new generation of digital tools used to diagnose and treat patients at home. The purveyors of these devices include many new players – such as medical device manufacturers, software developers and vendors, and app developers – not subject to the confidentiality duties that the law imposes on health care professionals, clinics, and hospitals.

The relationships consumers will forge with providers of digital home health tools are still evolving but seem unlikely to resemble the relationships of trust seen in traditional health care settings. Responsibility for protecting the data generated and collected by digital home health devices defaults, in many instances, to vendor-drafted privacy policies and terms of service. Scott Peppet's survey of twenty popular consumer sensor devices found these privacy protections to be weak, inconsistent, and ambiguous.[15]

Nor is the privacy of the home a helpful legal concept here. As conceived in American jurisprudence, the privacy of the home is a Fourth Amendment protection against governmental intrusion to gather evidence for criminal proceedings.[16] This has little relevance to a private-sector medical device manufacturer or software

[10] Id.

[11] See, for example, Am. Med. Ass'n, Code of Medical Ethics Opinion 3.2.1: Confidentiality, https://code-medical-ethics.ama-assn.org/ethics-opinions/confidentiality.

[12] See P. Jon White & Jodi Daniel, *Privacy and Security Solutions for Interoperable Health Information Exchange: Report on State Medical Record Access Laws* (2009), www.healthit.gov/sites/default/files/290-05-0015-state-law-access-report-1.pdf (providing a multistate survey of various aspects of state medical records laws).

[13] Furrow et al., supra note 9, at 161.

[14] Jack M. Balkin, The Three Laws of Robotics in the Age of Big Data, 78 Ohio State L. J. 1217, 1221 (2017).

[15] Scott R. Peppet, Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent, 93 Tex. L. Rev. 85, 145 (2014).

[16] Laura K. Donahue, The Fourth Amendment in a Digital World, 71 NYU Ann. Surv. Am. L. 553, 562–68 (2017).

vendor offering home diagnostic tools that gather personal health data that could be repurposed for research or a variety of other commercial uses that threaten users' privacy. The Fourth Amendment occasionally might be helpful – for example, if the government seeks data from a home diagnostic device to refute a user's alibi that she was at home at the time she stands accused of a crime at a different location. Unfortunately, this misses the vast majority of privacy concerns with at-home medical monitoring: Could identifiable health data leak to employers, creditors, and friends in ways that might stigmatize or embarrass the individual? Might data be diverted to unauthorized commercial uses that exploit, offend, or outrage the person the data describe? The Fourth Amendment leaves us on our own to solve such problems.

The privacy of the home enters this discussion more as a cultural expectation than as a legal reality. The home as a site of retreat and unobserved, selfhood-enhancing pursuits is a fairly recent innovation, reflecting architectural innovations such as hallways, which became common in the eighteenth century and eliminated the need for every member of the household to traverse one's bedroom to get to their own.[17] The displacement of servants by nongossiping electrical appliances bolstered domestic privacy, as did the great relocation of work from the home to offices and factories late in the nineteenth century.[18] The privacy of the home is historically contingent. It may be evolving in response to COVID-19-inspired work-from-home practices but, at least for now, the cultural expectation of privacy at home remains strong.

This strong expectation does not translate into a strong framework of legal protections. Private parties admitted to one's home are generally unbound by informational fiduciary duties and are free to divulge whatever they learn while there. As if modeled on a Fourth Amendment "consent search," the host consents at the point when observers enter the home but, once there, they are free to use and share information they collect without further consent. The privacy of the home, in practice, is protected mainly by choosing one's friends carefully and disinviting the indiscreet. The question is whether this same "let-the-host-beware" privacy scheme should extend to private actors whose digital home health tools we invite into our homes.

III PRIVACY AS INDIVIDUAL CONTROL OVER IDENTIFIABLE INFORMATION

Many privacy theorists reject spatial metaphors, such as the privacy of the home, in favor of a view that privacy is a personal right for individuals to control data about themselves.[19] After the 1970s, this "control-over-information" privacy theory became

[17] Solove, supra note 2, at 1140.
[18] Id.
[19] Id. at 1109–12. See also Ferdinand David Schoeman, Privacy: Philosophical Dimensions of the Literature, in *Philosophical Dimensions of Privacy: An Anthology* 1, 3 (Ferdinand David Schoeman ed., 1984).

the "leading paradigm on the Internet and in the real, or off-line world."[20] It calls for people – without regard to where they or their information happen to be located – to receive notice of potential data uses and to be granted a right to approve or decline such uses.

