The Perils of Parity: Should Citizen Science and Traditional Research Follow the Same Ethical and Privacy Principles?

Barbara J. Evans

Introduction

Some observers have questioned whether ethical and privacy principles developed for traditional research contexts are appropriate in the starkly different setting of citizen science. Rothstein et al. observed in 2015 that some scholars question "whether unregulated, citizen science health research containing few of the characteristics of the researcher-participant relationship would give rise to comparable ethical obligations to disclose incidental findings."[1] Patrick-Lake and Goldsack more recently noted an alarming ethics gap for citizen science and called for tailored efforts to address the special ethical challenges it presents.[2]

An alternative view is that ethical and privacy rights and duties are not, or should not be, context-dependent. By this view, there should be parity between the rights people have, regardless of whether they are participating in traditional research at an academic medical center or in citizen science unregulated by the Common Rule,[3] the FDA's research regulations,[4] or the Health Insurance Portability and Accountability Act (HIPAA)[5] Privacy Rule.[6] Thus, if people have a right of access to their data in traditional research contexts, they seemingly deserve that same right in citizen science.

This article offers a cautionary example of why, in practice, parity might be hard to achieve. The chosen example involves privacy-related rights of access to one's own data. These privacy-enabling access rights are frequently (and erroneously) conflated with the return of results, understood here as the sharing of interpreted results and incidental or secondary findings with research participants. There is a superficial resemblance in that privacy-related access rights and return of results both move information into research participants' hands. Yet they have distinct legal and ethical foundations and serve objectives that overlap somewhat but ultimately are distinct.[7] This article is not about return of results, which Susan Wolf discusses in a separate article in this issue.[8]

Privacy-related access rights have been a fixture of U.S. federal privacy laws dating back to the early 1970s, as seen in the Fair Credit Reporting Act of 1970[9] and the Privacy Act of 1974,[10] the latter having inspired the individual access right[11] that now adorns the HIPAA Privacy Rule. The congressional and regulatory purposes of privacy-related access rights are clearly enunciated and include, most prominently, enhancing privacy protections and enabling people to provide informed consent to secondary uses of their stored data.[12] Unless people can find out how much data is stored about them, they have no way to assess the level of privacy risk to which they are exposed or how well their privacy is being protected.[13] When designing the HIPAA Privacy Rule, the U.S. Department of Health and Human Services (HHS) also noted that the "decision whether to disclose a record may depend on what the record says, and so access to the record is integral to making an informed choice to disclose [personal information]."[14] This notion that individual data access is integral both to privacy and to informed consent is also recognized in European law[15] and in the privacy laws of some U.S. states.[16]

Unregulated research that uses mobile health data raises major privacy concerns that Rothstein et al. highlight in a companion article in this issue.[17] A related concern is that mobile health devices and

Barbara J. Evans, Ph.D., J.D., LL.M., *is the Mary Ann and Lawrence E. Faust Professor of Law, a Professor of Electrical and Computer Engineering, and the Director of the Center for Biotechnology & Law at the University of Houston.*

The Journal of Law, Medicine & Ethics, 48 S1 (2020): 74-81. © 2020 The Author(s)
DOI: 10.1177/1073110520917031
https://doi.org/10.1177/1073110520917031 Published online by Cambridge University Press

research applications (hereinafter, "apps") that process data from them, in many instances, are not subject to the HIPAA Privacy Rule. Consequently, individuals often lack HIPAA's privacy-enabling right of access to their own data. Without access rights, privacy protections are inherently incomplete, and informed consent is undermined by people's ignorance about the types of data they are consenting to share.

This article briefly describes the individual access right that exists in HIPAA-regulated research contexts. It then describes the spotty individual access rights in non-HIPAA-covered mobile health data environments. Providing a HIPAA-equivalent individual access right in mobile health research is simple in theory but raises thorny Food and Drug Administration (FDA) regulatory compliance issues that might chill citizen science. Individual access rights provide a cautionary example of how efforts to achieve parity can invite unintended consequences.

Parity of ethical and privacy rights and duties across research contexts sounds desirable. There is something in humans that yearns for our ethical principles to be universal and immune to vagaries of context, time, and place. Yet universality is hard to implement when contextual variations are real. Crafting context-appropriate ethical and privacy solutions requires a willingness to revisit and possibly to adjust the basic principles that inform(ed) the ethical conduct of (yesterday's) research.

