Who Are the People in Your Neighborhood? Personas Populating Unregulated mHealth Research

Megan Doerr and Christi Guerrini

I. Introduction

Ethical and policy questions are increasingly being raised about the large and growing universe of people conducting unregulated mHealth research. These questions relate to, among other things, safety, informed consent, privacy, ownership, and liability.[1] Although they are often discussed generally, each issue is more or less salient, and mechanisms for addressing them are more or less appropriate, depending on who exactly is conducting mHealth research and for what purposes. For example, safety is usually not a concern for researchers studying genetic data shared by others, but it is a major issue for those who modify medical devices that respond to personal health data, and different policies may be needed to address this concern depending on whether the end users are the hackers, their children, or third parties unknown to them.

Our goal in this article is to assist in evaluating the concerns that are being raised about unregulated mHealth research and potential policy solutions by giving shape to the emerging panoply of actors in this space. We do so through presentation of a set of personas, which are often used in user experience design (UX) to document a set of archetypical users whose goals and characteristics are representative of a larger group of users.[2] These personas derive from our professional observations of and activities in the emerging mHealth space. Some personas are manifest and can be described by reference to individuals or entities we perceive as exemplars. Others are conspicuous in different domains of unregulated research but could soon become active in mHealth research.

Each persona describes a distinct category of researchers in terms of their fundamental motivations, goals, and behaviors and also includes an overview of salient concerns associated with their activities. These descriptions are useful for evaluating existing and proposed policies applicable to mHealth from the perspective of each persona to understand how the policies will aid or frustrate various stakeholders. At the same time, these descriptions reveal ethical themes that are prevalent throughout the unregulated mHealth research ecosystem and might be used to help policy makers prioritize their attention to this space.

II. Definitions

Before detailing personas for the mHealth space, let us define more precisely who qualifies as an unregulated mHealth researcher subject to categorization. By *unregulated*, we mean that the activities of these individuals are not governed by traditional federal protections of human research subjects that apply to U.S. federally funded or supported research ("Common Rule")[3] or research regulated by the U.S. Food and Drug Administration (FDA).[4] Those protections require that an Institutional Review Board (IRB) evaluate the research plan to ensure that the anticipated risks to participants are minimized and reasonable in relation to the anticipated benefits and that their informed consent to participate is obtained. We appreciate, however, that some research activities might still be subject to other federal regulations, such as the Federal Trade Commission Act (FTCA),[5] the security and

Megan Doerr, M.S., L.G.C., *is Principal Scientist, Governance, at Sage Bionetworks. Her work focuses on app-based research, including the ELSI issues of informed consent, research participation, and data sharing for secondary use.* **Christi Guerrini, J.D., M.P.H.,** *is an Assistant Professor at the Center for Medical Ethics and Health Policy at Baylor College of Medicine. She has a K01 award from the National Human Genome Research Institute to study ownership interests in citizen science.*

The Journal of Law, Medicine & Ethics, 48 S1 (2020): 37-48. © 2020 The Author(s)
DOI: 10.1177/1073110520917028

privacy provisions of the Health Insurance Portability and Accountability Act (HIPAA)[6] and the Health InformationTechnology for Economic and Clinical Health Act (HITECH Act),[7] or the medical device provisions of the Federal Food, Drug, and Cosmetic Act (FDCA).[8] As we define it, unregulated research might also be subject to state laws and regulations directed to, among other things, the propertization of genetic data[9] or the practice of medicine.[10]

The activities of these individuals are connected in some way to *mHealth*, which is defined as the use of a mobile device to collect and analyze health or wellness data.[11] That device might travel with, on, or through the person being studied, or it might interact with devices that are with, on, or in the person being studied (e.g., a Bluetooth beacon interacting with a mobile device to give the location of a research participant). Data are collected actively through activities, passively via sensors, or in a hybrid fashion through a variety of activities and sensors.[12] Data are then maintained at the individual level or aggregated with data collected from other sources.

scientific investigation or policy, without regard to the individual's motivation for engagement. Thus, as described in more detail below, self-discoverers and grinders[14] are, ostensibly, investigating or experimenting on their own selves, but may be doing so at least in part to inspire others to conduct similar research on themselves or to stir more traditional researchers to take action. According to our definition, all of these individuals —and others — qualify as researchers and therefore description by persona.

Finally, we note that this article's broad understanding of researcher is consistent with the ethos of citizen science, which uses an inclusive rather than reductive lens for defining relevant communities. Although the definition of citizen science is contested and evolving,[15] it is typically described as an approach to scientific inquiry in which members of the public participate in ways other than, or in addition to, allowing personal data or biospecimens to be collected from them for analysis by others.[16] Public participation can take many forms and includes generating hypotheses, collecting or analyzing data, or disseminating results.[17]

Each persona describes a distinct category of researchers in terms of their fundamental motivations, goals, and behaviors and also includes an overview of salient concerns associated with their activities. These descriptions are useful for evaluating existing and proposed policies applicable to mHealth from the perspective of each persona to understand how the policies will aid or frustrate various stakeholders. At the same time, these descriptions reveal ethical themes that are prevalent throughout the unregulated mHealth research ecosystem and might be used to help policy makers prioritize their attention to this space.

The individuals whom we describe as *researchers* comprise a far larger population than is traditionally encompassed by this term. Specifically, researchers are often described as those attempting to create "generalizable knowledge," a definition derived from the very regulation that defines research.[13] One problem with this narrow understanding is that it excludes a plethora of people with interests in or interactions with research and whose activities may be germane to policy makers or regulators. For example, the traditional definition of researcher excludes those who inform or influence research, in either the immediate term or over time, by, for example, funding, instigating, or disrupting studies. To capture these and other relevant efforts, we therefore define researcher broadly as any individual who conducts, facilitates, or changes

Given that some mHealth research is conducted by citizen scientists,[18] it is appropriate that the description of individuals who participate in this space also is broad and inclusive.

III. Personas

In user design, personas are typically drawn from themes or trends seen in user interview data and harmonized with the business needs of the sponsoring organization or developers. For the purposes of developing personas of unregulated mHealth researchers, we derived themes and trends from our ongoing study of mHealth platforms and users, participation in relevant working groups, direct observation at conferences and meetings (e.g., DEF CON, Biohack the Planet), and review of both popular and scientific lit-

The Journal of Law, Medicine & Ethics, 48 S1 (2020): 37-48. © 2020 The Author(s)

erature. Analogous to UX design, through iterative discussion, we developed these personas with an eye to the public welfare priorities of policy makers considering this space.