This view is so widely held today that it enjoys a status resembling a religious belief or time-honored principle. Few people recall its surprisingly recent origin. In 1977, a Privacy Protection Study Commission formed under the Privacy Act of 1974 found that it was quite common to use people's health data in biomedical research without consent and recommended that consent should be sought.[21] That recommendation was widely embraced by bioethicists and by the more recent *Information Privacy Law Project* on the ethics of data collection and use by retailers, lenders, and other nonmedical actors in modern "surveillance societies."[22]

Control-over-information theory has its critics. An obvious concern is that consent may be ill-informed as consumers hastily click through the privacy policies and terms of use that stand between them and a desired software tool. In a recent survey, 97 percent Americans recalled having been asked to agree to a company's privacy policy, but only 9 percent indicated that they always read the underlying policy to which they are agreeing (and, frankly, 9 percent sounds optimistic).[23] Will people who consent to bring digital health devices into their homes carefully study the privacy policies to which they are consenting? It seems implausible.

A more damning critique is that consent, even when well-informed, does not actually protect privacy. A person who freely consents to broadcast a surgery or sexual encounter live over the Internet exercises control over their information but is foregoing what most people think of as privacy.[24] Notice-and-consent privacy schemes can be likened to the "dummy thermostats" in American office skyscrapers – fake thermostats that foster workplace harmony by giving workers the illusion that they can control their office temperature, which, in fact, is set centrally, with as many as 90 percent of the installed thermostats lacking any connection to the heating and air-conditioning system.[25] Consent norms foster societal harmony by

[20] Paul M. Schwartz, Internet Privacy and the State, 32 Conn. L. Rev. 815, 820 (2000).

[21] 5 USC § 552(a) and (d); Priv. Prot. Study Comm'n, *Personal Privacy in an Information Society* 280 (1977), https://archive.epic.org/privacy/ppsc1977report/.

[22] See, for example, Federal Policy for the Protection of Human Subjects of Biomedical Research ("Common Rule"), 45 CFR §§ 46.101–124 (2018); see, for example, Neil Richards, The Information Privacy Law Project, 94 Geo. L.J. 1087 (2006) and David Lyon, Surveillance Society: Monitoring Everyday Life, 33–35, 114–18 (2001).

[23] Brooke Auxier et al., Americans' Attitudes and Experiences with Privacy Policies and Laws, *Pew Rsch. Ctr.* (2019), www.pewresearch.org/internet/2019/11/15/americans-attitudes-and-experiences-with-privacy-policies-and-laws/.

[24] Anita L. Allen, Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm, 32 Conn. L. Rev., 861, 867 (2000).

[25] See Barbara J. Evans, The HIPAA Privacy Rule at Age 25: Privacy for Equitable AI, 50 Fla. State U. L. Rev., 781–82(2023) (citing investigative reports on dummy thermostats).

giving people the illusion that they can control their privacy risks, but, in reality, consent rights are disconnected from privacy and, indeed, exercising consent rights *relinquishes* privacy.

The loss of privacy is systemic in modern information economies: It is built into the way the economy and society work, and there is little an individual can do. Privacy is interdependent, and other people's autonomous decisions to share information about themselves can reveal facts about you.[26] Bioethicists recognize this interdependency in a number of specific contexts. For example, genomic data can reveal a disease-risk status that is shared with one's family members,[27] and, for Indigenous people, individual consent to research can implicate the tribal community as a whole by enabling statistical inferences affecting all members.[28]

Less well recognized is the fact that, in a world of large-scale, generalizable data analytics, privacy interdependency is not unique to genetically related families and tribal populations. It potentially affects everyone. When results are generalizable, you do not necessarily need to be reflected in the input data in order for a system to discover facts about you.[29] If people like you consent to be studied, a study can reveal facts about you, even if you opted out.

Biomedical science aims for generalizability and strives to reduce biases that cause scientific results not to be valid for everyone. These are worthy goals, but they carry a side effect: Greater generalizability boosts systemic privacy loss and weakens the power of consent as a shield against unwanted outside access to personal facts. Whether you consent or refuse to share whatever scraps of personal data you still control, others can know things about you because you live in a society that pursues large-scale data analytics and strives to make the results ever-more generalizable, including to you. Just as antibiotics cease to work over time as microbes evolve and grow smarter at eluding them, so consent inexorably loses its ability to protect privacy as algorithms grow smarter, less biased, and more clever at surmising your missing data.