Parity of ethical and privacy rights and duties across research contexts sounds desirable. There is something in humans that yearns for our ethical principles to be universal and immune to vagaries of context, time, and place. Yet universality is hard to implement when contextual variations are real. Crafting context-appropriate ethical and privacy solutions requires a willingness to revisit and possibly to adjust the basic principles that inform(ed) the ethical conduct of (yesterday's) research.

Scope of the Privacy Rule's Individual Data Access Right

Section 164.524 of the Privacy Rule grants people a right to inspect and receive copies of data identifiable to themselves if the data are maintained by a HIPAA-covered entity, such as a clinic, hospital, clinical laboratory, and some but not all research laboratories. The "designated record set" (DRS) refers to the data to which an individual has access under HIPAA.[18] The DRS includes much of the data stored in a covered entity's files that can be traced to the requesting individual.[19] It includes all records "[u]sed, in whole or in part ... to make decisions about individuals."[20] HHS has emphasized that this includes data used in non-medical as well as medical decision-making, and the DRS includes data the covered entity uses to make decisions about *any* individuals, even if the data were not so used when making decisions about the person requesting the data.[21] For example, if a hospital ever uses blood pressure data to make decisions about any of its patients, you could access your own blood pressure data stored in your medical records, even if blood pressure was not relevant to any decisions the hospital made in the course of treating you.

A person's DRS is not limited to clinically significant information and might include, for example, speculative notes included in a patient's chart or individual research results stored in a person's files at a HIPAA-covered institution.[22] Any information that is ascribed to a person carries potential privacy concerns and might lead to discrimination or stigmatization. Low-quality data can be as stigmatizing as high-quality data, and sometimes even more so. Accordingly, the DRS for laboratory data "includes not only the laboratory test reports but also the underlying information generated as part of the test, as well as other information concerning tests a laboratory runs on an individual."[23] HHS has clarified that the DRS for genomic testing includes "the completed test report, the full gene variant information generated by the test, as well as any other information in the designated record set concerning the test."[24]

HIPAA's access right is subject only to a few exceptions and they are narrow.[25] For example, the Privacy Rule lets HIPAA-covered research institutions suspend research participants' access rights temporarily during a clinical trial.[26] However, this exception allows research data to be withheld only if the individual consented to the access denial when consenting to the research,[27] and access must resume as soon as

The Journal of Law, Medicine & Ethics, 48 S1 (2020): 74-81. © 2020 The Author(s)

https://doi.org/10.1177/1073110520917031 Published online by Cambridge University Press

the trial is complete.[28] The existence of this exception confirms HIPAA's general rule, which is that research data raise privacy concerns, and people need access in order to understand and manage their privacy risks and to grant truly informed consents for secondary uses of the data. Moreover, HIPAA's access right is an important lever people can use to free their data for use in other research projects.

Individual Access Rights in Non-HIPAA Mobile Health Research Environments

This article adopts Wiggins' and Wilbanks' definition of citizen science as "a range of participatory models for involving non-professionals as collaborators in scientific research."[29] This concept is broad and encompasses the upper three of four tiers of participation that Bobe et al. recently described,[30] drawing on Arnstein's "ladder of participation."[31] The traditional 20th-century research model for which regulations like the Common Rule were originally conceived presumed the lowest level of participation, rife with informational and power asymmetries, in which research was done *to you*.[32] Citizen science, as described by Wiggins and Wilbanks, embraces three higher levels of participation, in which research is done *for you* (as when a patient advocacy or family group commissions professional researchers to study a particular question or assembles data and tissue specimens to aid such research), or *with you* (as when a scientist or research app developer engages research participants as active partners in research), or even *by you* (as in a do-it-yourself project, where the participants *are* the researchers).[33] Rothstein et al. explain why such research often escapes regulation under the Common Rule, the FDA's research regulations, and the HIPAA Privacy Rule.[34]

Outside the HIPAA-regulated environment, individuals' access to their personal health data grows dicey. Unless users happen to enjoy state-law protections that include access rights, the users must rely primarily on the law of contract: privacy policies stated in companies' end-user agreements and terms of use that many users click through without reading.

Scott Peppet surveyed the privacy policies of twenty popular consumer sensor devices and found only four that addressed data ownership.[35] Three of those four asserted that the sensor manufacturer/app developer (hereinafter, "mobile health company"), rather than the user, owns data that the sensor generates, with some asserting that the company has "sole and exclusive" ownership. Such assertions are legally questionable, but it is fair to say that mobile health companies that gather and store people's data enjoy a level of control that is tantamount to ownership. The information they store is "out of circulation even though it is not, strictly speaking, owned"[36] and many mobile health companies and app developers treat personal data "as if it were their private property."[37]

Professor Peppet notes the potential for "sensor fusion," in which "information from two disconnected sensing devices can, when combined, create greater information than that of either device in isolation."[38] For example, fitness tracker data on heart rate and respiration — each innocuous and hardly stigmatizing in itself — can, when combined, allow inferences about substance abuse.[39] Linking sensor data that reflect lifestyle, exposures, and environment to traditional health and genomic data, as some mobile research apps seek to do, could compound these privacy concerns.

