consider: would it have made those business ventures harder or easier to defend against a lawsuit by patients whose medical records were used? What would you recommend to a state that approaches you about how to design its own statutes concerning use of medical records in developing new diagnostic tools or treatments? Should it adopt one of these approaches? How might you improve on whichever one you think is most useful to achieve the normative result you seek to support?

B. European Union

The General Data Protection Regulation (GDPR) made effective in 2018 creates a broad set of new individual rights in personal data, including health data. GDPR imposes a comprehensive privacy framework that gives eight basic rights to individuals regarding their data. Some are analogous to rights in HIPAA, like rights of access and rectification. Others are simply stronger. For example, GDPR's consent requirement restricts the use of data to a tightly defined purpose of which the data controller has already informed the individual.

Some GDPR rights do not find analogues in the U.S. framework. For instance, the GDPR right to restrict processing and right of erasure afford individuals the ability to withdraw their consent and to place restrictions on the future use of their data or cause its deletion.[48] However, these rights are subject to caveats—the right to erasure, for instance, only applies when there is not a compelling reason to continue holding the data.

Elevated protections apply to "special category data," including genetic, biometric, and health data. This data can be used only if one of ten conditions is met, including application to health care or having explicit consent.[49] However, the consensus appears to be that GDPR does not apply to anonymized health data, a significant similarity to HIPAA.[50]

Another EU directive created an interesting set of sui generis "database rights" that can apply to electronic health records or any type of health data. Unlike the American *Feist Publications* rule, this right is distinct from copyright and does not require a showing of creativity or originality—only a "substantial investment in obtaining, verifying, or presenting" the data.[51] The contents of that database are then protected for fifteen years, with indefinite renewals available upon continued

---

[48] Lara Cartwright-Smith et al., *Health Information Ownership: Legal Theories and Policy Implications*, 19 Vand. J. Ent. & Tech. L. 207, 238 (2016); *Right to Restrict Processing*, U.K. Info. Comm'r's Office, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-restrict-processing/ (last visited Jan. 23, 2021).

[49] *See Special Category Data*, U.K. Info. Comm'r's Office, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/ (last visited Jan. 23, 2021).

[50] *See, e.g.*, *GDPR and Human Subjects*, Office of the Vice President for Research, Brown Univ., https://www.brown.edu/research/gdpr-and-human-subjects (last visited Jan. 23, 2021).

[51] Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the Legal Protection of Databases, ch. III, art. 7, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31996L0009#d1e757-20-1.

addition and investment.[52] There does not appear to be any reason why these rights would not extend to databases containing health data, although there is a curious dearth of public discussion explicitly making that connection.[53]

[52] *What You Need to Know About UK Database Rights*, Cooley GO, https://www.cooleygo.com/what-you-need-to-know-about-uk-database-rights/ (last visited Jan. 23, 2021).

[53] *But see* Fiona Kellas, *IP Considerations in Digital Health*, Maucher Jenkins (May 18, 2018), https://www.maucherjenkins.com/news-and-events/2018/ip-considerations-in-digital-health.

III. Reform Proposals

Many lawmakers and scholars contend that none of the legal systems reviewed in Part II is adequate to handle fairly and efficiently business initiatives of the sort described in Part I. They disagree, however, concerning what system of rules would be better. This Part presents a few of the major competing proposals.

Property, Privacy, and the Pursuit of Interconnected Electronic Medical Records

Mark A. Hall
95 Iowa L. Rev. 631 (2010).

IV. SHOULD PATIENTS HAVE PROPERTY RIGHTS?

A. In Favor of Property

When confronted with similar issues, lawmakers have created intellectual property rights—such as copyrights and patents—as exceptions to the general rule that information is in the public domain. These legal rights serve the focused goal of generating private incentives to invest time, energy, and resources into creating, discovering, and developing valuable information. Should a similar approach be used for medical information? Even though incentives are not needed to create medical information since it is created when patients seek treatment, similar financial rewards are needed to compile and transform it into useful forms. Property rights are an ideal way to bundle patients' rights into a legal form that can be monetized and put into a stream of commerce. Fully realizing the economic potential of valuable assets is, in modern times, property law's primary purpose: "We deem something property in order to facilitate its transfer."

Blackstone famously intoned that "[t]here is nothing which so generally strikes the imagination, and engages the affections of mankind, as the right of property." Even when noneconomic values loom large, some civil-rights advocates favor property protections because of their strength and resonance in our modern legal system. For instance, civil libertarian George Annas and his colleagues advocate giving people property rights in their own DNA in order to protect infringements from commercial interests. Even propertization opponent Sonia Suter concedes that "[p]roperty has always been a powerful tool to protect important interests because it is familiar and effective. [It] has teeth and 'symbolic force.'"

The opposite of propertization is placing information in the public domain. That route is unappealing for a variety of reasons. Providers' and insurers' existing property rights would be eliminated. That might pose significant constitutional issues and spark strong political opposition. Moreover, since privacy protections would remain, public-domain access would still be very limited. And, any economic benefits derived from this information would not flow back to patients. Conferring additional and superior property rights to patients appears to be a more feasible and appropriate route.