There is another concern with notice-and-consent privacy schemes in biomedical contexts, where the problem of bias has been empirically studied more than in some other sectors. Selection bias occurs when the people included in a study fail to reflect the entire population that, ultimately, will rely on results from that study.[30]

[26] Gergely Biczók & Pern Hui Chia, Interdependent Privacy: Let Me Share Your Data, in *Financial Cryptography and Data Security* 338 (Ahmad-Reza Sadeghi ed., 2013).

[27] Marwan K. Tayeh et al., The Designated Record Set for Clinical Genetic and Genomic Testing: A Points to Consider Statement of the American College of Medical Genetics and Genomics (ACMG), 25 Genet. Med. (2022).

[28] Krystal S. Tsosie et al., Overvaluing Individual Consent Ignores Risks to Tribal Participants, 20 Nat. Revs. Genetics 497 (2019).

[29] Cynthia Dwork et al., Calibrating Noise to Sensitivity in Private Data Analysis, in *Theory of Cryptography. TCC 2006. Lecture Notes in Computer Science* vol. 3876, 265 (S. Halevi & T. Rabin eds., 2006).

[30] James J. Heckman, Selection Bias, in *Encyclopedia of Social Measurement* (2005).

Consent norms can produce selection bias if some demographic groups – for example, older white males – consent more eagerly than other groups do. People's willingness to consent to secondary data uses of their health data varies among racial, ethnic, and other demographic groups.[31] If digital home health tools are trained using data acquired with consent, those tools may be biased in ways that cause them to deliver unreliable results and health care recommendations for members of historically underrepresented population subgroups, such as women and the less affluent.[32] Consent norms can fuel health care disparities. Admittedly, this is only one of many equity concerns with digital home health tools. The more salient concern, obviously, is whether these tools will be available to nonprivileged members of society *at all*. Many of these tools are commercially sold on a self-pay basis with no safety net to ensure access by those who cannot pay.

In October 2022, the White House published its *Blueprint for an AI Bill of Rights*, recommending a notice-and-consent privacy scheme in which "designers, developers, and deployers of automated systems" must "seek your permission" to use data in an artificial intelligence (AI) system.[33] It simultaneously calls for AI tools to be "used and designed in an equitable way" that avoids disparities in how the tools perform for different population subgroups.[34] In domains where selection bias is well-documented,[35] as in health care, these two goals may clash.

IV MEDICAL PRIVACY LAW

One possibility for regulating AI/machine learning (ML) home health tools would be to place them under the same medical privacy regulations – for example, the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule,[36] a major US medical privacy framework – used for data generated in clinical health care settings. This section argues against doing so.

[31] Kayte Spector-Bagdady, Governing Secondary Research Use of Health Data and Specimens: The Inequitable Distribution of Regulatory Burden Between Federally Funded and Industry Research, 8 J. L. & Biosciences 1, 2–3 (2021); Reshma Jagsi et al., Perspectives of Patients with Cancer on the Ethics of Rapid-Learning Health Systems, 35 J. Clinical Oncology 2315, 2321 (2017); Christine L. M. Joseph et al., Demographic Differences in Willingness to Share Electronic Health Records in the All of Us Research Program, 29 J. Am. Med. Informatics Ass'n 1271 (2022).

[32] US Gov't Accountability Off., *GAO-21-7SP, Artificial Intelligence in Health Care: Benefits and Challenges of Technologies to Augment Patient Care* 24 (2020).

[33] The White House Off. of Sci. & Tech. Pol'y, *Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People* 5, 26–27 (2022), www.whitehouse.gov/ostp/ai-bill-of-rights/.

[34] Id.

[35] See Brian Buckley et al., Selection Bias Resulting from the Requirement for Prior Consent in Observational Research: A Community Cohort of People with Ischaemic Heart Disease, 93 Heart 1116 (2007); Sharyl J. Nass et al. (eds.), Comm. on Health Rsch. & the Priv. of Health Info.: The HIPAA Priv. Rule, *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research* 209–14 (2009), www.nap.edu/catalog/12458.html (surveying studies of consent and selection bias).