To appreciate their privacy risks, users need access to the data that mobile health companies, including research app developers, gather and store. People also need to understand how their data might be shared with third parties. As for individual access, Professor Peppet's survey found that policies announced in end-user agreements and terms of service were inconsistent concerning individual access to, and exportation of, one's own raw sensor data.[40] In contrast to the HIPAA-regulated space, users have limited individual access rights that, all too often, are badly described. For example, some companies' policies allow user access to personally identifying information (PII) but not to non-PII,[41] while failing to define either of these terms. Does PII only include the user's name and other overt identifiers, or is sensor data considered PII if it is re-identifiable?[42]

As in the HIPAA-regulated space, re-identification of mobile health data is a growing concern. Professor Peppet cites an intelligence source for the proposition that if a fitness tracker reveals the gait at which a person walks, unique individual identification may be feasible.[43] Failure to define PII leaves the scope of a user's access rights indefinite. Professor Peppet cites Debjanee Barua et al. for the proposition that users want to be able to obtain copies of their data: "This is the simplest level of control over one's data—the ability to inspect, manipulate, and store your own information. But it's not usually possible."[44]

Mobile health companies often reserve the right to share or sell people's non-personal information (non-PII) more broadly than their PII, but these same uncertainties leave users guessing which types of personal data might be shared with third-party researchers.[45] Absent a clear policy to the contrary and absent relevant state privacy protections, users should assume that a company's promise not to share PII amounts to

The Journal of Law, Medicine & Ethics, 48 S1 (2020): 74-81. © 2020 The Author(s)
https://doi.org/10.1177/1073110520917031 Published online by Cambridge University Press

a promise to strip consumers' data of overt identifiers before it is shared.

In principle, these problems have a straightforward solution. Where the law of contract governs, problems can be resolved by agreement of the parties without recourse to ponderous legislative and regulatory solutions. As a group, people who use mobile health devices — and, in particular, those who participate in citizen science projects — are an educated, empowered lot.[46] Mobile health companies face strong incentives to be responsive to their users. If users demand HIPAA-equivalent individual access rights and boycott mobile health companies that do not grant them, the problem seemingly can be solved. Unfortunately, this approach raises potential FDA compliance issues for developers of research apps that harness data from mobile health devices.

FDA Oversight of Software Used in Mobile Health Research

This section explores the impact of the FDA's medical device and research regulations on a software developer that creates a research software platform to gather and study data from participants' mobile health devices. Let us assume the mobile health devices are of a sort — for example, fitness trackers — that qualify as general wellness devices that the FDA does not regulate as medical devices. In 2013 and 2015 guidance documents, the FDA indicated it would regulate such products only if they performed medical device functions that might pose a safety risk if the mobile product failed to function as intended.[47] The 21st Century Cures Act of 2016[48] confirmed that the FDA lacks authority to regulate software for encouraging wellness or a healthy lifestyle, unless the software crosses the line into "diagnosis, cure, mitigation, prevention, or treatment of a disease or condition."[49] In September 2019, the FDA issued final guidance clarifying the line between regulated and non-regulated wellness software after 21st Century Cures.[50]

This discussion assumes the mobile health company that supplies the fitness tracker has positioned its product as a low-risk general wellness device by adhering to the FDA's guidance regarding appropriate claims for such devices. For example, the mobile health company markets its product as a fitness tracker for use by healthy people to log their maximum heart rate and aerobic fitness while exercising. With these claims, the fitness tracker is exempt from FDA oversight.

The research app developer creates a new software platform that gathers data from people's fitness trackers and conducts research using those data. The study participants are people who own the fitness tracker and agree to download their data into the research software, which mines the data to discover new associations between people's daily heart rate history and various medical conditions. For example, the research software might search for patterns of heart activity that diagnose or predict various health events, such as asthma attacks or strokes.

