2

Patient Access to Health Device Data

Toward a Legal Framework

Charles Duan and Christopher J. Morten

I INTRODUCTION

The connected at-home health care device industry is booming.[1] Wearable health trackers alone constituted a $21 billion market in 2020, anticipated to grow to $195 billion by 2027.[2] At-home devices now purportedly make it possible to diagnose and monitor health conditions, such as sleep apnea, diabetes, and fertility, automatically, immediately, and discreetly. By design, these devices produce a wealth of data that can inform patients of their health status and potentially even recommend life-saving actions.[3]

But patients and their health care providers often lack access to this data.[4] Manufacturers typically design connected at-home devices to store data in cloud services run by the manufacturers themselves, requiring device owners to register accounts and accept the terms of use and limitations that the manufacturers impose. A recent survey of 222 mobile "app families" associated with wellness devices found that 64.4 percent "did not report sharing any data" with other apps or services.[5] A parent testified in Congress as to how a lack of data access impaired his daughter's ability

[1] See, for example, Erin Brodwin, Remote Monitoring Is Rapidly Growing – and a New Class of Patient-Consumer Is Driving the Shift, *STAT* (September 16, 2020), www.statnews.com/2020/09/16/remote-patient-monitoring-stat-report/; Sarah Krouse, Covid-19 Pandemic Drives Patients – and Deal Makers – to Telemedicine, *The Wall Street Journal* (August 25, 2020), www.wsj.com/articles/covid-19-pandemic-drives-patients-to-telemedicine-deal-makers-too-11598358823.

[2] Fortune Business Insights, Wearable Medical Devices Market Size Worth USD 195.57 Bn by 2027, *GlobeNewswire* (March 2, 2022), www.globenewswire.com/news-release/2022/02/03/2378221/0/en/Wearable-Medical-Devices-Market-Size-worth-USD-195-57-Bn-by-2027-With-stunning-26-4-CAGR.html.

[3] I. Glenn Cohen, Sara Gerke, & Daniel B. Kramer, Ethical and Legal Implications of Remote Monitoring of Medical Devices, 98 Milbank Q. 1257, 1259 (2020).

[4] See, for example, id. at 1266–67; John T. Wilbanks & Eric J. Topol, Stop the Privatization of Health Data, 535 Nature 345, 347 (2016); Elizabeth A. Rowe, Sharing Data, 104 Iowa L. Rev. 287 (2018).

[5] Quinn Grundy et al., Tracing the Potential Flow of Consumer Data: A Network Analysis of Prominent Health and Fitness Apps, 19 J. Med. Internet Res. e233, at 4 (2017).

https://doi.org/10.1017/9781009373234.004 Published online by Cambridge University Press

to manage Type I diabetes,[6] and patients with sleep apnea have had to circumvent technological device locks to extract data on their own sleep.[7] Many medical and wellness devices that patients use for in-home diagnosis and monitoring – which we simply call "health devices" – lock patients into manufacturers' ecosystems. This limits patients', and society's, ability to tap into the full value of the data, despite the extensive individual and social benefits that access could provide.

The problem here is not solely technical; it is also legal. Existing law in the United States provides patients with no guarantee of access to their data when it is generated and stored outside the traditional health care system. The Health Insurance Portability and Accountability Act (HIPAA) provides patients a legally enforceable right of access to copies of their electronic health records (EHRs), and, in recent years, the Department of Health and Human Services (HHS) has moved to make this right enforceable and meaningful.[8] But as HHS itself has observed about health devices and other "mHealth" technologies used outside the EHR ecosystem, manufacturers "are not obligated by a statute or regulation to provide individuals with access to data about themselves," so patients with data on such devices "may not have the ability to later obtain a copy."[9]

This chapter begins by identifying the individual and societal benefits of patient access to health device data. It then addresses the arguments for restricting such access, especially those based on intellectual property laws and policies. We conclude that such arguments are ultimately doctrinally and normatively unconvincing, such that they should not dissuade legislatures and federal agencies from legislating or regulating rights of access. We then consider what can and should be done to create a robust, administrable right of patients to access health device data that protects all stakeholders' interests, and we offer a nascent framework that draws from other regimes for patient and consumer access to personal information. We hope the framework will guide legislatures and regulators as they begin to address this important issue.