[36] 45 CFR pts. 160 and 164.

https://doi.org/10.1017/9781009373234.003 Published online by Cambridge University Press

Medical privacy law rejects control-over-information theory in favor of "privacy's other path" – confidentiality law,[37] a duty-based approach that places health care providers under duties to handle data carefully.[38] The HIPAA Privacy Rule does not itself impose any confidentiality duties. It does not need to do so, because it regulates one specific context – clinical health care – where most of the "covered entities"[39] it regulates have confidentiality duties under state law.[40]

The Privacy Rule is best modeled as what Helen Nissenbaum refers to as a contextual privacy scheme.[41] It states a set of "informational norms" – data-sharing practices that have been deemed permissible in and around clinical health care.[42] The Privacy Rule allows protected health information (PHI) to be disclosed after de-identification or individual authorization (HIPAA's name for consent).[43] This leads casual observers to think that it is a notice-and-consent privacy scheme, but it then goes on to state twenty-three additional rules allowing disclosure of PHI, often in identifiable formats, without consent but subject to various alternative privacy protections that, at times, are not as strong as one might wish.[44]

Where medical privacy is concerned, the European Union (EU)'s General Data Protection Regulation (GDPR) is more like the HIPAA Privacy Rule than most Americans realize. It grants leeway for the twenty-seven EU member states, when regulating data privacy in clinical health care settings, to go higher or *lower* than the GDPR's baseline consent standard.[45] A 2021 report for the European Commission

[37] Neil M. Richards & Daniel J. Solove, Privacy's Other Path: Recovering the Law of Confidentiality, 96 Geo. L.J. 123 (2007).

[38] See supra notes 9–13 and accompanying text.

[39] See 45 CFR § 160.102 (2018) (providing that the HIPAA regulations, including the Privacy Rule, apply to health care providers, such as physicians, clinics, hospitals, laboratories, and various other entities, such as insurers, that transmit "any health information in electronic form in connection with a transaction covered by this subchapter [the Administrative Simplification provisions of HIPAA]" and to their business associates); see also id. § 160.103 (defining the terms "covered entity" and "business associate").

[40] See Furrow et al., supra note 9.

[41] See Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (2010); Helen Nissenbaum, Privacy as Conceptual Integrity, 79 Wash. L. Rev. 119 (2004); Adam Barth et al., Privacy and Contextual Integrity: Framework and Applications, in *Proceedings of the 2006 IEEE Symposium on Security and Privacy* 184 (2006).

[42] See Evans, supra note 25, at 749–50, tbl. 1 (elaborating these norms). See also Letter from William W. Stead, Chair, Nat'l Comm. on Vital & Health Stat., to Hon. Sylvia M. Burwell, Secretary, U.S. Dep't of Health & Hum. Servs. app. A at 15–19 (November 9, 2016), www.ncvhs.hhs.gov/wp-content/uploads/2013/12/2016-Ltr-Privacy-Minimum-Necessary-formatted-on-ltrhead-Nov-9-FINAL-w-sig.pdf (https://perma.cc/J7DF-X9VP).

[43] 45 CFR § 164.502(d) (2013); see 45 CFR § 160.103 (defining "protected health information" (PHI, the information that the HIPAA Privacy Rule protects) as "individually identifiable health information" and defining the term "health information" for the purposes of the HIPAA Privacy Rule). See 45 CFR§ 164.502(a)(1)(iv) (allowing PHI to be released with individual authorization). See also id. at § 164.508 (describing the requirements for a valid individual authorization, which is HIPAA's term for a consent).

[44] Evans, supra note 25, at 749–50, tbl. 1.

[45] See Regulation 2016/679 of the European Parliament and of the Council of April 27, 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free

summarized member state medical privacy laws, which replicate many of the same unconsented data flows that the HIPAA Privacy Rule allows.[46]

The bottom line is that when you enter the clinical health care setting – whether in the United States or elsewhere – you will only have limited control over your information. A certain amount of data sharing is necessary to support the contextual goals of health care: For example, saving the life of a patient whose symptoms resemble yours by sharing your data with their physician; conducting medical staff peer review to rout out bad doctors; tracking epidemics; detecting child abuse; enabling the dignified burial of the deceased; and monitoring the safety of FDA-approved medical products. Your data can be used, with or without your consent, to do these and many other things considered essential for the proper functioning of the health care system and of society.