The question is whether the FDA can regulate the research software platform as a medical device, or at least regulate the human-subject research that relies on the platform. In recent years, the FDA has asserted authority to regulate "software as a medical device" (SaMD), which is "software intended to be used for one or more medical purposes that perform these purposes without being part of a hardware medical device."[51] Such software "utilizes an algorithm (logic, set of rules, or model) that operates on data input (digitized content) to produce an output for a medical use specified by the manufacturer."[52]

There are two ways to characterize the research app developer's activities, and both carry a risk that the software developer might fall under the FDA's medical device regulations unless the developer proceeds very carefully. The first characterization is that the research app developer is repurposing fitness trackers that are lawfully marketed as general wellness devices, altering their intended use and thereby transforming them into a new medical device capable of diagnosing or predicting health conditions such as asthma attacks and strokes. The FDA's intended use regulation at 21 C.F.R. § 801.4 states that a party who alters the intended use of an existing device is responsible for demonstrating that the device is safe and effective in the new intended use. "If, for example, a packer, distributor, or seller [or software developer] intends an article [in this case, the fitness tracker] for different uses than those intended by the person [that manufactured the fitness tracker], such packer, distributor, or seller [or software developer] is required to supply adequate labeling in accordance with the new intended uses."[53] To supply adequate labeling, it would be necessary to prove to the FDA that the fitness tracker is safe and effective in the new intended use — in other words, to seek a clearance or premarket approval for that use. Note that the research app developer, rather than the mobile health company that makes the fitness tracker, is the party on the hook to prove that the fitness tracker is safe and effective, when used together with the new software, to diagnose and predict asthma attacks and strokes. To the extent this has not yet been proved, the suggested new use is experimental and potentially might be subject to the FDA's research regulations, as discussed further below.

The Journal of Law, Medicine & Ethics, 48 S1 (2020): 74-81. © 2020 The Author(s)

https://doi.org/10.1177/1073110520917031 Published online by Cambridge University Press

The second characterization is that the research software platform is SaMD, offered as a separate accessory to people's fitness trackers. A device accessory is potentially subject to regulation as a device in its own right. The definition of medical devices that the FDA can regulate includes "any component, part, or accessory, which is ... intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease, in man or other animals... ."[54] If the research app developer *intends* for its software to be used to diagnose or predict asthma attacks and strokes, then the research software is a medical device that the FDA can regulate. Once again, if the research software has not yet been shown safe and effective for that use, then it is an experimental device, and the FDA potentially can regulate human-subject research that uses the software.

How can the research app developer avoid these outcomes? The FDA's research regulations are described in a companion article in this same issue,[55] and readers are referred there for background. The key points here are that much depends on the app developer's intent and on the risks posed by the citizen-science study. Does the software developer intend to submit data from the citizen-science study to the FDA to support clearance or premarket approval of the software for future use as a diagnostic or predictive product? If so, compliance with the FDA's research regulations is required.

Even if the answer to that first question is "no," does the software developer intend for the research software to be used "in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease,"[56] or does the developer instead merely intend to use the software to conduct basic scientific "investigations to expand medical knowledge or conduct medical research"?[57] The FDA's investigational device exemption (IDE) regulations[58] generally do not apply to basic scientific research that uses an experimental device, unless the research incorporates a device study — that is, a study that aims to prove the experimental device is safe and effective.[59] Finally, does the research that uses the fitness tracker together with the new software pose significant risk to the research participants? If so, the FDA can nevertheless require an IDE.

How the FDA answers these questions could depend on whether research participants will have access to individualized data and results generated by the research software platform. Sharing individual research findings — such as a finding that a participant's heart rate data, as analyzed by the research software, seem to indicate an elevated risk of a stroke — might cause the FDA to infer that the software developer *does* intend diagnostic uses of the research software. Moreover, sharing such information with participants might place them at significant risk if the inferences drawn by the research software turn out to be wrong.

Individual data access policies are one of many factors the FDA can consider when determining whether research requires an IDE. This reasoning was apparent in two draft guidances on laboratory-developed tests that the FDA published in 2014[60] but later abandoned.[61] One of the draft guidances indicated that research laboratories would need an IDE if research participants would have access to experimental test results that had not been confirmed by a medically accepted diagnostic product or procedure.[62] It did not seem coincidental that the FDA published this draft

The fact that HIPAA's regulations are mandatory for HIPAA-covered researchers may have helped persuade the agency not to read too much intent into the fact that a laboratory honors individuals' access rights. In the non-HIPAA-covered space of mobile health research and research software developers, however, the FDA might view things differently. Creating a HIPAA-equivalent access right for participants in citizen-science projects would, in all likelihood, be done through policies reflected in software developers' end-user agreements and terms of service. When no state or federal law makes individual access rights mandatory, the FDA might be more inclined to view a software developer's decision to grant such rights as evidence that the developer intends diagnostic use of information from research.