II BENEFITS OF PATIENT ACCESS

There are important individual and societal benefits when patients can access their own health data. Foremost for individuals is the fulfillment of patient autonomy

[6] Smart Health: Empowering the Future of Mobile Applications, Hearing Before the Subcomm. on Rsch. & Tech. of the H. Comm. on Sci., Space and Tech., 114th Cong. 43–44 (2016) (testimony of Howard Look).

[7] Jason Koebler, Why Sleep Apnea Patients Rely on a CPAP Machine Hacker, *Vice News* (November 15, 2018), www.vice.com/en/article/xwjd4w/im-possibly-alive-because-it-exists-why-sleep-apnea-patients-rely-on-a-cpap-machine-hacker.

[8] See, for example, press release, US Dep't of Health and Human Svcs. (HHS), *Five Enforcement Actions Hold Healthcare Providers Accountable for HIPAA Right of Access* (November 30, 2021), www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf (on HHS Office of Civil Rights' HIPAA Right of Access Initiative).

[9] HHS, *Examining Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA* (2020), https://perma.cc/2JZU-DQJF.

https://doi.org/10.1017/9781009373234.004 Published online by Cambridge University Press

and dignity. Health device data informs decisions about treatment, so a patient without access can neither make fully informed decisions about a course of care nor evaluate a provider's recommendations.[10] Patients may also need access to health device data to "transport" their data to new health care providers for safekeeping,[11] or to repair their devices.[12] From a research perspective, patients can and do exploit health device data to useful ends, since their own health stands to benefit from insights and discoveries drawn from that data.[13] Many patients use health device data for "quantified self" or "n=1" research to discover how best to manage their own health.[14]

Turning to broader societal benefits, a key starting point is the research that is enabled when patient data is aggregated.[15] For example, the National Institutes of Health (NIH)-run ClinVar database receives genetic variant data authorized for inclusion by individual patients and now contains over two million records representing 36,000 different genes, which public and private enterprises have used to advance research and create consumer products and services.[16] The ClinVar model of government-supported collaborative dataset-building is one starting point for the idealistic vision of "medical information commons" – the collective, shared governance of medical knowledge (rather than proprietary or authoritarian governance of the same)[17] – that researchers and regulators alike believe would be a tremendous boon to science.[18]

[10] See generally Charlotte Blease, I. Glenn Cohen, & Sharon Hoffman, Sharing Clinical Notes: Potential Medical-Legal Benefits and Risks, 327(8) JAMA 717 (2022). For example, the US Copyright Office has observed that people with sleep apnea use "CPAP machine data to adjust their machines and enhance their treatment and health." US Copyright Office, *Section 1201 Rulemaking: Eighth Triennial Proceeding to Determine Exemptions to the Prohibition on Circumvention* 143 (October 2021) [hereinafter Eighth Triennial], https://cdn.loc.gov/copyright/1201/2021/2021_Section_1201_Registers_Recommendation.pdf. Patients cannot always "rely on the data directly provided on the machines' displays because the algorithms in CPAP machines could provide inaccurate readings." Id.

[11] See, for example, Sharona Hoffman, Access to Health Records: New Rules Another Step in the Right Direction, *JURIST* (February 20, 2019), www.jurist.org/commentary/2019/02/sharona-hoffman-health-records-proposal/.

[12] See Fed. Trade Comm'n, *Nixing the Fix: An FTC Report to Congress on Repair Restrictions* 41–42 (2021), www.ftc.gov/reports/nixing-fix-ftc-report-congress-repair-restrictions.

[13] Mary A. Majumder & Amy L. McGuire, Data Sharing in the Context of Health-Related Citizen Science, 48 J.L. Med. & Ethics 167 (2020); Sharona Hoffman, Citizen Science: The Law and Ethics of Public Access to Medical Big Data, 30 Berkeley Tech. L.J. 1741, 1755 (2015).