Calebresi and Melamed's seminal economic theory also supports this route. Their classic article outlines the general criteria by which society should prefer a property regime over a liability, or, in our case, regulatory regime for determining access to and use of valuable resources. In general, property rules are preferable when markets determine best uses more efficiently than courts or regulatory agencies. Markets are generally preferred in economic arenas unless "market valuation of the entitlement is deemed inefficient," or when a liability or regulatory rule "facilitates a combination of efficiency and distributive results which would be difficult to achieve under a property rule."

In medical settings, these obviously are large questions that demand wide-ranging analysis, but much of that can be short-circuited by observing that we do not face an all-or-nothing choice. Medical privacy law already contains much of the normative content missing from property law in its plethora of restrictions on access to and use of medical information. The issue, then, is whether the law governing medical records should be overwhelmingly normative—under a legal regime that specifies most of the allowable and unallowable uses—or instead should have a neutral zone that permits individuals more leeway to decide what uses to make of their medical information and what value those uses should have. Adding property rights to privacy protections moves us in that direction.

The main concern of privacy law is controlling access to information rather than putting information to innovative uses. Therefore, it does not embrace a set of norms and practices that countenance financial transactions. Privacy law facilitates the ready release of information only for narrow and specific treatment purposes. Thus, it primarily expresses negative liberties: the rights to exclude, limit, and refuse. Property law, in contrast, embraces a broader set of positive liberties: the rights to use, transfer, and develop.

Also, medical privacy rights grow out of the special nature of the relationships between patients and clinicians. Therefore, privacy rights are enforceable only against the particular providers who generate and possess this information. It is difficult to anticipate and specify all the conditions needed to allow the free flow of medical information since this depends on who possesses and controls the information and on its variety of potential uses. The same is true for specifying necessary protections. Building these rights and protections into the legal status of the information itself is therefore an advantage. The other option is for freedoms and protections to derive only from the origins or location of the information—that is, a patient's particular relationship with the person who holds the information.

Property law addresses these enforcement concerns by creating rights that "run with the chattel." In other words, the rights are enforceable against the world at large and not just against particular parties based on their relationship with the patient. Also, property law provides a strong legal basis for seeking injunctive remedies against infringements. To these extents, property law might confer more extensive rights than privacy law alone.

Finally, property law invokes a fairly standard bundle of protections that are well-established and understood in the law, rather than requiring specification and interpretation of each stick in the bundle. This relative simplicity and ease of recognition facilitate more efficient development. Using examples from for the former Soviet bloc, property law scholar Michael Heller concludes that productive use "emerges more successfully in resources that begin transition [into a newly

created market economy] with a single owner holding a near-standard bundle of market legal rights." It is always possible to craft more tailored legal specifications that fit a particular subject area more exactly, but perfection should not be pursued to the detriment of workable improvements. Property law theorist Henry Smith explains that standardized legal bundles can ultimately be more efficient because they are recognizable and so conserve on information costs: legal "lumpiness has its advantages" because "the on/off quality of [property law] allows complexity to be managed through modularity."

B. Against Property

There are several substantial arguments against giving patients property rights in their medical information. Many privacy advocates view propertization of personal information as "morally obnoxious . . . anathema" because of the law's expressive or symbolic function. They feel that property law connotes a crass commercial attitude about information that inherently has deeply emotional and existential human significance. Sonia Suter articulates this position most forcefully. In her view, medical information is "integral to the self" because it "is about us in very central and personal ways." Rather than protecting "the wholeness of the self and of relationships through which the self flourishes," property "by definition, commodifies and disaggregates the parts from the self." Therefore, "conceptualizing [medical] information as property distorts and impoverishes our understanding of the dignitary, personhood interests we have in this information and the nature of relationships we hope will be built around and through its disclosure."

Those who stress the special significance of personal medical information are adamantly opposed to governing its use primarily through marketplace norms. Intellectual property and privacy law scholars are rightly concerned that reducing the exchange of information to purely transactional legal analysis will permit commercial practices that give people little or no choice over what becomes of their vital information. According to Jessica Litman, the assumption "that initial legal ownership of [information] would enable individuals to restrain their downstream use by negotiating conditions of use before disclosing them . . . . seems to be inspired by a fairy-tale picture of easy bargaining in cyberspace through the use of intelligent agents . . . . [t]hat's nonsense." Mark Lemley agrees that, "from a privacy perspective, an intellectual property right that is regularly signed away may turn out to be less protection than we want to give individuals. To do any good, the right might have to be inalienable and waivable only in certain limited circumstances."