The resulting ten personas of unregulated mHealth researchers are presented generally along a spectrum that describes, on one end, empowerment or philanthropic objectives, and on the other end, financial or misanthropic objectives. When possible, we give examples of each persona. However, it is important to note that the descriptions and classifications of the individuals and entities that we selected as examples are our own; their perspectives on their activities could be different.

1. The Empowered Patient Persona

The **empowered patient** is a person living with a condition or disease who uses mHealth tools or devices to inform their choices about their care or enable self-directed management of their condition. The empowered patient may hack existing medical devices, develop novel devices, use existing devices for novel applications, or collect data from mHealth devices to design or execute self-interventions. These behaviors may arise due to frustration related to the patient's options for care for their disease or condition or the perceived or real lack of attention by the medical or research enterprise to the symptoms or issues of greatest importance to them. Their frustration may be related to the perceived or real lack of attention by the medical or research enterprise to the symptom of greatest importance to them. They may be discouraged by the seemingly "glacial pace" of medical research, or the rate of translation of research findings to clinical care.[19] The empowered patient may attempt to circumvent regulations or closed systems that thwart access to their own data or information about treatment or options.

Dana Lewis[20] is an example of the empowered patient persona. Ms. Lewis, who is living with Type 1 diabetes, became frustrated with the crude systems available to her to monitor and control her blood sugar levels. Through self-taught, unregulated mHealth hacking, Ms. Lewis developed a reciprocal communication loop, enhanced with predictive algorithms, between her glucose monitor and insulin pump, creating a system that functions as an artificial pancreas.

Though the empowered patient attempts to better their own care, they might not understand the risks of activities that they undertake or they might be (too) willing to accept unreasonable risks. The empowered patient might overestimate their skills or knowledge.

It is important to note that the empowered patient may, intentionally or unintentionally, create a network effect with other empowered patients. It is difficult to estimate the prevalence of this evolution given that those who create such networks may naturally become more widely known. Though Ms. Lewis undertook unregulated mHealth research with herself as both researcher and participant, her work has grown into OpenAPS,[21] a network of people living with Type 1 diabetes implementing the same (or similar) artificial pancreas hack, among other activities. Additional considerations for policy makers may arise as empowered patients share their unregulated mHealth research activities with others.

2. The Concerned Caregiver Persona

Concerned caregivers engage directly in unregulated mHealth research or seek to influence the research ecosystem to benefit the care of a loved one, such as a child, parent, or spouse. Like empowered patients, concerned caregivers may be frustrated by the perceived pace of innovation or discovery for their loved one's condition.[22] They may develop novel mHealth devices, use existing devices for novel application, or collect data from devices to design or execute interventions for their loved one. Through their actions, caregivers might experience feelings of agency or empowerment[23] that mitigate the myriad negative emotions frequently associated with having a loved one with or at risk of a health condition.

Two examples of concerned caregivers are John Costik and Dan Webster. Mr. Costik[24] developed a system to remotely monitor his diabetic son's continuous glucose monitor, streaming low blood sugar alerts in real time through the cloud first to Mr. Costik's phone and eventually to his smartwatch. Dr. Webster,[25] out of frustration from the absence of a systematic way to track the changes in his wife's moles and her associated risk for melanoma, developed the ResarchKit[26] app MoleMapper.[27] Using the app, the couple were able to map and document her moles over time, providing supplemental data for regular dermatologist visits. In both cases, the development and use of an mHealth tool allowed the concerned caregiver more frequent, even continuous, monitoring of the loved one's condition, facilitating potentially more effective and empowered caregiving.

The concerned caregiver arrives in the unregulated mHealth space altruistically. While they would never knowingly put a loved one in harm's way, the relational dynamics between the caregiver and loved one may raise concerns about voluntariness and consent. This dynamic may be particularly fraught between a parent (or primary caregiver) and child (or other vulnerable class of participant), already a difficult relationship to govern in the regulated research context. The con-

The Journal of Law, Medicine & Ethics, 48 S1 (2020): 37-48. © 2020 The Author(s)

cerned caregiver may overestimate their knowledge as a researcher or be so excited by the promise of self-initiated solutions that they may not see clearly the risks involved, or may be too willing to accept such risks on behalf of another.

Finally, as with empowered patients, concerned caregivers' actions may lead to community activism, either by nucleating a community of fellow caregivers/empowered patients or through the open sharing of a caregiver-developed tool, approach, or knowhow for broader use. As with empowered patients, it is difficult to estimate the prevalence of this evolution given that those caregivers who do make this leap may naturally become more widely known. In our two examples, Mr. Costik founded the "CGM in the Cloud" Facebook group, and Dr. Webster publicly released the MoleMapper through the iOS app store. Again, additional considerations for policy makers may arise as concerned caregivers share their unregulated mHealth research activities with others.

3. The Empowered Community Persona

Empowered communities may be a direct outgrowth of the empowered patient or concerned caregiver personas or may congregate around an ideal and then discover unregulated mHealth research as a tool. In the first case, individuals with a condition and/or their caregivers band together to use mHealth tools to drive research or influence the research or clinical care ecosystem. In the latter, a community ideal, such as democratization of science, opens the door to mHealth experimentation. A key impetus for empowered community development is power in numbers: converging with others around a condition or ideal to amplify the community's impact on research or the clinical care ecosystem through financial or political influence.

Empowered communities that have grown from empowered patients and concerned caregivers include the already mentioned mentioned APS,[28] CGM in the Cloud,[29] and MoleMapper app[30] examples, as well as groups like Crohnology,[31] an online, patient-powered research network founded by Sean Ahrens, a man living with Crohn's disease. Crohnology is a platform for community sharing of observations and interventions for Crohn's disease symptom mitigation and control. Further, although not yet manifest in the mHealth space, we anticipate concerned caregiver-initiated crowdfunding mHealth efforts like those seen in rare disease communities to accelerate gene therapies.[32]

An example of a community ideal-nucleated empowered community is BioCurious,[33] a non-profit hacker/makerspace in Silicon Valley. BioCurious was founded on the belief that biology should be accessible, affordable, and open to everyone. As a community-run lab, it serves as a physical meeting space for biohackers, citizen scientists, and others who want to experiment. Unregulated mHealth tools and approaches are rapidly becoming integrated within its varied project portfolio.

When assessing the policy concerns surrounding empowered communities, we must think about the group as the unit for analysis. Groupthink and peer pressure may play outsized rolls in even the most empowered community. Further, the volume of data collected by such groups may (inadvertently) legitimize insights derived from faulty measurements.