[14] See Melanie Swan, The Quantified Self: Fundamental Disruption in Big Data Science and Biological Discovery, 1 Big Data 85, 91–92 (2013).

[15] See Wilbanks & Topol, supra note 4.

[16] See Melissa J. Landrum & Brandi L. Kattman, ClinVar at Five Years: Delivering on the Promise, 39 Hum. Mutation 1623, 1625 (2018); ClinVar Submissions, Nat'l Lib. Med. (last visited April 19, 2022), www.ncbi.nlm.nih.gov/clinvar/submitters/.

[17] Katherine J. Strandburg, Brett M. Frischmann, & Michael J. Madison, The Knowledge Commons Framework, in *Governing Medical Knowledge Commons* 9 (Katherine J. Strandburg, Brett M. Frischmann, & Michael J. Madison eds., 2017).

[18] See, for example, Jorge L. Contreras, Leviathan in the Commons: Biomedical Data and the State, in *Governing Medical Knowledge Commons* 19 (Katherine J. Strandburg, Brett M. Frischmann, &

Research on aggregated health data also allows patient groups and civil society watchdogs to verify manufacturers' claims and ensure that health devices function as advertised – especially important given that those devices are only lightly regulated.[19] Aggregated health device data also promises to become a variety of the "real-world evidence" increasingly used to conduct public health research and validate the safety and efficacy of other products the same patients are using.[20] But these potential benefits depend on patient data aggregated at a sufficient scale.[21]

Societal spillover effects explain, at least in part, why market forces do not prompt manufacturers to satisfy patient demand for data access. Patient self-researchers tend to be consumer-innovators who share their insights and discoveries altruistically, at low or no cost, which may undercut the manufacturers.[22] And the value of aggregated patient data cannot easily be captured by a single entity. As a result, there is no straightforward way for patients and health device manufacturers to transact for data access.

Another economic disconnect arises from competition among device manufacturers. When patients can easily extract their data from one device and port it to a competing device, they avoid "lock-in," which promotes patient choice and fosters competition.[23] In an effort to avoid such competition, however, device manufacturers have incentives to limit patient data access. Indeed, some have implemented technical measures to keep even savvy patients from extracting data and asserted laws against the circumvention of those technological measures to further keep patients from their data.[24]

III LEGALITY OF PATIENT ACCESS

To be sure, there are real concerns with giving patients access to health device data.[25] Device manufacturers have pointed to these as reasons to limit such access. The main concerns fall into three categories.

Michael J. Madison eds., 2017) (on government's role in fostering public medical databases); Critical Path Inst., Rare Disease Cures Accelerator-Data and Analytics Platform, https://c-path.org/programs/rdca-dap/ (exemplary FDA-funded effort).

[19] See Rowe, supra note 4, at 313.

[20] Sanket S. Dhruva et al., Real-World Evidence: Promise and Peril for Medical Product Evaluation, 43 PT 464, 469 (2018).

[21] See, for example, Barbara J. Evans, Genomic Data Commons, in *Governing Medical Knowledge Commons* 74, 81 (Katherine J. Strandburg, Brett M. Frischmann, & Michael J. Madison eds., 2017) (on the "data access challenge").

[22] See Eric von Hippel, *Democratizing Innovation* 77–91 (2005).

[23] David Blumenthal, A Big Step Toward Giving Patients Control over Their Health Care Data, *Harvard Business Review* (March 15, 2019), https://hbr.org/2019/03/a-big-step-toward-giving-patients-control-over-their-health-care-data.

[24] See Wilbanks & Topol, supra note 4.

[25] By "access" to their own data, we mean not just patients' ability to view their own data, but also their ability to download it, to archive it, and to share it.