The Journal of Law, Medicine & Ethics, 48 S1 (2020): 74-81. © 2020 The Author(s)
https://doi.org/10.1177/1073110520917031 Published online by Cambridge University Press

guidance three days before the compliance date of a HIPAA rule change that greatly expanded HIPAA's access right to data held at HIPAA-covered laboratories.[63] The timing suggests that the FDA viewed expanded HIPAA access as posing risks to research participants, or else regarded individual access as a factor suggesting intent for diagnostic use of research data. The fact that the FDA eventually withdrew this draft guidance is a hopeful sign that the agency realizes that providing HIPAA access does not imply any particular intent on the part of a HIPAA-covered laboratory, other than an intent to comply with a mandatory federal privacy law.

The fact that HIPAA's regulations are mandatory for HIPAA-covered researchers may have helped persuade the agency not to read too much intent into the fact that a laboratory honors individuals' access rights. In the non-HIPAA-covered space of mobile health research and research software developers, however, the FDA might view things differently. Creating a HIPAA-equivalent access right for participants in citizen-science projects would, in all likelihood, be done through policies reflected in software developers' end-user agreements and terms of service. When no state or federal law makes individual access rights mandatory, the FDA might be more inclined to view a software developer's decision to grant such rights as evidence that the developer intends diagnostic use of information from research. There is considerable evidence that people's willingness to enroll in a research project depends on whether they will find out information about themselves.[64] One survey found that "[t]he most influential factor affecting the respondent's willingness to participate in the study seemed to be the offer of individualized results."[65] Developers of research apps presumably are aware of these facts. Their voluntary choice to adopt policies allowing individual access to research data could be seen as a way of marketing their software to users who, according to the evidence just cited, have every intent to make diagnostic use of the data they receive.

The FDA's intended use regulation provides that "if a manufacturer knows, or has knowledge of facts that would give him notice that a device introduced into interstate commerce by him is to be used for conditions, purposes, or uses other than the ones for which he offers it, he is required to provide adequate labeling for such a device which accords with such other uses to which the article is to be put."[66] Even if a software developer *intends* for its software to be used only for basic scientific research, the fact that the developer is voluntarily granting individual access rights (when law does not require it to do so), together with the fact that participants plan to use their data for self-diagnosis,[67] might lead the FDA to infer that the software developer intends the diagnostic use. If that happens, the research app becomes SaMD that the FDA can regulate, including by requiring an IDE for the research if the FDA deems it to pose significant risk to the participants.

A typical application to the FDA for an IDE or IND (investigational new drug exemption) is thousands of pages long and requires many months and sometimes years to prepare.[68] Imposing IDE requirements on the software platforms used in citizen-science projects thus could have a profoundly chilling effect on citizen science activity. Efforts to create HIPAA-equivalent individual access rights for persons participating in citizen science projects have a potential to create costly and burdensome FDA compliance obligations for research app developers. Despite the importance of individual access rights as a crucial privacy protection, the potential FDA compliance impacts of providing such rights in non-HIPAA-covered mobile health research may hinder attainment of privacy parity.

Conclusion

It is distasteful to consider that some research contexts warrant different, lesser ethical and privacy protections than others. The United States has long tolerated a striking lack of parity between research that is or is not regulated by the Common Rule and between data environments that are or are not HIPAA-covered. As citizen science emerges as an important new mode of research activity, it seems timely to take steps to avoid having it become yet another sore spot of ethical and privacy disparities. Yet parity presents implementation challenges that are real and highly context-specific. This article has explored one aspect of the problem.

If HIPAA-equivalent individual access rights cannot be achieved in citizen science projects, privacy rights will remain inherently incomplete unless alternative solutions can be crafted. This challenge invites a deeper reconsideration of the ethical and privacy principles that should govern in this context. There are alternatives to placing citizen science under the same ethical and privacy norms that guided traditional research in the 20th century. Not all of these alternatives represent unpalatable moral compromises or ethical derogations.

For example, HIPAA's individual access right was originally conceived as a *quid pro quo* for other provisions of HIPAA, such as its waiver provision,[69] that facilitate unconsented third-party access to people's data.[70] The thought was that if third parties have access to your personal information, then you need access, too, so that you can understand the privacy risks to which you are exposed as a result of the wide-

The Journal of Law, Medicine & Ethics, 48 S1 (2020): 74-81. © 2020 The Author(s)
https://doi.org/10.1177/1073110520917031 Published online by Cambridge University Press

spread, uncontrolled dissemination of your data that HIPAA allows.[71] If providing HIPAA-equivalent individual access rights proves infeasible in citizen science projects, an alternative (and very simple) way to protect participants' privacy interests would be to provide strong commitments not to share their data without their express authorization. Such a solution might actually be superior to HIPAA's protections, which are not without their flaws.