4. The Self-Discoverer Persona

Whereas empowered patients and concerned caregivers use mHealth to treat or manage specific health conditions, **self-discoverers** use mHealth to better understand and improve their health. The ultimate aim of self-discoverers is to obtain insights that might help them avoid disease or improve their general state of wellness. So defined, self-discoverers include individuals who upload their raw genetic data to third-party genetic interpretation services, including mHealth tools, to learn about their genetic disease predispositions or to purchase diet or fitness plans or nutritional supplements customized to their DNA.[34] In some cases, the individual's primary objective in sharing their raw genetic data with such services is to understand their ancestral origins or identify genetic relatives.[35] When those services also provide health and wellness information, the participants become self-discoverers, even if unintentionally. On the other end of the spectrum are self-discoverers who intensively record their fitness, sleep, nutritional, or physiological data using mobile devices for the specific purpose of obtaining personal health or wellness insights. As an example of this kind of self-discoverer, members of the Quantified Self (QS) community recently organized to conduct high-frequency self-testing of their blood lipid levels using portable analyzers.[36]

In many cases, self-discoverers do not themselves conduct research with the personal data that they collect. However, just as Narcissus, who could not pull himself away from his own reflection, might have prompted others to investigate what he was doing, self-discoverers also can attract scientific attention. For example, openSNP maintains a public database of users' genetic data and research interest in those data continues to grow.[37] Further, some users of third-party genetic interpretation services share the results with their clinicians, which has prompted research into, among other things, the validity of the results.[38] Finally, self-discoverers are participating in studies of

The Journal of Law, Medicine & Ethics, 48 S1 (2020): 37-48. © 2020 The Author(s)

their efforts. For example, some participants in the QS blood-testing project elected to participate in a study of the feasibility and utility of systematic ethical reflection as a mechanism for providing ethical oversight of self-monitoring activities.[39]

For self-discoverers, relevant ethical and policy concerns include the accuracy of the health and wellness data that are the bases of their activities. If the data are inaccurate, self-discoverers might be prompted to act in ways that are costly and potentially harmful. Even if the information is accurate, it might be presented in a way that is confusing or misleading, causing users (and their clinicians) to misunderstand them.[40] Finally, such services might not sufficiently safeguard against the unauthorized disclosure of users' information to others or their downstream uses of that information to discriminate or embarrass.[41] One downstream use that recently has become the subject of vigorous debate is searching of public genetic databases by law enforcement to generate investigative leads in criminal cases.[42]

5. The Grinder Persona

Also called bodyhackers, body modifiers, and do-it-yourself (DIY) cyborgs, **grinders** are individuals who implant devices, including mHealth devices and devices that transmit information to mHealth devices, into their bodies.[43] Whereas self-discoverers aim to understand their bodily functions, grinders seek to enhance or otherwise change those functions, sometimes in pursuit of transhumanist objectives to unite man with machine.[44] Grinders who qualify as unregulated mHealth researchers include Tim Cannon, co-founder of Grindhouse Wetware, who implanted his open source biotechnology company's Circadia device into his skin to transmit biometric data to his mobile phone,[45] and Anastasia Synn, a self-described "cyborg magician" who implanted a temperature chip in her arm.[46]

Although grinders do not conduct traditional scientific studies, their activities are in the realm of research given that they are testing the body's response to the implantation or are coated with materials that have not been established as safe and effective for body implantation.[47] Further, grinders' activities take place alongside, and so undoubtedly influence, the regulated research and development of medical devices that are intended for body implantation. Kevin Warwick, for example, is a biomedical researcher with academic appointments who famously implanted a device in the nerves of his arm that he used to control a robot hand via the internet using his thoughts.[48] The same device has since been used by scientists to restore movement in paralyzed persons.[49]

In the absence of customary peer, institutional, and regulatory oversight, professional scientists' mHealth research may not be scrutinized for scientific or ethical validity. Without the mandated support of ethics and regulatory professionals, the professional scientist persona may not recognize (or accept) the full extent of the ethical responsibilities they have for their research. Many have pointed to Facebook's "emotional contagion" study as an example of professional scientists abdicating ethical responsibility for their work while operating in an unregulated mHealth context. Further, the misconduct of research by professional scientists has the potential to sow distrust in the scientific enterprise and/or the legitimacy of rigorously conducted research.

Because many devices implanted by grinders are not intended for human implantation and implants are not always performed or subsequently monitored by medical professionals, grinders' activities raise serious safety concerns. Indeed, in 2017, an Australian woman died from septicemia following the implantation of a plastic snowflake under the skin of her right hand, which became infected.[50] The man who implanted the snowflake was not a healthcare professional and has been charged with manslaughter in her death.[51] Although the case did not involve an mHealth device, it highlights liability issues for those who perform any kind of body modification and also potential gaps in oversight where local medical, piercing, and tattoo licensure laws do not cover body modification procedures. At the same time, government interference with grinders' activities raise important questions about what are appropriate limits to bodily autonomy.

The Journal of Law, Medicine & Ethics, 48 S1 (2020): 37-48. © 2020 The Author(s)

6. The Data Sharer Persona

Individuals who use mHealth for personal health or self-exploration purposes often collect data about themselves as a result of these activities that are potentially valuable to others. When they transfer those data from or with the help of mobile devices, they become **data sharers**. Some sharing is intended solely to support scientific discovery that might help others and is made without any expectation of or even desire for personal gain. For example, more than 80% of customers of 23andMe, a direct-to-consumer genetic testing firm, provide permission for the firm to use their genetic data in research studies that the firm conducts or supports.[52] Customers might also download their raw genetic data onto their mobile phones and then contribute those data — along with fitness tracking and social media data — to other research initiatives, such as those hosted on Open Humans.[53]

While altruism is a common reason for sharing, some data sharers are motivated by financial gain. Recently, businesses have emerged to help individuals monetize their health information — in some cases using mHealth devices. For example, the CoverUS app has plans to broker the sale of users' health data to interested buyers in exchange for cash rewards.[54] Similarly, Hu-manity.co has developed a mobile app through which users will soon be able to sell their medical histories and other "inherent human data."[55] Hu-manity.co describes the ability to receive fair market value for such data as a "human right" that the company will "fight for."[56] Where people are in possession of especially valuable health data because, for example, they belong to very small or difficult-to-recruit research populations, they might limit their sharing to only the highest bidders. IIn these cases, data sharers might be more appropriately called data scalpers.

Data sharers not only facilitate research through direct contributions to research studies. If use of personal data brokers becomes common, data sharers also have the potential to change how scientists amass data. As one example, if personal health data comes to be viewed as the valuable legal property of the people they describe, studies might need to increase their standard compensation to recruit and retain participants. More serious ethical concerns will be raised if these and other changes have the cumulative effect of reducing every interaction between scientists and those whose data they wish to study to a financial transaction. Other policy issues are raised when recipients of data do not honor the terms under which contributions are made, such as recipients' commitments to keep those data private and secure.