First, there are costs associated with authenticating users, formatting data, and otherwise providing access to records. This problem can be solved by permitting reasonable, small charges for data access.[26]

Second, device manufacturers may be better stewards of sensitive health data than patients, in terms of privacy and cybersecurity.[27] In theory, manufacturers enjoy economies of scale that enable them to protect health records from data breaches and other compromising disclosures, while individual patients may fail to secure their data or fall victim to privacy-invading scams. Yet, there are countervailing considerations: Manufacturers' vast databases are themselves an attractive and recurring target for data malfeasance,[28] and some manufacturers' shady deals with privacy-intrusive data brokers suggest that companies holding volumes of lightly regulated personal data may not be better positioned than patients to protect data security and privacy.[29]

The third concern often raised as a reason to limit patient access is that the data is somehow proprietary to the device manufacturers. This intellectual property concern requires a bit of conceptual unpacking, as it operates on two different levels. First, it is a *legal* or *doctrinal* argument, in which the manufacturers assert specific intellectual property rights over the data. Second, it is a *normative*, *policy-oriented* argument that exclusive control over patient data is desirable to protect incentives to develop health devices and data ecosystems.

Evaluating these arguments requires distinguishing the types of health device data. First, there is the software code that the device manufacturer writes. Second, the device takes the raw measurements of the patient and stores them. Third, the device (or external software) may perform computations on the raw data to produce values intended to approximate a natural phenomenon, such as a pulse. Fourth, the device may compute data outputs of the manufacturer's own invention. For example, a device might use pulse measurements across a night to produce a "sleep score," indicating how well, in the manufacturer's opinion, the patient slept, and offer recommendations on how to sleep better.[30]

[26] See 45 CFR § 164.524(c)(4) (providing for a "reasonable, cost-based fee" for patient data access under the HIPAA).

[27] See Cohen et al., supra note 3, at 1282–83.

[28] FDA Issues New Alert on Medtronic Insulin Pump Security, *Healthcare IT News* (July 1, 2019), www.healthcareitnews.com/news/fda-issues-new-alert-medtronic-insulin-pump-security; Joe Carlson, FDA Says Pacemakers, Glucose Monitors and Other Devices Could Be Vulnerable to Hackers, *Star Tribune* (March 3, 2020), www.startribune.com/fda-says-pacemakers-glucose-monitors-and-other-devices-could-be-vulnerable-to-hackers/568452772/.

[29] Joseph Cox, How the US Military Buys Location Data from Ordinary Apps, *Vice News* (November 16, 2020), www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x; Alfred Ng & Jon Keegan, Who Is Policing the Location Data Industry?, *The Markup* (February 24, 2022), https://themarkup.org/ask-the-markup/2022/02/24/who-is-policing-the-location-data-industry.

[30] See, for example, Larry Magid, Devices Measure Quantity, Quality of Sleep, *Mercury News* (December 21, 2018), www.mercurynews.com/2018/12/20/magid-devices-measure-quantity-quality-of-sleep/.

Our focus is the second and third types of information – raw measurements and computed estimates of physiological properties – because they are likely to be of the most interest to patients. We therefore refer hereinafter to these two types of data together simply as "patient data." With access to this patient data, patients likely will not need to view source code on the device to put the data to use. Manufacturer-specific computations and scores are likely not useful for cross-device interoperability, and the black-box nature of the algorithms often used to compute such scores limits their usefulness for care and research alike.[31]

Two intellectual property regimes are most frequently raised to justify withholding patient data from patients: Copyright law and trade secret protection.[32] Yet neither provides a genuine doctrinal basis for "ownership" of patient data or barriers to patient access.

Copyright law, which protects creative works of authorship from unauthorized copying, almost certainly cannot justify withholding patient data. Raw physiological measurements and estimates of natural phenomena are facts, ineligible for protection under copyright.[33] Furthermore, given the immense health benefits that patients can enjoy from their own data, data access likely qualifies as fair use, exempt from copyright infringement.[34] Indeed, the US Copyright Office has consistently agreed since 2015 that patient access to medical device data is not copyright infringement, thus, permitting patients to circumvent the technological locks that interfere with their access to data on medical devices.[35]

Nor is patient data a trade secret. First, every legal definition of a trade secret requires the information in question be *secret* to qualify for protection.[36] Patient data

[31] To be sure, patient access to these types of information would be useful in some situations, such as testing the reliability of manufacturers' invented health "scores." The nature of proprietary rights over device source code and manufacturer-specific computed data is an important area for further research.