A second alternative to consider is the reduced-privacy research model that Bobe et al. recently described.[72] This model proposes that some types of research should "selectively recruit individuals with fewer significant interests in personal privacy."[73] The idea sounds dreadful at first, until they explain that Harvard's Personal Genome Project (PGP) and its affiliated international sites exemplify this model, recruiting participants who are willing to embrace broad sharing of their genomic data for research. Not all people value privacy as much as Institutional Review Boards and privacy advocates assume people do. People drawn to citizen science might, if surveyed, turn out to be a bunch of privacy risk-seekers, in which case replicating HIPAA's privacy protections might not be something they even desire. Policymakers should ask them what they want, before presuming to tell them what is good for them. These are merely two examples, offered as an invitation to a wider dialogue about whether traditional and citizen science really can — or really should — follow the same ethical and privacy principles.

Acknowledgments

Preparation of this article was funded in part by National Human Genome Research Institute (NHGRI) and National Cancer Institute (NCI) grant #R01CA207538 (Rothstein, Wilbanks, PIs) on "Addressing Ethical, Legal, and Social Issues (ELSI) in Unregulated Health Research Using Mobile Devices" and by NHGRI and NCI grant #1R01HG008605 (Wolf, Clayton, Lawrenz, PIs), on "LawSeq: Building a Sound Legal Foundation for Translating Genomics into Clinical Application." The views expressed in this article are those of the author and not necessarily those of the funders.

Note

The author has no conflicts of interest to disclose.

References

1. M.A. Rothstein et al., "Citizen Science on Your Smartphone: An ELSI Research Agenda," *Journal of Law, Medicine & Ethics* 43, no. 4 (2015): 897-903, at 901.
2. B. Patrick-Lake and J.C. Goldsack, "Mind the Gap: The Ethics Void Created by the Rise of Citizen Science in Health and Biomedical Research," *American Journal of Bioethics* 19, no. 8 (2017): 1-2.
3. 45 C.F.R. pt. 46, subpt. A.
4. 21 C.F.R. pts. 50, 54, 56, 809, 812.
5. Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 18, 26, 29, and 42 U.S.C. (2012)).
6. 45 C.F.R. pts. 160, 164 (2018).
7. B.J. Evans and S.M. Wolf, "A Faustian Bargain that Undermines Research Participants' Privacy Rights and Return of Results," *Florida Law Review* 71, no. 5 (2019): 1281-1345, at 1296–1307.
8. S.M. Wolf, "Return of Results in Participant-Driven Research: Learning from Transformative Research Methods," *Journal of Law, Medicine & Ethics* 48, no. 1, Supp. (2020): 159-166.
9. Pub. L. No. 90-321, 84 Stat. 1128 (codified as amended at 15 U.S.C. § 1681 (2012)) (authorizing collection and storage of individuals' financial and credit data without their consent but granting individuals a right of access to their data).
10. Pub. L. No. 93–579, 88 Stat. 1896 (codified as amended at 5 U.S.C. §§ 552(a), (d) (2012)) (providing an individual right of access to data held in governmental databases).
11. 45 C.F.R. § 164.524 (2018).
12. B.J. Evans, "The Genetic Information Nondiscrimination Act at Age 10: GINA's Controversial Assertion that Data Transparency Protects Privacy and Civil Rights," *William & Mary Law Review* 60, no. 6 (2019): 2017-2109, at 2055-2066 (reviewing the stated legislative and regulatory purposes).
13. *Id.*, at 2059.
14. U.S. Dep't of Health & Human Servs., *Confidentiality of Individually Identifiable Health Information: Recommendations of the Secretary of Health and Human Services, Pursuant to Section 264 of the Health Insurance Portability and Accountability Act of 1996* (September 11, 1997), *available at* <https://aspe.hhs.gov/report/confidentiality-individually-identifiable-health-information> [https://perma.cc/2V9X-XFAV] (last visited January 22, 2020).
15. Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data and Repealing Directive 95/46/EC, art. 15, 2016 O.J. (L 119): 1, 43.
16. *See, e.g.*, California Consumer Privacy Act, 2018 Cal. Legis. Serv. 3 (West) ("[I]t is the intent of the Legislature to further Californians' right to privacy by giving consumers an effective way to control their personal information, by ensuring the following rights[, including] … [t]he right of Californians to access their personal information."); *id.*, at 3–4 (amending Part 4 of Division 3 of the Civil Code to add § 1798.100(d), which provides individuals with a right of access to their data).
17. M.A. Rothstein et al., "Unregulated Health Research Using Mobile Devices: Ethical Considerations and Policy Recommendations," *Journal of Law, Medicine & Ethics* 48, no. 1, Suppl. (2020): 196-226.
18. 45 C.F.R. § 164.524(a).
19. 45 C.F.R. § 164.501 ("*Designated record set* means: (1) A group of records maintained by or for a covered entity that is: (i) The medical records and billing records about individuals maintained by or for a covered health care provider; (ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) Used, in whole or in part, by or for the covered entity to make decisions about individuals."); *see also id.* § 160.103 (treating genetic information as health information for purposes of the Privacy Rule); *id.* § 164.501 ("[T]he term record means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.").
20. *Id.* § 164.501.
21. B.J. Evans et al., "Regulatory Changes Raise Troubling Questions for Genomic Testing," *Genetics in Medicine* 16, no. 11 (2014): 799-803, at 800.
22. U.S. Dep't of Health & Human Servs., Individuals' Right under HIPAA to Access their Health Information 45 CFR § 164.524 (February 25, 2016), *available at* <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html> [https://perma.cc/9S7L-3QEP] (last visited January 22, 2020).
23. *Id.*
24. *Id.*