Finally, although data sharers do not usually retain legal interests in the data they give away, they might retain moral interests in how the data are used and controlled. This can result in public controversy, as when 23andMe customers who had opted into research use of their genetic data were upset by news that the company had obtained a patent related to Parkinson's disease using their data.[57] The customers were concerned that the patent would be used to restrict access to genetic testing, contrary to the customers' belief that their data would be used to help patients.[58]

7. The Professional Scientist Persona

The principal focus of **professional scientists** in unregulated mHealth contexts is the generation of generalizable knowledge. This persona may, as a result of their work, derive profit (or accrue financial losses), but the fiscal implications of the research they conduct are not the primary impetus for or refiner of their work. Their engagement in unregulated mHealth research arises from their paid responsibilities.

For decades, the Federal Wide Assurance for the Protection of Human Subjects (FWA) agreement has complicated the professional scientist's relationship with unregulated research generally, and more recently with unregulated mHealth research, by tying ethics oversight to the funding source for a given study. Through their FWA, organizations who have received federal research funding have had the option to extend federal research regulations to their unregulated research activities (colloquially known as "checking the box").[59] For example, in 2013 Sage Bionetworks, a non-profit research organization,[60] received funding from the Robert Wood Johnson Foundation (RWJF), a philanthropy dedicated to public health, to develop the Parkinson mPower and Share the Journey mHealth studies.[61] This work would have constituted unregulated mHealth research by Sage Bionetworks' professional scientists had Sage, which received concurrent federal funding for other projects, not previously voluntarily extended their FWA to cover all their research activities. Interestingly, the percentage of FWA recipients who "checked the box" declined markedly, from around 90% at its peak in the 1980s[62] to less than 50%[63] before the final revisions to the Federal Policy for the Protection of Human Subjects (the Common Rule) went into effect in January 2019.[64] The revised Common Rule withdraws the option for organizations to check the box, eliminating voluntary compliance with the Common Rule by organizations,[65] although there has been some discussion that the Office for Human Research Protections (OHRP)

The Journal of Law, Medicine & Ethics, 48 S1 (2020): 37-48. © 2020 The Author(s)

would extend this option for an unspecified period of time.[66]

In the absence of customary peer, institutional, and regulatory oversight, professional scientists' mHealth research may not be scrutinized for scientific or ethical validity. Without the mandated support of ethics and regulatory professionals, the professional scientist persona may not recognize (or accept) the full extent of the ethical responsibilities they have for their research.[67] Many have pointed to Facebook's "emotional contagion" study as an example of professional scientists abdicating ethical responsibility for their work while operating in an unregulated mHealth context.[68] Further, the misconduct of research by professional scientists has the potential to sow distrust in the scientific enterprise and the legitimacy of rigorously conducted research.

8. The Data Entrepreneur Persona

Data entrepreneurs harvest mHealth data from platforms and monetize it. Their monetization of mHealth data may result in health innovation or discovery or may be purely for commercial gain (e.g., targeted marketing). Although a data entrepreneur may desire community or individual health benefit, all data entrepreneurs are driven by financial gain.

Examples of unregulated mHealth data entrepreneurs include companies like TREND Community, a for-profit company founded by parents of a child with a rare disease.[69] TREND, with the permission of rare disease online community groups, harvests social media data from disease-specific discussion groups on large platforms (e.g., Facebook) using sanctioned developer APIs.[70] TREND then digests the anonymized data using natural language processing and machine learning to identify novel themes, like symptoms that are potentially treatable by drugs. Themes are returned to the community from whom the data were derived for free and are sold by TREND, for example to pharmaceutical companies.

Strava, a free online platform for athletes to share mHealth data, is another example of a data entrepreneur.[71] Strava digests mHealth data of tens of millions of users and monetizes it for advertising and through Strava Metro,[72] a form of public health heat mapping for urban planners and municipalities. Following astute review of previously released data,[73] and subsequent outcry from the Pentagon,[74] Strava recently updated the privacy settings of its heat mapping feature.[75]

Challenges faced by data entrepreneurs include operating within the limits of unregulated or underregulated mHealth platforms from which the data they seek to monetize are derived. In the case of TREND Community, the company struggles with the notification process they use for online community groups before they harvest data[76] — beyond agreements with the moderators of the group and encouraging moderators to post about the upcoming data harvest, the majority of social media platforms do not (currently) facilitate implementing informed consent processes or even the ability to easily bifurcate groups to honor opt-in or opt-out preferences. Further, returning insights that may eventually be discarded after more rigorous investigation could harm individuals, caregivers, or communities who lack access to interpretation resources.

9. The False Flag Persona

The **false flag** persona uses shell identities to access mHealth information that might otherwise be protected under federal regulations to further their research aims. By exploiting unregulated or underregulated mHealth platforms, false flags serve as a conduit of protected information in unprotected form, facilitating uses of health information that would be illegal if those data were collected by other means.

Historical misuse of workers' health information led to many of the very protections false flags seek to circumvent. The advent of mHealth platforms, and the dearth of regulation surrounding the information gathered through them, has only provided new opportunities for such exploitation.[77] Workplace efficiency innovations and employee wellness programs are two potential examples. Recent patent applications from Walmart[78] and Amazon[79] highlight larger employers' desire to maximize the efficiency of their workforce. At the same time, these devices may collect — purposefully or inadvertently — health information about employees that if collected in traditional contexts would be considered protected and unavailable to employers for use in employment decision making. Likewise, companies large and small have adopted employee wellness programs,[80] tracking an ever-increasing panoply of health data[81] that many worry will be used to discriminatory ends.[82]

The exploitation of loopholes in the protection of mHealth data should concern policy makers, especially considering the granularity and specificity of those data. Workers have few protections against false flags.[83] Lack of harmonization of existing federal regulations may open the door for false flags.[84] Concerns are also raised by the lack of transparency regarding how, exactly, false flags are using the data that they collect or with whom they are sharing and selling it.

The Journal of Law, Medicine & Ethics, 48 S1 (2020): 37-48. © 2020 The Author(s)

10. The Sociopath Persona

Finally, the **sociopath** is interested in mHealth as a vehicle to create chaos and cause harm. The sociopath might achieve these objectives by tampering with medical devices that talk to mobile devices, such as pacemakers and spinal simulators, or the mobile devices or mHealth apps that report or interpret such data; exposing the vulnerability of these devices and apps to enable attack by others; altering data used or generated by these devices and apps; or stealing such data for ransom, private sale, or public disclosure.