[32] See, for example, Timo Minssen & Justin Pierce, Big Data and Intellectual Property Rights in the Health and Life Sciences, in *Big Data, Health Law, and Bioethics* 307 (I. Glenn Cohen et al. eds., 2018); Rowe, supra note 4, at 299–301 (2018); Comments of AdvaMed and Medical Imaging and Technology Alliance opposing the 1201 exemption at 5 (2015), https://cdn.loc.gov/copyright/1201/2015/comments-032715/class%2025/AdvaMed_Class25_1201_2014.pdf [hereinafter AdvaMed-MITA 2015]. Cf. *Med. Imaging & Tech. All.* v. *Libr. of Cong.*, no. 1:22-cv-00499 (DDC filed February 25, 2022) (ongoing litigation alleging, *inter alia*, that the US Copyright Office violates copyright law by authorizing repair personnel to circumvent technical "locks" on health devices) [hereinafter MITA litigation].

[33] See *Feist Publ'ns, Inc.* v. *Rural Tel. Serv. Co.*, 499 US 340, 345 (1991); US Copyright Office, *Section 1201 Rulemaking: Sixth Triennial Proceeding to Determine Exemptions to the Prohibition on Circumvention* 393 (October 2015). See also, for example, *Midler* v. *Ford*, 849 F.2d 460 (9th Cir. 1988) (holding voices uncopyrightable); US Copyright Office, in *re Second Request for Reconsideration for Refusal To Register Equilibrium* (2020), www.copyright.gov/rulings-filings/review-board/docs/equilibrium.pdf, at 5 (concluding fingerprints are uncopyrightable).

[34] See Eighth Triennial, supra note 10.

[35] Id. But see MITA litigation, supra note 32 (alleging that the US Copyright Office erred in permitting repair personnel to do so).

[36] See, for example, 18 USC 1839(3)(B) (federal definition); UTSA § 1.4 (definition common in state law).

https://doi.org/10.1017/9781009373234.004 Published online by Cambridge University Press

of all sorts is shared with patients, health care providers, and others and, thus, is not actually secret. Second, even if subsets of patient data are kept secret, they are not the sort of information that trade secrecy law protects. To qualify as a trade secret, information must derive "independent economic value" from its secrecy.[37] As Hrdy has explained, "secret information *whose value does not stem from secrecy* cannot be a trade secret."[38] Unlike traditionally protectable information – manufacturing processes, precise recipes, and so on – patient data derives economic value from aggregation and sharing, not secrecy.[39]

To be sure, some (nonpatient data) aspects of devices' software and mechanical designs may be deemed trade secrets.[40] The European Medicines Agency (EMA) offers helpful guidance here, in its official view of the limits of trade secrecy protection of clinical trial data.[41] (Like the patient data that is the focus of this chapter, clinical trial data describes patients' health and is enormously valuable to researchers and patients themselves.) EMA announced that a large majority of clinical trial data "should not be considered" proprietary.[42] In EMA's view, only "innovative features" of the methods *through which data is collected* can constitute trade secrets.[43] EMA expressly defines narrow categories of information it deems innovative and protectable.[44] These focus on methods for gathering data more quickly or cheaply, such as immunogenicity assays.[45] Notably, EMA's categories do *not* permit proprietary claims to the outcome data that describes patients' health (analogous to health devices' patient data); EMA instead mandates that all outcome data be publicized.[46]

[37] Id.

[38] Camilla Alexandra Hrdy, The Value in Secrecy, 91 Fordham L. Rev. 557, 596 (2022).

[39] Id. See also, for example, *Yield Dynamics, Inc.* v. *TEA Sys. Corp.*, 154 Cal. App. 4th 547, 561 n.13, 564–65, 566–67 (2007) (holding a company's software not a trade secret, despite secrecy and economic value, because the software was built on a combination of open-source and secret code and the company had not proven that economic value derived from continued secrecy).

[40] See, for example, AdvaMed-MITA 2015, supra note 32, at 5–6 (asserting trade secret rights in the source code in medical devices).