These concerns have pressing salience for access to and control of medical information. One of the core elements in property law's classic bundle of rights is full alienability—allowing property owners to permanently relinquish all of their rights to a purchaser. Although actual commercial practices embrace many less absolute transactional forms such as leasing and licensing, property law disfavors prohibitions of full alienation. Yet it is unlikely our legal regime would ever allow patients to forever relinquish rights to access and control their private medical information because full alienability conflicts with the values we associate with personal medical information. In general, medical-information law should have a strong normative content—specifying permissible and impermissible uses and modes of obtaining consent. Privacy law does this to a considerable extent, but most of property law is adamantly neutral.

This clash between property and privacy regimes could be avoided by constructing a more limited bundle of property rights, as intellectual property law usually does, for example, by limiting the length of those rights, or as patent law specially does to take account of the importance of medical uses. For instance, "property rights" in medical information could be defined in a way that is nonexclusive and that permits free government access for public health and research purposes without having to pay "just compensation." But, the more sticks that are removed or shortened, the less compelling the argument is for pursuing a bundling approach at all. As Mark Lemley observes, "a properly designed right would look rather more like a system of regulation than a system of property rights."

An information system's architecture could be designed creatively to reduce the complexity of a nonbundled regulatory regime. The detailed limits required by regulators or desired by contracting parties could be specified and enforced efficiently by embedding them in the software that operates I-EMRs [interconnected electronic medical records]. The technological sophistication of electronic systems makes it possible to protect individual rights at a much more granular level than traditional regulatory or contracting systems. Thus, according to Jonathan Zittrain, using a "trusted system may allow for 'baby-splitting' among interests that is not feasible in more traditional regimes." For example, "in place of the stalemate over who should 'own' a record, a well-defined self-enforcing rights architecture could allow information sharing without having to ultimately resolve matters in as coarse a way as 'owner' or 'nonowner."

Still, if any kind of property regime were adopted for medical information, additional lines would need to be drawn between medical information and other personal information, over which there are no property rights. The balance of opinion among property- and privacy-law scholars opposes propertizing personal information generally. For medical information, there are good reasons to find the propertization arguments more compelling, but if we accepted those arguments we would then need to differentiate the two realms of personal information, which adds an additional element of complexity.

However, much the same is true for any type of intellectual property regime. Because property rights are not inherent in information, it is always necessary when creating intellectual property to define and justify what is protected from what is not. In part, we have undertaken this chore already for medical information by defining special privacy protections. Similar definitions could also describe the scope of patients' property rights. However, property law definitions would likely differ from those in existing privacy law because, as noted above, the latter arise from special fiduciary responsibilities of health care providers and they have somewhat different aims. Excavating these additional layers is another reason to pause before leaping into a property regime.

Finally, property rights might frustrate the very goals they seek by inhibiting the public-goods value of medical information. Creating more legal rights may not be the best solution to an anticommons problem that was created in part by too many legal rights in the first place. "An intellectual property law governing personal data would result in the creation of literally billions of new intellectual property rights every day; economics wisely counsels us not to expect frictionless licensing in this circumstance." The Internet, for instance, owes its spectacular success to the fact that its basic structure and elements are all in the public domain. Imagine how its development might have stalled or been severely stunted if key elements were protected by copyrights or patents that owners refused to license or provide for free.

For medical information, Professor Marc Rodwin makes an impressive argument that conferring property rights would interfere with important public goods, such as assembling research databases and engaging in public health monitoring. His focus is primarily on de-identified data rather than the personalized medical records we consider here, but his objections must be considered carefully. If patients had property rights in their personal medical data, would the government have to pay them "just compensation" for any "taking" of medical information for public purposes? Not if the information is not identifiable to the patient, since any property interest resides in patient-specific information. Government presumably would not take identifiable information except for public health purposes under its police power, as now happens without constitutional objection. Any newly created or expanded property rights would be against the backdrop of these long-standing government practices and policies and therefore could be made subject to them. Still, creating new property rights might give patients more legal power than they currently possess to refuse uses or demand payments for either public or private purposes.

C. Common Ground

Whichever route is pursued, it will not lead to a pure legal regime. As with any other type of intellectual property, because these legal rules are specially constructed to serve an instrumental purpose, we cannot avoid a fairly sui generis set of rules, especially considering the unique importance attached to medical information. Therefore, in the end it may not matter a great deal whether the bundle of rights in medical information is built stick by stick, starting with simple contract and privacy rights, or winnowed and reconstructed from a larger standard set of property rights. This gravitational pull toward a common ground can be seen in the broader debate over personal information generally. Some scholars favor a special bundle of property rights, others favor a special set of tort rules, and still others feel that contract rights are sufficient if properly enforced. Despite these differences, what is common (albeit far from identical) among them is a set of shared concerns about the following important interests that require legal protection and facilitation. By more finely mapping this common ground, the following principles can guide construction of patients' rights to license access to their own medical information.

1. People should be able themselves, or through their agents, to authorize access to and use of their medical information for financial rewards, and these licenses should be transferable.