The exploitation of loopholes in the protection of mHealth data should concern policy makers, especially considering the granularity and specificity of those data. Workers have few protections against false flags. Lack of harmonization of existing federal regulations may open the door for false flags. Concerns are also raised by the lack of transparency regarding how, exactly, false flags are using the data that they collect or with whom they are sharing and selling it.

mHealth might also be used by sociopaths to perpetuate harmful stereotypes or discriminatory agendas. For example, it has recently come to light that white nationalists are using direct-to-consumer genetic testing to confirm their "whiteness" and justify their racist claims.[85]

Although theft of health data is unfortunately not unusual,[86] to our knowledge, no cases of mHealth device or data interference or manipulation have yet been reported. Still, vulnerabilities are well known and are sure to be exploited for misanthropic purposes. In recognition of this constant threat, attendees of the 2019 DEF CON conference were not allowed to enter the Biohacking Village Device Lab to view and conduct security testing of the medical devices on display until they had signed an agreement to "act in good faith, in the best interest[s] of patients," and "avoid inadvertently putting life and safety at risk."[87] This commitment is consistent with the broader effort of a grassroots group of white-hat hackers to establish a Hippocratic Oath for Connected Medical Devices.[88]

Sociopaths themselves may not conduct research with mHealth devices or data. However, they necessarily impact the R&D activities of device manufacturers, which test and refine anti-tampering features for products. Recently, the FDA recalled two insulin pumps after identifying potential risks related to the wireless communication between the pumps and other devices, such as blood glucose meters, continuous glucose monitoring systems, remote controllers, and USB devices. The FDA was concerned that the pumps could be remotely accessed by someone other than the user or caregiver and programmed to deliver unsafe doses of insulin.[89] The pumps will likely be redesigned following significant investigation to address this access problem.

By weaponizing mHealth apps, devices, and data, sociopaths raise significant public health concerns. Unlike empowered patients, self-discoverers, and grinders, who accept the risk that they might be harmed by their activities, sociopaths harm others who have not and would never give such consent. Moreover, sociopaths can potentially injure a large number of people within a short period of time and might be next to impossible to avoid, identify, or bring to justice, especially if they are located in a different country than where their attacks take place. Finally, the activities of sociopaths also raise complex policy questions regarding what kinds of security breaches are foreseeable, who is liable when such breaches occur, and what role regulators should play in ensuring that manufacturers timely identify and address vulnerabilities.

IV. Discussion

We described ten personas of unregulated mHealth researchers based on our professional interactions in and observations of their activities. The descriptions of these personas reveal commonalities among unregulated mHealth researchers despite the considerable diversity of their goals and behaviors. As depicted in Figure 1, unregulated mHealth researchers have general aims that range from primarily philanthropic to misanthropic and objectives that range from primarily self focused to other-focused. Most personas are focused on pursuits intended (directly or indirectly) to benefit society. The activities of false flags and sociopaths present special policy problems because they are by nature opaque, yet given their potential for widespread harm, require close monitoring.

Importantly, a person or entity might qualify for multiple personas, at the same time or over time, depending on their specific activities. For example,

The Journal of Law, Medicine & Ethics, 48 S1 (2020): 37-48. © 2020 The Author(s)

Figure 1
Personas by Primary Beneficiary and Purpose

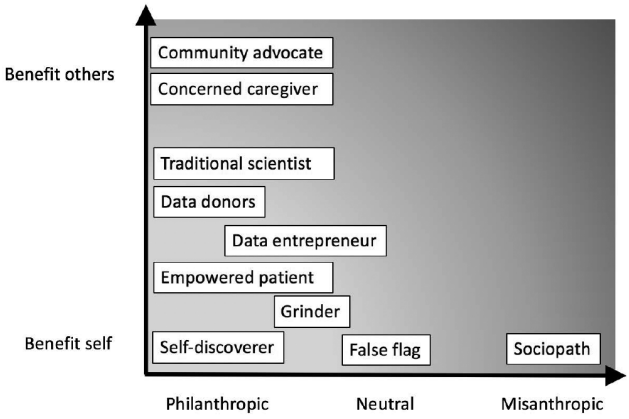
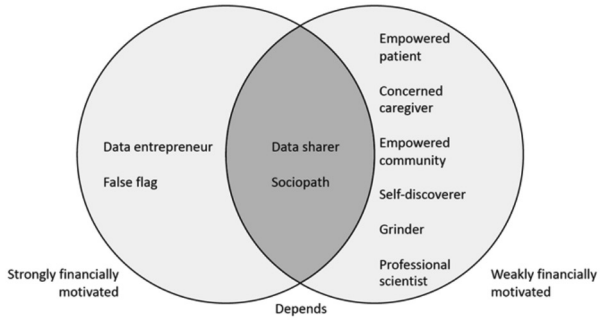


Figure 2
Personas by Financial Motivation



an individual who uses mHealth to manage her Type I diabetes (empowered patient) might care for a child who is also diabetic (concerned caregiver). She might donate data to studies of diabetes (data sharer) and eventually start an advocacy group to support individuals with Type 1 diabetes (empowered community) that aggregates and then itself sells these data for research purposes (data entrepreneur). As another example, an individual who uses mHealth to manage her Crohn's disease (empowered patient) might participate in self-discovery activities to learn about her general risk for cardiovascular disease (self-discoverer). Later, she might implant a device that transmits biometric data related to her cardiovascular health to her mobile phone (grinder). As a final example, a nonprofit institution might be engaged in harvesting wellness data from social media sites (data entrepreneur) that the institution's scientists then investigate in a research study (professional scientist). To help prioritize policy attention, it would be useful to have a better understanding of when and how individuals and entities move between personas and which personas occupy most of their time and resources.

The personas reveal strong profit motives among some unregulated mHealth researchers that might be obscured when they are considered as an undifferentiated whole. As depicted in Figure 2, these profit motives are strong for health entrepreneurs, false flags, and some data sharers and sociopaths. Although monetizing mHealth data is probably ethically acceptable in most circumstances, it is possible that buyers might feel more entitled to use those data in unethical ways — for example, in violation of data use agreements. To avoid such abuses, practices and policies might require greater transparency about the end users and uses of purchased mHealth data.

Some personas highlight a fundamental tension between bodily autonomy and the freedom to know and help oneself, on the one hand, and safety, on the other hand. This tension is best exemplified by self-discoverers and grinders, who sometimes put themselves in harm's way to achieve personal empowerment and self-expression objectives. Empowered patients and concerned caregivers also risk injury, but they might be more willing to accept those risks given the potential rewards of their activities — for example, successful treatment or management of a debilitating disease. This tension is frequently noted with respect to biohacking activities such as DIY gene editing.[90] Its prevalence in the mHealth space provides additional reason to study perceptions of safety, risk, and informed consent in citizen science.