Notably, the HIPAA Privacy Rule takes no position on individual data ownership, so state medical records laws that vest the ownership of medical records in health care providers are not "less stringent" than HIPAA and, thus, are not preempted.[47] In many states, providers legally own their medical records, subject to various patient interests (such as confidentiality and patient access rights) in the data contained in those records.[48] Some states clarify provider ownership in their state medical records acts; others reach this conclusion through case law.[49] Only New Hampshire deems the medical information in medical records to be the property of the patient,[50] and a handful of states provide for individuals to own their genetic information.[51]

Movement of Such Data and Repealing Directive 95/46/EC, OJ 2016 No. L 119, 1. See GDPR art. 6 (requiring consent for the processing of personal data, id. § 1(a), but allowing unconsented processing for various purposes such as legal compliance, "to protect the vital interests of the data subject or another natural person," for tasks "carried out in the public interest," see id. §§ 1(b)–(f), and allowing member states to specify provisions "to adapt the applications of the rules" in some of these circumstances). See GDPR art. 9 (addressing the processing of "special categories of personal data," which include health data and requiring consent, id. § 2(a), but allowing member states to establish different conditions and safeguards for data used in "preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment, or the management of health or social care systems and services," id. § 2(h), and for public health, id. § 2(i), and for public interest purposes including scientific research, id. § 2(j)). See also GDPR art. 89 (allowing member state law to derogate from the various rights provided by the GDPR when those "rights are likely to render impossible or seriously impair the achievement" of various public-interest goals including scientific research).

46 Johan Hansen et al., *Assessment of the EU Member States' Rules on Health Data in the Light of GDPR*, Eur. Comm'n, Specific Contract No. SC 2019 70 02 (in the context of the Single Framework Contract Chafea/2018/Health/03) (2021), https://health.ec.europa.eu/system/files/2021-02/ms_rules_health-data_en_0.pdf.

47 See 45 CFR §§ 160.202–.203 (Privacy Rule preemption provisions).

48 See Am. Health Laws. Ass'n, *Health Law Practice Guide* § 4:11 (2022).

49 See, for example, *Pyramid Life Ins. Co.* v. *Masonic Hosp. Ass'n of Payne Cty.*, 191 F. Supp. 51 (W.D. Okla., 1961).

50 Am. Health Laws. Ass'n, supra note 54.

51 See Jessica L. Roberts, Progressive Data Ownership, 93 Notre Dame L. Rev. 1105, 1128 (2018) (citing five states' genetic data ownership statutes).

https://doi.org/10.1017/9781009373234.003 Published online by Cambridge University Press

What could go wrong if purveyors of digital home health devices were added to the list of covered entities governed by the HIPAA Privacy Rule? The Privacy Rule relies on an underlying framework of state laws to place its covered entities under duties of confidentiality.[52] Many sellers of home health devices are not bound by those laws. Without those laws, the Privacy Rule's liberal norms of data sharing could allow too much unauthorized data sharing.

Similar problems arose after 2013, when "business associates" were added to the list of HIPAA-covered entities.[53] Many business associates – such as software service providers offering contract data-processing services to hospitals – fall outside the scope of the state health laws that place health care providers under duties of confidentiality. The amended Privacy Rule did not address this problem adequately, leaving an ongoing privacy gap.[54]

Placing business associates – or, by analogy, digital home health care providers – under strong duties of confidentiality seemingly requires legal reforms at the state level. Federal solutions, such as HIPAA reforms or the proposed AI Bill of Rights, are not, by themselves, sufficient.

V CONTENT-BASED PRIVACY PROTECTION

A uniform scheme of content-based privacy regulations stratifies the level of privacy protection based on inherent data characteristics (e.g., data about health) without regard to where in the overall economy the data are held. The fact that Sally is pregnant receives the same protection whether it came from a home pregnancy test, a clinical diagnostic test, or a Target™ store's AI marketing algorithm.[55] This reasoning has strong superficial appeal, but there may be good reasons to distinguish health-related inferences drawn within and outside the clinical care context.

Some factors justify *stronger* privacy protections for digital home health data than for clinical health data. In clinical settings, most (not all) unconsented HIPAA data disclosures go to information fiduciaries, such as health care professionals, courts, and governmental agencies subject to the federal Privacy Act. In home care settings, the baseline assumption is that the users and recipients of people's digital health data are not information fiduciaries, which strengthens the case for strong individual control over data disclosures.