The Journal of Law, Medicine & Ethics, 48 S1 (2020): 74-81. © 2020 The Author(s)

https://doi.org/10.1177/1073110520917031 Published online by Cambridge University Press

25. 45 C.F.R. § 164.524(a)(2), (3) (listing unreviewable and reviewable grounds for denial of access).
26. *See id.* § 164.524(a)(2)(iii).
27. *Id.*
28. *Id.*
29. A. Wiggins and J. Wilbanks, "The Rise of Citizen Science in Health and Biomedical Research," *American Journal of Bioethics* 19, no. 8 (2019): 3-14.
30. J. Bobe, M.N. Meyer, and G. Church, "Privacy and Agency Are Critical to a Flourishing Biomedical Research Enterprise: Misconceptions about the Role of CLIA," *Florida Law Review Forum* (2019), *available at* <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3499923> (last visited January 22, 2020).
31. S.R. Arnstein, "A Ladder of Citizen Participation," *Journal of the American Planning Association* 35, no. 4 (1969): 216-224.
32. Elisa A. Hurley, "Why We Need to Keep the Term "Research Subject' in Our Research Ethics Vocabulary," *Ampersand* blog (February 22, 2019), *available at* <https://blog.primr.org/research-subject-vs-research-participant> (last visited January 22, 2020).
33. Bobe et al., *supra* note 30, at 9.
34. Rothstein et al., *supra* note 17.
35. S.R. Peppet, "Regulating the Internet of Things: First Steps toward Managing Discrimination, Privacy, Security, and Consent," *Texas Law Review* 93, no. 1 (2014): 85-179, at 145.
36. M.A. Hall, "Property, Privacy, and the Pursuit of Interconnected Electronic Medical Records," *Iowa Law Review* 95 (2010): 631-663, at 646.
37. M.A. Rodwin, "Patient Data: Property, Privacy & the Public Interest," *American Journal of Law & Medicine* 36 (2010): 586-618, at 588.
38. Peppet, *supra* note 35, at 93.
39. *Id.*
40. Peppet, *supra* note 35, at 145.
41. *Id.*, at 129, 143.
42. *Id.*, at 143-44.
43. *Id.*, at 129.
44. *Id.*, at 161-162; D. Barua et al., "Viewing and Controlling Personal Sensor Data: What Do Users Want?" in *Persuasive 2013: Proceedings of the 8th International Conference on Persuasive Technology* (Shlomo Berkovsky and Jill Freyne eds., 2013): at 15-26.
45. *Id.*, at 144.
46. Health Data Exploration Project, *Personal Health Data for the Public Good: New Opportunities to Enrich Understanding of Individual and Population Health* (2014), *available at* <http://hdexplore.calit2.net/wp-content/uploads/2015/08/hdx_final_report_small.pdf> (last visited January 22, 2020).
47. Food and Drug Administration, *Device Software Functions Including Mobile Medical Applications* (September 26, 2019), *available at* <https://www.fda.gov/medical-devices/digital-health/mobile-medical-applications> (last visited January 22, 2020).
48. Pub. L. 114-255 (2016).
49. 21 U.S.C. § 360j(o)(1)(B).
50. Food and Drug Administration, *General Wellness: Policy for Low Risk Devices: Guidance for Industry and Food and Drug Administration Staff* (September 27, 2019), *available at* <https://www.fda.gov/regulatory-information/search-fda-guidance-documents/general-wellness-policy-low-risk-devices> (last visited January 22, 2020).
51. International Medical Regulators Device Forum, IMDRF SaMD Working Group, *Software as a Medical Device (SaMD): Key Definitions* (December 9, 2013), *available at* <http://www.imdrf.org/docs/imdrf/final/technical/imdrf-tech-131209-samd-key-definitions-140901.pdf> (last visited January 22, 2020).