[41] Eur. Med. Agency, *External Guidance on the Implementation of the European Medicines Agency Policy on the Publication of Clinical Data for Medicinal Products for Human Use* (2018) [hereinafter EMA], https://perma.cc/28UL-6ZQK.

[42] Id. at 52.

[43] Id. at 54.

[44] Eur. Med. Agency, *Policy on Publication of Clinical Data for Medicinal Products for Human Use* Annex 3 (2019) [hereinafter EMA 2019], www.ema.europa.eu/en/documents/other/european-medicines-agency-policy-publication-clinical-data-medicinal-products-human-use_en.pdf; Regulation 536/2014, of the European Parliament and of the Council of April 16, 2014 on Clinical Trials on Medicinal Products for Human Use and Repealing Council Directive 2001/20/EC Text with EEA relevance, O.J. (L 158) 1, 1–76.

[45] EMA 2019, supra note 44, at Annex 3.

[46] EMA, supra note 41, at 58. The NIH apparently shares the EMA's view. See 81 Fed. Reg. 64,982, 64,996–97 (stating that "trial results in summary form" "can be provided without disclosing trade secret or confidential commercial information").

What remains of health device manufacturers' intellectual property claims is a normative argument that data inaccessibility gives manufacturers incentives to innovate.[47] Yet, there are serious defects to this normative argument. First, patients themselves have a countervailing incentive to innovate – their own health depends on it. Second, the "innovation" manufacturers wish to protect may not be beneficial at all: Secrecy can conceal safety problems, false claims of efficacy, racially biased outcomes, and other defects. Normatively and doctrinally, trade secrecy should not and does not protect this kind of secrecy.[48] As the Supreme Court has stated, if the disclosure of secret information reveals "harmful side effects of the [trade secret holder's] product and causes the [holder] to suffer a decline in the potential profits from sales of the product, that decline in profits stems from a decrease in the value of the [product] to consumers, rather than from the destruction of an edge the [holder] had over its competitors, and cannot constitute the taking of a trade secret."[49]

IV TOWARD A REGULATORY FRAMEWORK

Although we have argued patients should have access to health device data as a legal and policy matter, the practical fact remains that manufacturers are currently free to build devices that deny such access at a technological level. There is, thus, a need for a legal framework to secure such access. No such framework currently exists: The existing regulations are generally limited to narrow classes of medical records or apply only to traditional health care providers and some of their business associates.

To develop an effective framework, it is useful to survey existing consumer data-access regimes both within the health care system and otherwise. We arrange them into three categories, roughly ranked by the strength of their mandates.

The most powerful regimes mandate patients' right to data access. The HIPAA Privacy Rule provides patients with "a right of access to inspect and obtain a copy of protected health information" from health care providers.[50] Similarly, European law and the laws of some states provide consumers with rights to retrieve

[47] Manufacturers tend to emphasize the policy argument that innovation could suffer without strengthened intellectual property protection of some sort – perhaps acknowledging that existing doctrine does not prohibit patients from accessing patient data. See, for example, 2015 comments of AdvaMed opposing the 1201 exemption, https://cdn.loc.gov/copyright/1201/2015/comments-032715/class%2027/AdvaMed_Class27_1201_2014.pdf, at 7 (asserting vaguely that patient access "poses trade secrecy concerns" while insisting "trade secrets may be the only viable form of protection for companies conducting research and development in this area").

[48] See Hrdy, supra note 38, at 7–8 (discussing "type failures"); Sharon Sandeen, Out of Thin Air: Trade Secrets, Cybersecurity, and the Wrongful Acquisition Tort, 19 Minn. J.L. Sci. & Tech. 373 (2018); Amy Kapczynski, The Public History of Trade Secrets, U.C. Davis L. Rev. 1367, 1429–36 (2022).

[49] *Ruckelshaus* v. *Monsanto Co.*, 467 U.S. 986, 1011 n.15 (1984). See also *Pub. Citizen Health Rsch. Grp.* v. *FDA*, 704 F.2d 1280, 1291 n.30 (D.C. Cir. 1983).