Without clear recognition of the core entitlement to commercialize access rights, network benefits will not be sufficiently captured, or "internalized" to give anyone in the health care finance and delivery system (as it is currently structured) enough incentive to invest in the construction of I-EMRs. Conferring rights of access and use should not be demandable as an absolute condition of providing or insuring health care services. However, positive or negative incentives can be offered as long as they are not unconscionable—for instance, providing a modest discount to patients who allow their data to be warehoused.

2. Default rules should be set with some degree of paternalism toward protecting patients' interests, in order to take account of the cognitive and other limitations on consent involving vital medical information.

For instance, default rules can be set in a way that forces more choice and more information. Usually, to minimize transaction costs legal default rules are set in an "opt-out" fashion, so that

these rules apply unless otherwise specified, according to what most parties would accept when fully informed. However, if a substantial minority strongly dislikes the majority option, there may be good reason to adopt a more protective default rule that requires parties to affirmatively opt in to the majority position. Otherwise, the net social condition might be suboptimal if the default position is offered only on a take-it-or-leave-it basis, with no real choice or with a technical "choice" but inadequate notice.

3. Some rights or protections should be nonwaivable (or inalienable) and should follow the information regardless of agreement or provenance.

For instance, patients should always retain their basic rights to inspect, copy, and correct medical records, and patients should have a nonwaivable right to revoke any permissions they give for access or use. Enabling patients to back out of an improvident bargain helps correct market flaws by preventing initial mistakes from having long-term consequences. This power also gives market participants a strong incentive to conform their behavior to patients' expectations. Further protections are available by overseeing the "infomediaries" that assemble and process medical information and by embedding safeguards in the software architecture of the system. These protective mechanisms can originate either from regulators or entrepreneurs.

4. Patients' rights to control or sell access to their medical information should be limited to data that can be linked to them personally.

If information is anonymized (or "deidentified") so that it cannot reasonably be connected to anyone in particular, the individual's claim to "ownership" of the information should cease, along with the need for strong legal protections. Recognizing this limit will foster more public goods derived from medical research and public health monitoring.

Much Ado About Data Ownership

Barbara J. Evans
25 Harv. J.L. & Tech. 70 (2011)

I. INTRODUCTION

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Privacy Rule, a major federal regulation affecting health information privacy, is criticized both for hindering access to health data and for allowing too much data access. . . . Regulatory approaches that have worked fairly well in clinical research "are not easily exported and applied to the very different challenges of [informational] research." As the Department of Health and Human Services ("HHS") was developing the HIPAA Privacy Rule in 2000, multiple public commenters, including several members of Congress, voiced this same concern. Research with data and tissues has grown in importance, making these problems more apparent and fueling calls for reform. In 2009, the Institute of Medicine ("IOM") called for changes to the HIPAA Privacy Rule. The IOM recommended replacing the Privacy Rule with an unspecified "new approach" for regulating privacy and access to data for use in health research. HHS recently published an advance notice of

proposed rulemaking ("ANPRM"), which called for changes to the Common Rule but offered few specifics, instead posing seventy-four broad questions for public comment.

Rather than reforming the regulations, other proposals seek legislation to clarify data ownership. Ownership of the data held in administrative and clinical databases is a matter of state law and, in most states, data ownership is not clearly defined. Patient data ownership is touted by some observers as a way to enhance patient privacy and by others as a way to make data more widely available for research. Still others call for public (governmental) ownership to enhance researchers' access to data. While differing in details, data propertization proposals seem to agree that property rights in data are important and that clarifying them should be high on the legislative agenda. Ominously, this view is starting to infect policymakers, raising a real risk that what began as an abstract scholarly debate may end in ill-advised legislation.

The urge to propertize health data needs to be weighed skeptically and with a clear understanding of how property rights actually work. If pursued, data ownership may disappoint many of its proponents because of a surprising truth: the framework of patient entitlements and protections afforded by the HIPAA Privacy Rule and the Common Rule is strikingly similar to what patients would enjoy if they owned their data. Part II challenges the claim that private data ownership would improve privacy protection. It finds that both regimes — patient ownership of data, on the one hand, and the federal regulatory protections, on the other — provide pliability-rule protection[32] that strikes a balance between patient control and the public's need for data access. Both regimes allow some unconsented uses of patients' data, and the grounds for nonconsensual data use are substantively similar under either regime. This similarity suggests that property rights may not be the right locus for reform. Creating property rights in data would produce a new scheme of entitlements that is substantively similar to what already exists, thus perpetuating the same frustrations all sides have felt with the existing federal regulations.

Part III challenges the claim that clarifying data ownership would improve access to useful data resources for clinical care, public health, and research. This claim was central to the recent debate between Professors Hall and Schulman and Professor Rodwin, who disagreed whether private or public ownership of patients' data would better promote data access. Data propertization proposals fail because patients' raw health information is not in itself a valuable data resource, in the sense of being able to support useful, new applications. Creating useful data resources requires significant inputs of human and infrastructure services, and owning data is fruitless unless there is a way to acquire the necessary services. . . .