[52] See supra notes 9–13 and accompanying text.

[53] See US Dep't of Health & Hum. Servs., *Direct Liability of Business Associates* (July 16, 2021) www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/factsheet/index.html (discussing 2013 revisions to the HIPAA Privacy Rule).

[54] See Jim Hawkins et al., Non-Transparency in Electronic Health Record Systems, in *Transparency in Health and Health Care in the United States* 273, 281 (Holly Fernandez Lynch et al. eds., 2019).

[55] Charles Duhigg, How Companies Learn Your Secrets, *The New York Times Magazine* (February 16, 2012).

There can be important differences in data quality. Data generated in clinical settings is subject to regulatory and professional standards aimed at ensuring data quality and accuracy. Data generated by home health devices does not always meet these same quality standards. Digital home health data might be inaccurate, so that its release is not only stigmatizing but defamatory (false). Again, this counsels in favor of strong consent norms. Other factors might cut the other way.

The EU's GDPR and the California Consumer Privacy Act are sometimes cited as consistent, content-based privacy schemes.[56] Such schemes could offer consistency in a home care system where licensed professionals, nonmedical caregivers, and commercial device companies are all differently regulated. Yet these laws are inferior to the HIPAA Privacy Rule in various respects. An important example is the treatment of inferential knowledge. Under the GDPR, people have access to their raw personal input data but can have trouble accessing inferences drawn from those data.[57] Wachter and Mittelstadt note that "individuals are granted little control or oversight over how their personal data is used to draw inferences about them" and their "rights to know about (Articles 13–15), rectify (Article 16), delete (Article 17), object to (Article 21), or port (Article 20) personal data are significantly curtailed for inferences."[58]

The GDPR recognizes the legitimacy of competing claims to inferential knowledge. Inferences are not just a product of the input data from which they were derived, so that an inference "belongs" to the person it describes. Data handlers invest their own effort, skills, and expertise to draw inferences. They, too, have legitimate claims to control the inference. In contrast, the HIPAA Privacy Rule grants individuals a right to inspect, to obtain a copy of, and to request correction of not only their raw personal data (e.g., medical images and test results), but also the medical opinions and inferences drawn from those data.[59] This is the only informational norm in the HIPAA Privacy Rule that is mandatory: Covered entities *must* provide people with such access if they request it. The point of this example is that fact-specific analysis is needed before jumping to policy conclusions about which framework is better or worse for digital home health care.

VI CONCLUSION

This chapter ends where it began, with Solove's insight that "[n]ot all privacy problems are the same." The modern generation of digital home health devices raises novel privacy concerns. Reaching for solutions devised for other contexts – such as

[56] See supra note 45 (GDPR); California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100–.199.
[57] See generally Sandra Wachter & Brent Mittelstadt, A Right to Reasonable Inferences: Re-thinking Data Protection Law in the Age of Big Data and AI, 2019 Colum. Bus. L. Rev. 494 (2018).
[58] Id. at 494–95.
[59] See 45 CFR §§ 164.524 and .526.

https://doi.org/10.1017/9781009373234.003 Published online by Cambridge University Press

expanding the HIPAA Privacy Rule to cover digital home health providers or cloning the GDPR – may yield suboptimal policies. Consent norms, increasingly, are understood to afford weak data-privacy protections. That is especially true in digital home health care, where consent rights are not reliably backstopped by fiduciary duties limiting what data handlers can do with health data collected in people's homes. State legislation to set fiduciary duties for digital home health providers may, ultimately, be a better place to focus than on new federal privacy policies. Medical privacy law reminds us that achieving quality health care – in any context – requires an openness to responsible data sharing. Will those needed data flows exist in a world of privately sponsored digital home health tools whose sellers hoard data as a private commercial asset? The goal of a home health privacy framework is not merely to protect individual privacy; it also must enable the data flows needed to ensure high-quality care in the home health setting. At the same time, the "wild west" environment of digital home health might justify a greater degree of individual control over information than has been customary in traditional clinical care settings. Forging a workable consensus will require hard work, and the work has only just begun.

https://doi.org/10.1017/9781009373234.003 Published online by Cambridge University Press