[50] 45 CFR § 164.524.

https://doi.org/10.1017/9781009373234.004 Published online by Cambridge University Press

data about themselves.[51] These laws employ a range of enforcement mechanisms, including civil actions by consumers, state attorney general investigations, and administrative monetary penalties. For example, the HHS's Office for Civil Rights recently began penalizing HIPAA-covered health care providers that fail to supply patients' protected health information upon request or charge excessive fees for them,[52] prompting improvement after years of subpar compliance.[53]

A second approach is softer financial incentives and disincentives – "carrots" and "sticks" – to encourage data holders to offer access. This was the primary approach used for the adoption of EHRs: The HITECH Act of 2004 both offered providers incentive payments for adopting certified EHR systems in their practices, and imposed a modest penalty on Medicare reimbursements for providers who did not.[54] Today, after billions of dollars of investment by HHS, the vast majority of providers have adopted EHRs,[55] and those systems largely comply with HHS's voluntary certification standards because the financial benefits created sufficient demand.[56] HHS's ongoing ability to set certification standards has enabled the agency to require EHR systems to export data in standardized interoperability formats, to expose application programming interfaces for data access, and to stop companies' "information blocking" practices that hamper patients' ability to access their own health records.[57]

A third possibility is to build public infrastructure or subsidize private infrastructure that coordinates patient data access. With ClinVar, for example, genetic testing laboratories voluntarily submit annotated reports of genetic variants to an NIH-run database, with patient consent. They make these voluntary submissions because, among other reasons, foundations and publishers often require them as a condition of grants or publication.[58] The presence of established, stable, government-supported infrastructure for data sharing makes such data submission requirements more common and more effective. In this way, legislatures and regulators can incentivize data sharing even without direct regulation.

[51] See, for example, Cal. Civ. Code § 1798.100(a); GDPR art. 15.

[52] Jennifer J. Hennessy et al., HIPAA Right of Access Initiative: 2020 Year in Review, *The National Law Review* (December 11, 2020), www.natlawreview.com/article/hipaa-right-access-initiative-2020-year-review.

[53] Carolyn T. Lye et al., Assessment of US Hospital Compliance with Regulations for Patients' Requests for Medical Records, 1 JAMA Netw. Open e183014 (2018).

[54] Centers for Medicare and Medicaid Services, Medicare and Medicaid Programs, Electronic Health Record Incentive Program Final Rule, 75 Fed. Reg. 44,314 (July 28, 2010).

[55] HHS Office of the Nat'l Coordinator for Health Info. Tech. (ONC), *HealthIT Quick Stat #61: National Trends in Hospital and Physician Adoption of Electronic Health Records*, www.healthit.gov/data/quickstats/national-trends-hospital-and-physician-adoption-electronic-health-records. ("As of 2019, about three-quarters of office-based physicians (72%) and nearly all non-federal acute care hospitals (96%) had adopted a certified EHR.")

[56] Id.

[57] 21st Century Cures Act Final Rule, 85 Fed. Reg. 25642 (May 1, 2020) (codified at 45 CFR pts. 170, 171).

[58] See Karen E. Wain et al., The Value of Genomic Variant ClinVar Submissions from Clinical Providers: Beyond the Addition of Novel Variants, 39 Hum. Mutation 1660, 1661 (2018).

We integrate aspects from these regimes into a nascent framework for patient access to at-home health care device data. Our framework-in-progress has three elements: A legal hook to induce device manufacturers to make patient data accessible to patients, a technical standard for data storage and access, and infrastructure for patients to deposit and use their data.