Despite this progress, important problems remain unresolved. A major challenge in twenty-first century privacy law and research ethics will be to come to terms with the inherently collective nature of knowledge generation in a world where large-scale informational research is set to play

---

[32] *See* Abraham Bell & Gideon Parchomovsky, *Pliability Rules*, 101 Mich. L. Rev. 1 (2002). The important feature of pliability rule protection, for purposes of this discussion, is that it offers a dynamic scheme of entitlements in which a baseline rule of consensual ordering of data access can shift to nonconsensual access under specified circumstances. *See id.* at 5 ("Pliability, or pliable, rules are contingent rules that provide an entitlement owner with property rule or liability rule protection as long as some specified condition obtains; however, once the relevant condition changes, a different rule protects the entitlement -- either liability or property, as the circumstances dictate. Pliability rules, in other words, are dynamic rules, while property and liability rules are static.").

a more prominent role. Informational research differs starkly from interventional research, exemplified by randomized, controlled clinical trials, which were the major workhorse of late twentieth-century biomedical discovery. A person's refusal to participate in a clinical trial does not jeopardize the broader clinical research enterprise, which can move forward using other willing research subjects; only 600–3000 people are needed for a typical clinical drug trial. In contrast, a person's refusal to participate in informational research may bias the dataset and reduce its statistical power for everyone. Many important types of informational research must be done collectively with large, inclusive datasets. An individual's wish not to participate, perhaps motivated by privacy concerns, potentially places other human beings at risk and undermines broader public interests — for example, in public health or medical discovery — in which the individual shares. Existing regulations lack tools to resolve this complex dilemma. . . .

II. WHY DATA OWNERSHIP WOULD NOT PROTECT PATIENTS' PRIVACY

A. Nonconsensual Access to Patient Data Under a Property Regime

Data propertization proposals fall into two broad categories: pro-privacy proposals that portray private ownership as a way to bolster patients' power to block unwanted uses of their data and pro-access proposals that aim to promote wider availability of data for clinical, research, and public health uses. The pro-privacy proposals rest on a mythical view of private property. Three centuries ago, Sir William Blackstone noted how the human imagination is drawn to the idea of property as "that sole and despotic dominion which one man claims and exercises over external things of the world in total exclusion of the right of any other individual in the universe." This idea resonates with the "autonomy über alles" strand of privacy advocacy that asserts that a patient's right to control access to health data should trump all other interests, even society's interest in conducting studies that might save or improve other people's lives. Blackstone, however, was merely describing how people imagine property. He himself did not espouse this view, nor has American law ever done so.

Different assets call for different forms of ownership, and proponents of patient data ownership do not always specify what they have in mind. Data ownership might, for example, need to look something like the nonexclusive rights riparian owners have in a river that runs by their land — a right to use the river oneself but not to interfere with others' simultaneous uses for fishing and navigation — or like a copyright, which expires after a fixed term of years and allows fair use by others even during that term. Pro-privacy proposals seem to draw on the ideal of property reflected in the saying, "one's home is one's castle." In the usual course of events, access to a person's home requires a consensual transaction with the owner, and unconsented uses can be enjoined. This package of rights and remedies corresponds to property-rule protection, and it is what privacy proponents seem to be seeking in their calls for data ownership: consensual ordering of data access and the power to stop unconsented uses.

The fatal flaw in pro-privacy proposals is this: having a property right does not ensure property-rule protection. Law recognizes that there are many situations where consensual transactions cannot be relied on as a way of ordering an owner's relations with the larger community. In many circumstances, a property owner only receives liability-rule protection, which means the owner can be forced to give up her property in return for compensation that is externally set, often by a court, legislature, or administrative agency. That compensation may be zero. The government —

when acting under its police power to protect the public's health, safety, morals, or welfare — has broad power to confiscate or interfere with property without compensating the owner. Dating back to colonial times, the state's police power has been used not just to prevent property owners from injuring others, but also to pursue broader public welfare objectives for the benefit of the community. "[T]here was no single paradigm of public welfare that confined what we now call the police power. Then, as now, lawmakers pursued a shifting amalgam of goals . . . . Legislation coercively promoted uses of private land that were viewed as conducive to the community's well-being." Consistent with this tradition, the government can require nonconsensual access to data for use in public health activities, which long have been viewed as a legitimate exercise of the state's police power. This would remain true even if data were patient-owned.

The state also has eminent domain power to take property for "public use" without the owner's consent, subject to payment of just compensation. The public uses that can support a taking are quite broad and could include private, commercial research uses of data, if data were patient-owned. Takings require "some showing of 'publicness"' of the intended use, and takings that lack the requisite public quality can be enjoined. Public uses traditionally involved placing the property under public ownership or transferring it to a private company, such as a utility or railroad, that is obligated to serve the public, often but not always for a regulated price. There was never a requirement that the fruits of a taking be made *freely* available to the public: railroads and stadiums built on taken land routinely require users to buy tickets. Modern courts, somewhat controversially, allow takings that transfer property to new private owners for commercial projects that need not be open to the general public and for projects that offer only indirect public benefits, such as boosting local tax revenues or aiding urban renewal or land reform.