Those perceptions will depend, likely in large part, on the nature of the potential harm at issue and who is affected. Each persona has a different harm profile. We suspect that many would agree that profiles encompassing harm to others — especially when those others are numerous and include vulnerable populations — warrant more immediate policy attention than profiles limited to self-harm. A potential advantage of the personas we have described is that they provide an architecture for building these harm profiles, which in turn can help guide the development of tailored public policies for unregulated mHealth research activities.

Acknowledgments
Research on this article was funded by the following grant: Addressing ELSI Issues in Unregulated Health Research Using Mobile Devices, No. 1R01CA20738-01A1, National Cancer Institute, National Human Genome Research Institute, and Office of Science Policy and Office of Behavioral and Social Sciences Research in the Office of the Director, National Institutes of Health, Mark A. Rothstein and John T. Wilbanks, Principal Investigators.

Note
CG has nothing to declare. MD is employed by Sage Bionetworks, the not-for-profit organization referenced in the Professional Scientist Persona.

The Journal of Law, Medicine & Ethics, 48 S1 (2020): 37-48. © 2020 The Author(s)
https://doi.org/10.1177/1073110520917028 Published online by Cambridge University Press

References

1. M.A. Rothstein, J.T. Wilbanks, and K.B. Brothers, "Citizen Science on Your Smartphone: An ELSI Research Agenda," *Journal of Law, Medicine & Ethics* 43, no. 4 (2015): 897-903.
2. A. Cooper, *The Inmates Are Running the Asylum* (Indianapolis: Macmillan Publishing Co., Inc., 1999): at 123.
3. 45 C.F.R. part 46.
4. 21 C.F.R. parts 50, 56.
5. 15 U.S.C. ch. 2, subch. I.
6. Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 18 U.S.C., 26 U.S.C., 29 U.S.C., and 42 U.S.C.).
7. Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, tit. XIII, 123 Stat. 115, 226-79 (2009) (codified as amended in scattered sections of 42 U.S.C.).
8. Federal Food, Drug, and Cosmetic Act (FDCA), Pub. L. No. 75-717, 52 Stat. 1040 (1938) (codified as amended at 21 U.S.C. §§ 301 et seq.)..
9. Alaska Stat. Ann.§ 18.13.010(a)(2); Colo. Rev. Stat. Ann.§ 10-3-1104.7(1)(a); Fla. Stat. Ann.§ 760.40(2)(a).
10. For example, a biohacker named Josiah Zayner was under investigation in California for allegedly practicing medicine without a license in violation of state laws that govern medical practice. R. Hsu, "Is Biohacking 'the Practice of Medicine?': Regulators Might Think So," Baylor College of Medicine PolicyWise Blog, July 19, 2019, *available at* <https://blogs.bcm.edu/2019/07/19/is-biohacking-the-practice-of-medicine-regulators-might-think-so/> (last visited January 13, 2020).
11. C. Sahin, "Rules of Engagement in Mobile Health: What Does Mobile Health Bring to Research and Theory?" *Contemporary Nurse* 54, nos. 4-5 (2018): 374-387.
12. A. Coravos et al., "Digital Medicine: A Primer on Measurement," *Digital Biomarkers* 3, no. 2 (2019): 31-71.
13. 45 C.F.R. § 46.102(l).
14. See *infra* Part III.4-5.
15. M.V. Eitzel et al., "Citizen Science Terminology Matters: Exploring Key Terms," *Citizen Science: Theory and Practice* 2 (2017): 1-20; L. Ceccaroni, A. Bowser, and P. Brenton, "Civic Education and Citizen Science: Definitions, Categories, Knowledge Representation," in L. Ceccaroni and J. Piera, eds., *Analyzing the Role of Citizen Science in Modern Research* (Hershey, PA: IGI Global, 2017): at 1-23. The definition is also associated with its own ethical concerns. C.G. Guerrini et al., "Biomedical Citizen Science or Something Else? Reflections on Terms and Definitions," *American Journal of Bioethics* 19, no. 8 (2019): 17-19.
16. C.J. Guerrini et al., "Donors, Authors, and Owners: How Is Genomic Citizen Science Addressing Interests in Research Outputs?" *BMC Medical Ethics* 20, no. 84 (2019).
17. National Academies of Sciences, Engineering, and Medicine, "Mapping the Landscape," in *Learning through Citizen Science: Enhancing Opportunities by Design* (Washington, D.C.: The National Academies Press, 2018): at 27-52.
18. *See* Rothstein, Wilbanks, and Brothers, *supra* note 1.
19. "The #WeAreNotWaiting Diabetes DIY Movement," Healthline, *available at* <https://www.healthline.com/health/diabetesmine/innovation/we-are-not-waiting#1> (last visited January 13, 2020).
20. A. Rao and M. Cunnane, "Diabetes Hacking 101," WNYC Studios, April 22, 2016, *available at* <https://www.wnyc.org/story/diabetes-hacking-with-ben-west/> (last visited January 13, 2020).
21. OpenAPS.org, *available at* <https://openaps.org/> and <https://www.youtube.com/watch?v=kgu-AYSnyZ8> (both last visited January 13, 2020).
22. See "#WeAreNotWaiting Diabetes DIY Movement," *supra* note 19.
23. Six Until Me, "We Are Not Waiting: CGM in the Cloud (Part 1)," July 10, 2014, *available at* <https://sixuntilme.com/wp/2014/07/10/cgm-cloud-part/> (last visited January 13, 2020).
24. *Id.*
25. YouTube, "MoleMapper," October 15, 2015, *available at* <https://youtu.be/iAvw-gCGPI98> (last visited January 13, 2020).
26. ResearchKit, *available at* <http://researchkit.org/> (last visited January 13, 2020).
27. MoleMapper, *available at* <https://molemapper.org/> (last visited January 13, 2020).
28. See OpenAPS.org, *supra* note 21.
29. Facebook, CGM in the Cloud, *available at* <https://www.facebook.com/groups/cgminthecloud/> (last visited January 13, 2020; login required).
30. *See* MoleMapper, *supra* note 27.
31. Crohnology, *available at* <https://crohnology.com/> (last visited September 23, 2019).
32. Families of Children with Rare Disease Fuel Gene Therapy Research," *The Scientist*, April 30, 2018, *available at* <https://www.the-scientist.com/features/families-of-children-with-rarediseases-fuel-gene-therapy-research-64279> (last visited January 20, 2010).
33. BioCurious, "Silicon Valley's Hackerspace for Biology," *available at* <http://biocurious.org/> (last visited January 13, 2020).
34. S.C. Nelson and S.M. Fullerton, "'Bridge to the Literature'? Third-Party Genetic Interpretation Tools and the Views of Tool Developers," *Journal of Genetic Counseling* 27, no. 4 (2018): 770-781.
35. *Id.*
36. A.D. Grant, G.I. Wolf, and C. Nebeker, "Approaches to Governance of Participant-led Research: A Qualitative Case Study," *BMJ Open* 9 (2019): e025633.
37. B. Greshake et al., "openSNP — A Crowdsourced Web Resource for Personal Genomics," *PLoS ONE* 9, no. 3 (2014): e89204; T. Haeusermann et al., "Open Sharing of Genomic Data: Who Does It and Why," *PLoS ONE* 12, no. 5 (2017): e0177158.
38. S. Tandy-Connor et al., "False-Positive Results Released by Direct-to-Consumer Genetic Tests Highlight the Importance of Clinical Confirmation Testing for Appropriate Patient Care," *Genetics in Medicine* 20, no. 12 (2018): 1515-1521; T. Moscarello et al., "Direct-to-Consumer Raw Genetic Data and Third-Party Interpretation Services: More Burden Than Bargain?" *Genetics in Medicine* 21, no. 3 (2019): 539-541
39. See Grant et al., *supra* note 36.
40. C.G. Allen et al., "The Impact of Raw DNA Availability and Corresponding Online Interpretation Services: A Mixed-methods Study," *Translational Behavioral Medicine* 8, no. 1 (2018): 105-112.
41. C.G. Guerrini et al., "Who's on Third? Regulation of Third-Party Genetic Interpretation Services," *Genetics in Medicine* 22, no. 1 (2020): 4-11.
42. E. Murphy, "Law and Policy Oversight of Familial Searches in Recreational Genealogy Databases," *Forensic Science International* 292 (2018): e5-e9.
43. B. Popper, "Cyborg America: Inside the Strange New World of Basement Body Hackers," *The Verge*, August 8, 2012, *available at* <https://www.theverge.com/2012/8/8/3177438/cyborg-america-biohackers-grinders-body-hackers> (last visited January 13, 2020).
44. *Id.*
45. The DIY Cyborg," VICE, October 31, 2013, *available at* <https://www.vice.com/en_us/article/7b79kx/diy-cyborg> (last visited January 13, 2010).
46. R. Robbins, "A Cyborg Magician Explains Why She Implanted 26 Microchips and Magnets in Her Body," STAT, September 6, 2019, *available at* <https://www.statnews.com/2019/09/06/a-cyborg-magician-explains-why-she-implanted-26-microchips-and-magnets-in-her-body/> (last visited January 13, 2020).