52. Food and Drug Administration, Software as a Medical Device (SAMD): Clinical Evaluation," December 8, 2017, at 11, *available at* <https://www.fda.gov/media/100714/download> (last visited January 22, 2020).
53. 21 C.F.R. § 801.4.
54. 21 U.S.C. § 321(h).
55. Rothstein et al., *supra* note 17.
56. 21 U.S.C. § 321(h).
57. Medical Devices; Procedures for Investigational Device Exemptions, 45 *Fed. Reg.* at 3735. *See also* Rothstein et al, *supra* note 17.
58. 21 C.F.R. pt. 812.
59. *See* Rothstein et al., *supra* note 17.
60. Food and Drug Administration, Framework for Regulatory Oversight of Laboratory Developed Tests; Draft Guidance for Industry, Food and Drug Administration Staff, and Clinical Laboratories; Availability, 79 *Fed. Reg.* 59,776 (October 3, 2014); Food and Drug Administration, Notification and Medical Device Reporting for Laboratory Developed Tests; Draft Guidance for Industry, Food and Drug Administration Staff, and Clinical Laboratories; Availability, 79 *Fed. Reg.* 59,779 (October 3, 2014).
61. *See* Food and Drug Administration, Discussion Paper on Laboratory Developed Tests (LDTs) (2017), *available at* <https://www.fda.gov/downloads/medicaldevices/ productsandmedicalprocedures/invitrodiagnostics/laboratorydevelopedtests/ucm536965.pdf> [https://perma.cc/HN5A-W4G9] (last visited December 16, 2019) (noting that FDA announced it would not be issuing final guidance on laboratory developed tests to allow further discussion).
62. Food and Drug Administration, Framework for Regulatory Oversight of Laboratory Developed Tests: Draft Guidance 36-37 (2014), *available at* <https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ ucm416685.pdf> [https://perma.cc/B28U-TNCJ] (last visited December 16, 2019).
63. CLIA Program and HIPAA Privacy Rule; Patients' Access to Test Reports; Final Rule, 79 *Fed. Reg.* 7290, 7293 (February 6, 2014) (codified at 42 C.F.R. pt. 493 and 45 C.F.R. pt. 164).
64. L.S. Parker, "Returning Individual Research Results: What Role Should People's Preferences Play?" *Minnesota Journal of Law, Science and Technology* 13, no. 2 (2012): 449-484, at 456, 471-72; S.F. Terry, "The Tension between Policy and Practice in Returning Research Results and Incidental Findings in Genomic Biobank Research," *Minnesota Journal of Law, Science and Technology* 13, no. 2 (2012): 691-736, at 708- 709.
65. Parker, *supra* note 64, at 472.
66. 21 C.F.R. §801.4.
67. Parker, *supra* note 64; Terry, *supra* note 64.
68. Institute of Medicine, The Future of Drug Safety: Promoting and Protecting the Health of the Public (2007): at 33, *available at* <https://www.nap.edu/catalog/11750/the-future-of-drug-safety-promoting-and-protecting-the-health> (last visited January 22, 2020) (reporting that the average new commercial IND submission to the FDA is 14,000 pages long).
69. 45 C.F.R. § 164.512(i).
70. Evans, *supra* note 12, at 2094-97 (tracing the historical development of HIPAA's access right and citing the sources that enunciated its rationale).
71. *Id.* (citing analysis of this issue in two reports commissioned by Congress).
72. Bobe et al., *supra* note 30, at 6-8.
73. *Id.*, at 6.

The Journal of Law, Medicine & Ethics, 48 S1 (2020): 74-81. © 2020 The Author(s)

https://doi.org/10.1177/1073110520917031 Published online by Cambridge University Press