The possibility of eminent domain appears to have been lost on privacy advocates who view data ownership as a way to halt unconsented, private-sector research use of data. Modern takings doctrine would allow privately owned health data to be taken for use in academic and commercial research that offers a prospect of developing a beneficial therapy. This is true even if the new therapy, when successfully developed, would be available only to patients who can pay for it. It seems doubtful that patients would be entitled to compensation when their data were taken for use in research. Courts construe "just compensation" to mean payment of market value — what the property would fetch in an alternative, consensual sale on the open market. There is no compensation for subjective value, such as the emotional attachment an owner has to a particular home, or for undeveloped use rights — what the undeveloped property might have been worth if the current owner had chosen to develop it. There also is no compensation for consequential costs of the taking, such as an owner's moving expenses. These same limitations presumably would apply if patient-owned data were taken for public use in research. When patients wish to have their data "lie fallow" because of privacy concerns, the fair market value of the data arguably is zero: if patients oppose having their data used in research at all, there is no alternative consensual use by which to gauge the data's market value. The value of unused data is largely subjective, reflecting an emotional attachment to the data and a wish to keep it secret. This is not compensable under modern takings doctrine.

B. Nonconsensual Data Access Under the Existing Federal Regulations

The HIPAA Privacy Rule and the Common Rule offer a framework of patient entitlements and protections that is strikingly similar to what patients would enjoy if they owned their data. Under

ordinary circumstances, both regulations require consensual ordering of data access: they require a privacy authorization or informed consent before data can be used. However, both regulations contain exemptions, exceptions, and definitional nuances that shift to a regime of liability-rule protection under certain circumstances. . . .

Under the current regulations, certain activities that are considered to have high social value — such as using data for judicial, law enforcement, and public health purposes — are not subject to the usual consent and authorization requirements. Nonconsensual research use of data is allowed under conditions aimed at reducing privacy risks to the data subjects. Such use is allowed if the data have been deidentified, coded in compliance with specified standards, or converted to a limited data set. Nonconsensual research uses are also allowed if an Institutional Review Board or privacy board (collectively, "IRB") approves a waiver of the usual consent or authorization requirements. Data supplied to researchers under a HIPAA waiver must meet "minimum necessary" requirements — i.e., no more information can be disclosed than is necessary to accomplish the intended research purpose. However, there is no requirement that the data be de-identified or even coded to qualify for a waiver. In theory, it is possible to disclose fully identified data under a waiver, if the research requires the use of identified data and if an IRB deems the other waiver conditions to be met.

While some people object to any nonconsensual use of their data, there is fairly solid public support for police power uses of data — such as monitoring the spread of epidemics — that protect public health, safety, and welfare. The public also has some degree of comfort with the use of de-identified and other "masked" forms of data despite ongoing concerns about the potential for such data to be reidentified. Waivers do not inspire similar levels of public understanding. They are subject to ongoing critique from research institutions and IRBs that find the waiver provisions cumbersome to apply and from scholars and privacy advocates who view them as an abuse-prone bypass to consent requirements. . . .

Report to the President—Big Data and Privacy: A Technological Perspective

President's Council of Advisors on Science and Technology, May 1, 2014.

4.4.1 Anonymization or de-identification

Long used in health-care research and other research areas involving human subjects, anonymization (also termed de-identification) applies when the data, standing alone and without an association to a specific person, do not violate privacy norms. For example, you may not mind if your medical record is used in research as long as you are identified only as Patient X and your actual name and patient identifier are stripped from that record. Anonymization of a data record might seem easy to implement. Unfortunately, it is increasingly easy to defeat anonymization by the very techniques that are being developed for many legitimate applications of big data. In general, as the size and diversity of available data grows, the likelihood of being able to re-identify individuals (that is, re-associate their records with their names) grows substantially. One

compelling example comes from Sweeney, Abu, and Winn.[120] They showed in a recent paper that, by fusing public, Personal Genome Project profiles containing zip code, birthdate, and gender with public voter rolls, and mining for names hidden in attached documents, 84-97 percent of the profiles for which names were provided were correctly identified. Anonymization remains somewhat useful as an added safeguard, but it is not robust against near-term future reidentification methods. PCAST does not see it as being a useful basis for policy. Unfortunately, anonymization is already rooted in the law, sometimes giving a false expectation of privacy where data lacking certain identifiers are deemed not to be personally identifiable information and therefore not covered by such laws as the Family Educational Rights and Privacy Act (FERPA).

"President Weighs in on Data from Genes"

By Julie Hirschfield Davis
New York Times, Feb. 25, 2016

President Obama on Thursday waded into the complex and high-stakes debate over whether patients own their genetic information, saying that he believes that his tissues and any discoveries that stem from his DNA belong to him.