As to the first element, legislation or regulation to compel access, akin to HIPAA, would be most forceful and effective. For example, in 2019, Senators Klobuchar and Murkowski proposed creating a HIPAA-like statutory right of patients "to access, amend, and delete a copy of the personal health data that companies collect or use,"[59] including data from all "cloud-based or mobile technologies that are designed to collect individuals' personal health data."[60]

US states also have substantial authority to legislate around HIPAA and could themselves create statutory patient-data access rights. Texas, for example, subjects some HIPAA-exempt entities, such as schools and public health researchers, to some of the obligations that HIPAA imposes.[61] The California Consumer Privacy Act (CCPA) arguably creates a right of access to health device data not covered by HIPAA, though this theory is so far untested.[62]

Federal regulators could also explore their existing legal authority to require device manufacturers to share data. For example, the Federal Trade Commission could apply its authority to police unfair and deceptive practices to health device makers that market patient access to data as a feature of their products and require that these companies meet their claims.[63]

Alternatively, following the example of the HITECH Act, Congress could provide financial incentives for health devices that meet data access standards, for example, making such devices reimbursable under Flexible Spending Account (FSA) plans or Medicare. A different, intriguing possibility could leverage the status quo of minimal regulation to create new financial incentives and disincentives. Current Food and Drug Administration (FDA) guidance exempts health devices from clearance and approval requirements only if they "present a low risk to the safety of users and other persons."[64] As noted above, patients' data access can enable researchers to

[59] Protecting Personal Health Data Act, S. 24, 117th Cong. (2021); press release, *Klobuchar, Murkowski Introduce Legislation to Protect Consumers' Private Health Data* (February 2, 2021), www.klobuchar.senate.gov/public/index.cfm/2021/2/klobuchar-murkowski-introduce-legislation-to-protect-consumers-private-health-data.

[60] S. 24, supra note 59.

[61] See Tex. Health & Safety Code Ann. §§ 181.001(b)(2)(A) (defining a "covered entity" under Texas law).

[62] Jonathan Deitch, Protecting Unprotected Data in Mhealth, 18 Nw. J. Tech & Intell. Prop. 107 (2020); see also Cohen et al., supra note 3, at 1276.

[63] HHS ONC, *Conceptualizing a Data Infrastructure for the Capture, Use, and Sharing of Patient-Generated Health Data in Care Delivery and Research Through 2024* 23 (January 2018), www.healthit.gov/sites/default/files/onc_pghd_final_white_paper.pdf.

[64] US Food and Drug Admin., *General Wellness: Policy for Low-Risk Devices* 2 (September 26, 2019), www.fda.gov/media/90652/download.

study the safety risks of devices, so it could be reasonable for the FDA to change its policies and extend a presumption of safety (and thus of exemption from regulation) only to those devices that make data accessible to patients – and perhaps to qualified researchers, too. Manufacturers that choose to withhold data would not be, per se, prohibited from marketing their products, but would be subject to stricter FDA oversight, which would come with new costs.

The second element of the framework is a technical standard to govern how data is to be stored and accessed. Since health devices typically store data in manufacturers' cloud servers, there is little sense in requiring less than electronic access via a network-connected application programming interface, akin to the requirements for EHR systems. Furthermore, both research and interoperability would benefit from greater standardization of data formats, in light of the profusion of health devices and manufacturers.[65] HHS and its Office of the National Coordinator for Health Information Technology could play an important role here, as it did in the standardization of EHRs.

The third element is an institutional infrastructure for aggregating and sharing data. We propose a public, ClinVar-like repository of patient-authorized submissions of appropriately anonymized device data. Without such a repository, patient access and data interoperability will likely still enable new research and other benefits for patients, but they also could augment the power of firms that amass data and broker access. A government-run repository of patient data arguably has several benefits. As a focal point for data aggregation, it empowers all researchers, not just the largest firms. Also, firms that contribute to this central repository share a relationship with the government that could be leveraged to ensure data privacy and security. And a public repository enables the government and outside experts to think through and develop privacy practices that best protect patients, rather than leaving these questions, in the first instance, to profit-driven firms.

V CONCLUSION

In this chapter, we have argued for a legal right of patients to access their own health device data. We have begun to trace a legal framework for access, one that includes three key elements: A legal "hook" to coax or compel device manufacturers to share data with patients, a technical standard to govern how data is stored and accessed, and an institutional infrastructure for aggregating and sharing data. We intend to expand on this framework in future work.

[65] See Dov Greenbaum, Avoiding Overregulation in the Medical Internet of Things, in *Big Data, Health Law, and Bioethics* 129, 138 (I. Glenn Cohen et al. eds., 2018).