The Journal of Law, Medicine & Ethics, 48 S1 (2020): 37-48. © 2020 The Author(s)

47. A. Hines, "Magnet Implants? Welcome to the World of Medical Punk," *New York Times,* May 12, 2018, *available at* <https://www.nytimes.com/2018/05/12/us/grindfest-magnet-implants-biohacking.html> (last visited January 13, 2020).
48. K. Warwick et al., "The Application of Implant Technology for Cybernetic Systems," *JAMA Neurology* 60, no. 10 (2003): 1369-1373.
49. C.E. Bouton et al., "Restoring Cortical Control of Functional Movement in a Human with Quadriplegia," *Nature 533*, no. 7602 (2016): 247-250.
50. M. Russell, "Body Modifier Brendan Russell to Stand Trial Over Woman's Snowflake Implant Death," News.com.au, July 19, 2019, *available at* <https://www.news.com.au/national/nsw-act/courts-law/body-modifier-brendan-russell-to-stand-trial-over-womans-snowflake-implantdeath/news-story/ca3b-047c9a9b426fedca8d08a0550464> (last visited January 13, 2020).
51. *Id.*
52. 23AndMe, "About Us," *available at* <https://mediacenter.23andme.com/company/about-us/> (last visited January 13, 2020).
53. Open Humans, *available at* <https://www.openhumans.org/> (last visited January 13, 2020).
54. CoverUS, *available at* <https://coverus.health/> (last visited January 13, 2020).
55. Hu-manity.co, *available at* <https://hu-manity.co/who-is-hu-manity-co123-2/> (last visited January 13, 2020).
56. Hu-manity.co, "Frequently Asked Questions," *available at* <https://hu-manity.co/faqs/> (last visited January 13, 2020).
57. S. Sterckx et al., "'Trust is Not Something You Can Reclaim Easily': Patenting in the Field of Direct-to-Consumer Genetic Testing," *Genetics in Medicine* 15, no. 5 (2013): 382-387.
58. *Id.*
59. Federal Policy for the Protection of Human Subjects, 82 Fed. Reg. 7149, 7180 (January 19, 2017) (codified at 45 C.F.R. part 46).
60. Sage Bionetworks, *available at* <www.sagebionetworks.org> (last visited January 13, 2020). We note that one of the authors (Doerr) is employed by Sage Bionetworks.
61. J. Comstock, "Partners' Engagement Engine and 7 More RWJF-Backed Digital Health Projects," MobiHealth News, March 25, 2015, *available at* <https://www.mobihealthnews.com/41768/part-ners-engagementengine-and-7-more-rwjf-backed-digital-health-projects> (last visited January 13, 2020).
62. L. Odwazny, "Finding Flexibility in the Federal Regulations-Fear Not the Feds!" (2014), *available at* <https://www.nwabr.org/eventsprograms/2014-ohrp-research-community-forum-irbeducation-conference/conference-presentation> (last visited January 13, 2020).
63. Children's Hospital of Philadelphia Research Institute, "Federalwide Assurance (FWA): Compliance with Federal Regulatory Requirements and Guidelines," *available at* <https://irb.research.chop.edu/federalwide-assurance-fwa> (last visited January 13, 2020).
64. Federal Policy for the Protection of Human Subjects: Six Month Delay of the General Compliance Date of Revisions While Allowing the Use of Three Burden-Reducing Provisions During the Delay Period, 83 Fed. Reg. 28,497 (June 19, 2018).
65. Federal Policy for the Protection of Human Subjects, 82 Fed. Reg. at 7181.
66. Changes to Human Subject Research Rules Impact Studies Funded Non-Federally, Fox Rothschild, LLC, February 11, 2019, *available at* <https://www.foxrothschild.com/publications/changes-to-human-subject-research-rulesimpact-studies-funded-non-federally/> (last visited January 13, 2020).
67. J. Metcalf, E. Moss, and D. Boyd, "Owning Ethics: Corporate Logics, Silicon Valley, and the Institutionalization of Ethics," *Social Research: An International Quarterly* 82, no. 2 (2019): 449-476..
68. C. Chambers, "Facebook Fiasco: Was Cornell's Study of 'Emotional Contagion' an Ethics Breach?" *The Guardian*, July 10, 2014, *available at* <https://www.theguardian.com/science/head-quarters/2014/jul/01/facebook-cornell-study-emotional-contagion-ethics-breach> (last visited January 13, 2020).
69. TREND Community, *available at* <https://trend.community/> (last visited September 23 2019).
70. *Id.*
71. Strava Business, *available at* <https://business.strava.com/> (last visited September 23 2019).
72. A. Gulley, "Strava's Plan to Revolutionize Commuting," Outside Online, May 15, 2014, *available at* <https://www.out-sideonline.com/1923291/stravasplan-revolutionize-commuting?source=post> (last visited January 13, 2020).
73. D. Robb, "Building The Global Heat Map," Medium, November 1, 2017, *available at* <https://medium.com/strava-engineering/the-global-heat-map-now-6x-hotter-23fc01d301de> (last visited January 13, 2020).
74. B. Chappell, "Pentagon Reviews GPS Policies After Soldiers' Strava Tracks Are Seemingly Exposed," National Public Radio, January 29, 2018, *available at* <https://www. npr.org/sections/I-way/2018/01/29/581597949/pentagon-reviews-gps-data-after-soldiers-strava-tracks-are-seemingly-exposed> (last visited January 13, 2020).