"I would like to think that if somebody does a test on me or my genes, that that's mine, but that's not always how we define these issues," Mr. Obama said during a White House forum on a major biomedical research initiative he began last year.

The president said that the success of his Precision Medicine Initiative, which aims to collect genetic data on one million American volunteers so scientists can develop drugs and treatments tailored to individual patients, hinged at least in part on "understanding who owns the data."

Many researchers and the universities and medical centers that back them regard genetic material and the results from tests they conduct on it as their intellectual property and are reluctant to share it. But consumer groups and some health advocacy organizations believe that individuals are the rightful owners of the data and the discoveries that emanate from them.

Advances in genetics and cell biology and the use of electronic medical records have paved the way for more sophisticated research into genes that may increase the risk of developing certain diseases. The debate over such research has broad implications for privacy and the success of precision medicine efforts, which depend on access to troves of genetic data.

Mr. Obama's comments on Thursday seemed to place him in the camp of individual patients.

---

[120] Sweeney, et al., "Identifying Participants in the Personal Genome Project by Name," *Harvard University Data Privacy Lab*. White Paper 1021-1, April 24, 2013. http://dataprivacylab.org/projects/pgp/.

"Right now, what happens is the best researchers and the best universities, oftentimes they're kind of hoarding their samples," Mr. Obama said, essentially for fear of losing their grants if they do not keep control of them.

The president's remarks elated some health advocates who have long argued that participants in genetic testing should be partners in the research that their cells enable.

"I had chills and a few tears, because I had not heard this before from the president or anyone high-up at the White House," said Sharon F. Terry, the chief executive of the Genetic Alliance, who was in the auditorium, across from the White House, as Mr. Obama spoke.

"The Precision Medicine Initiative has been trying to shift the conversation toward the idea that participants should be partners," Ms. Terry said. "But this is a really, really hard issue."

The Obama administration has been working to address it. On Thursday, the Department of Health and Human Services issued new guidance to clarify that patients should have access to their medical records, including genomic testing results.

Dr. Francis S. Collins, the director of the National Institutes of Health, has said participants in the Precision Medicine Initiative should be treated as "partners in research, not subjects." The program's principles include finding "innovative, responsible and consumer-friendly ways of sharing research data with participants."

The N.I.H. announced on Thursday that Vanderbilt University would team with Verily, formerly known as Google Life Sciences, to begin building the group of one million American volunteers who will participate in the individualized medicine effort.

Mr. Obama signed legislation in December providing about $200 million for the program.

The President Says Patients Should Own Their Genetic Data. He's Wrong

By Jorge Contreras
34 Nature Biotechnology 585 (2016)

As reported by the *New York Times*, US President Obama recently told a gathering of scientists, policymakers and patient advocates that individuals should own the data that comes from studying their DNA. He observed that "if somebody does a test on me or my genes . . . that's mine." Although, at first blush, the idea that we should own our data has an intuitive appeal, it contradicts a century of US legal precedent and, if put into effect, could have serious ramifications for biomedical research.

The President's comments were made during a White House briefing on the Precision Medicine Initiative (PMI), an ambitious new federal program that will fund the analysis of DNA from more than a million American volunteers. If the PMI gets off the ground, it will be the largest study of its kind ever conducted, and it could revolutionize our understanding of human disease and physiology.

To achieve its goals, the PMI will need to overcome significant fiscal, scientific and data-management hurdles. But perhaps the greatest challenge for this and other population-wide genetic studies will be persuading large numbers of individuals to contribute their DNA to the cause. Unlike drug trials and other experimental medical procedures, the cheek swabs and other minimally invasive techniques used to collect this DNA present no physical risk or harm. Nevertheless, there is a general public unease surrounding research using human DNA.

Some of this unease may arise from accounts of past research abuses, including the notorious Tuskegee syphilis experiments and the commercial exploitation of a poor black patient's cells, as recounted in Rebecca Skloot's *The Immortal Life of Henrietta Lacks*. Stories like these have made it clear that the public will need to be engaged in the research enterprise if large-scale research projects like PMI are to succeed.

But claiming that individuals 'own' the data derived from their DNA is not the right way to achieve this goal. Information cannot be 'owned' in the same way as land, tangible goods or even intangibles like money and securities. Pure data, once known, is, as Justice Louis Brandeis wrote nearly a century ago, as "free as the air to common use".

Since then, US courts have repeatedly denied individuals' ownership claims over data derived from their cells and tissue. Just imagine the chaos that would ensue if each of the million participants in the PMI could claim ownership over discoveries that were made after large pools of DNA were analyzed. If a drug or a vaccine were developed years after the study ended, should that person be entitled to compensation? Should everyone whose DNA was analyzed? What if one person's DNA were simply part of a control group, or of a trial that yielded no meaningful results? As one federal court cautioned, in *Greenberg* v. *Miami Childrens' Hospital*, the recognition of personal property rights in such data "would cripple medical research".

Yet the temptation to give individuals such ownership rights is strong. Several states have already passed legislation granting individuals ownership of the data derived from their DNA. And several recent lawsuits have objected to research based on claims seeking property-like control over genetic data. Among these was a 2009 Texas suit seeking to prevent the use of stored infant blood spots for a range of public health purposes[5]. To settle that suit, the state of Texas agreed to destroy over 5 million existing blood samples, resulting in the loss of an irreplaceable research resource.

In another highly publicized case, members of the Havasupai Indian tribe sued Arizona State University (ASU; Phoenix, AZ) for $50 million, arguing that DNA samples allegedly collected to investigate diabetes were impermissibly being used to investigate other things, such as schizophrenia and human migratory patterns[6]. To settle the case, ASU agreed to discontinue the research and return all samples, even though broad consent forms had been signed by the individual donors.

Admittedly, individuals have legitimate concerns regarding how their donated DNA will be used. But giving them ownership of the resulting data is not the best way to address those concerns, nor

---

[5] *Beleno v. Lakey*, Order, Civ. Action No. SA-09-CA-188-FB (W.D. Tex. 17 September 2009).

[6] *Havasupai Tribe v. Ariz. Bd. of Regents*, 220 Ariz. 214, 217 (2008).

is the complex set of exceptions and exclusions currently proposed in an amended version of the federal Common Rule[7]. Instead, federal and state legislation should be enacted to prevent the types of research abuses that have occurred in the past. In 2008, the US Congress took a first step when it passed the Genetic Information Nondiscrimination Act (GINA) to outlaw discrimination by health insurers and employers on the basis of genetic information. That legislation could be expanded to cover more: life and disability insurance, education, loan applications and so on.

Other rules could be put in place to ensure that an individual's health information will not be used for direct marketing purposes and that anonymized data will not be 'reverse engineered' to identify specific individuals. And existing federal research regulations, such as the Common Rule and HIPAA Privacy Rule, which today cover mostly government-funded research, could be expanded to cover private sector initiatives as well.

If large-scale genetic research studies like the PMI are to succeed, the US Administration should think carefully about the best way to achieve its goals. Ample legal measures are available to protect the public from research abuses, but giving individuals ownership of research data is not one of them.

Oregon Senate Bill 703

Whereas the Health Insurance Portability and Accountability Act of 1996 (HIPAA) protects the privacy and security of the protected health information of an individual and affords the individual the right to access, amend and obtain an accounting of disclosures of the individual's protected health information; and

Whereas HIPAA balances these protections and individual rights with the need to avoid the creation of unnecessary barriers to the access of quality health care; and

Whereas, notwithstanding individuals' expectations that protected health information will be used and disclosed as necessary to treat them, to bill for treatment and, to some extent, to operate a covered entity's health care business, protected health information is often used for purposes unrelated to treatment, payment or health care operations of the covered entity; and

Whereas companies that provide services on behalf of covered entities that give them and their contractors access to protected health information, routinely de-identify individuals' protected health information in order to sell the information in de-identified form to third parties for remuneration; and

Whereas after protected health information has been de-identified, it is no longer protected by or subject to HIPAA; however, the de-identification process itself is a use of protected health information that may only be performed under limited circumstances and for limited purposes under HIPAA; and

---

[7] US Department of Homeland Security et al. *Fed. Reg.* 80, 53933 (8 September 2015).

Whereas an individual may authorize a use or disclosure of the individual's protected health information that is not otherwise permitted by HIPAA, such as for the de-identification of protected health information for the purpose of commercial sale; and

Whereas the individual who authorizes the de-identification of the individual's protected health information for the purpose of commercial sale should have the right to assert a property interest in the health information such that the individual may receive remuneration in connection with the commercial sale; now, therefore,

Be It Enacted by the People of the State of Oregon: . . .

SECTION 2. (1) A covered entity, business associate, subcontractor or other third party doing business in this state may not engage in the commercial sale of protected health information, health information or de-identified data without first obtaining a signed authorization from the individual.

(2) A covered entity, business associate, subcontractor or other third party doing business in this state may not discriminate against or penalize an individual who declines to sign an authorization or who elects to receive remuneration in exchange for signing an authorization.

(3) A covered entity, business associate, subcontractor or other third party shall provide a share of any remuneration received by the covered entity, business associate, subcontractor or other third party to an individual who elects to receive remuneration in exchange for signing an authorization.

(4) A third party that has not obtained a signed authorization from the individual may not engage in the commercial sale of any protected health information, health information or de-identified data purchased or otherwise obtained from a covered entity, business associate or subcontractor without first documenting that a signed authorization has been obtained by the covered entity, business associate or subcontractor in accordance with subsection (1) of this section.

(5) This section does not apply to a public body, a federal agency or the business associates or subcontractors of a public body or federal agency with respect to health information created, received, transmitted or maintained by the business associate or subcontractor on behalf of the public body or federal agency.

(6) Violation of subsection (1), (2), (3) or (4) of this section is an unlawful practice under ORS 646.608.