75. D. Lumb, "After Exposing Secret Military Bases, Strava Restricts Data Visibility," *engadget*, March 13, 2018, *available at* <https://www.engadget.com/2018/03/13/after-exposing-secret-military-bases-strava-restricts-data-visi/> (last visited January 13, 2020).
76. Personal communication from Blair Van Brunt to author (MD) (August 29, 2019).
77. I. Anjunwa, K. Crawford, and J. Schultz, "Limitless Worker Surveillance," *California Law Review* 105, no. 3 (2017): 735-776.
78. A. Mateescu and A. Nguyen, "Explainer: Workplace Monitoring & Surveillance," Data & Society, February 6, 2019, *available at* <https://datasociety.net/wp-content/uploads/2019/09/DandS_WorkplaceMonitoringandSurveillance-.pdf> (last visited January 13, 2020); C. O'Donovan, "Walmart's Newly Patented Technology for Eavesdropping on Workers Presents Privacy Concerns," BuzzFeed News, July 11, 2018, *available at* <https://www.buzzfeednews.com/article/carolineodonovan/walmart-just-patented-audio-surveillance-technology-for> (last visited January 13, 2020).
79. C. Yeginsu, "If Workers Slack Off, the Wristband Will Know. (And Amazon Has a Patent for It.)," *New York Times*, February 1, 2018, *available at* <https://www.nytimes.com/2018/02/01/technology/amazon-wristband-tracking-privacy.html> (last visited January 13, 2020).
80. L. Schencker, "Would You Wear a Fitbit for Work?," *Chicago Tribune*, November 11, 2016, *available at* <https://www.nytimes.com/2018/02/01/technology/amazon-wristband-tracking-privacy.html> (last visited January 13, 2020).
81. C. Rowland, "With Fitness Trackers in the Workplace, Bosses Can Monitor Your Every Step — and Possibly More," *Washington Post*, February 16, 2019, *available at* <https://www.washingtonpost.com/business/economy/with-fitness-trackers-in-the-workplace-bosses-can-monitor-your-every-step--and-possibly-more/2019/02/15/75ee0848-2a45-11e9-b011-d8500644dc98_story.html> (last visited January 13, 2020).
82. P. Holley, "Wearable Technology Started by Tracking Steps. Soon, It May Allow Your Boss to Track Your Performance," *Washington Post*, June 28, 2019, *available at* <https://www.washingtonpost.com/technology/2019/06/28/wearable-technology-started-by-tracking-steps-soon-it-may-allow-your-boss-track-your-performance/> (last visited January 13, 2020).
83. Ajunwa, Crawford, and Schultz, *supra* note 77; A. Delgado, "Employee Privacy at Stake as Surveillance Technology Evolves," CBS News, August 14, 2018, *available at* <https://www.cbsnews.com/news/employee-privacy-surveillance-technology-evolves/> (last visited September 23, 2019).

The Journal of Law, Medicine & Ethics, 48 S1 (2020): 37-48. © 2020 The Author(s)

84. J.J. Lazzarotti, "Wellness Programs Continue to Face Compliance Challenges," Jackson Lewis Benefits Law Advisor, February 7, 2019, *available at* <https://www.benefitslawadvisor.com/2019/02/articles/employeehealth-welfare-plans/wellness-programs-continue-to-facecompliance-challenges/> (last visited January 13, 2020).
85. E. Boodman, "White Nationalists are Flocking to Genetic Ancestry Tests. Some Don't Like What They Find," STAT, August 16, 2017, *available at* <https://www.statnews.com/2017/08/16/white-nationalists-geneticancestry-test/> (last visited January 13, 2020).
86. J. Vincent, "1.5 Million Affected by Hack Targeting Singapore's Health Data," *The Verge*, July 20, 2018, *available at* https://www.theverge.com/2018/7/20/17594578/singapore-health-data-hack-sing-health-prime-minister-lee-targeted (last visited September 23, 2019); "Hackers are Stealing Millions of Medical Records — and Selling Them on the Dark Web," *CBS News,* February 14, 2019, *available at* <https://www.cbsnews.com/news/hackers-steal-medical-records-sell-them-on-dark-web/> (last visited September 23, 2019).
87. Biohacking Village Device Lab Registration Form, DEF CON 2019 (on file with authors).
88. B. Woods, A. Coravos, and J.D. Corman, "The Case for a Hippocratic Oath for Connected Medical Devices: Viewpoint," *Journal of Medical Internet Research* 21, no. 3 (2019): e12568.
89. E. Wicklund, "FDA Issues Recall For Medtronic mHealth Devices Over Hacking Concerns," *mHealth Intelligence*, June 28, 2019, *available at* <https://mhealthintelligence.com/news/fda-issues-recall-for-medtronic-mhealth-devices-over-hacking-concerns> (last visited January 13, 2020).
90. C.J. Guerrini, G.E. Spencer, and P.J. Zettler, "DIY CRISPR," *North Carolina Law Review* 97, no. 5 (2019): 1399-1462, *available at* <https://scholarship.law.unc.edu/nclr/vol97/iss5/17> (last visited January 13, 2020).

The Journal of Law, Medicine & Ethics, 48 S1 (2020): 37-48. © 2020 The Author(s)