Protecting Participants in Genomic Research: Understanding the "Web of Protections" Afforded by Federal and State Law

Leslie E. Wolf, Catherine M. Hammack, Erin Fuse Brown, Kathleen M. Brelsford, and Laura M. Beskow

Rapid scientific and technological advances have led to an explosion of research data.[1] Researchers now commonly collect biospecimens for genomic analysis; real-time lifestyle and behavioral data from mobile devices; and information from electronic health records, in addition to other participant-reported data.[2] This rich combination of data creates new opportunities for understanding and addressing important health issues, but also intensifies challenges to protecting research participants' privacy and confidentiality.[3]

Unlike the uniform protection of personal data provided by the European Union's General Data Protection Regulation, in the United States, legal protections depend on how data are generated, who holds the data, and which state's law applies.[4] While federal laws, such as the Common Rule,[5] the Privacy and Security Rules under the Health Insurance Portability and Accountability Act (HIPAA),[6] and the Genetic Information Nondiscrimination Act (GINA),[7] collectively impose some confidentiality obligations and limit some potential harms, they also have significant gaps that may or may not be filled by state law.[8]

To understand better how and to what extent existing laws protect research participants in large-scale genomic research, we conducted empirical research that included two separate components: (1) interviews with a diverse group of nationally-recognized thought leaders to explore their views of confidentiality-related topics at the forefront of genome research, and (2) structured legal research assessing research-specific and general federal and state laws that may protect research participants' interests. The primary results of these two endeavors are reported elsewhere.[9] Here, we integrate the findings and apply them to realistic research scenarios involving various privacy threats. By examining our legal findings alongside multidisciplinary expert perspectives, our goal is to illuminate

Leslie E. Wolf, J.D., M.P.H., *is a Distinguished University Professor and Professor of Law at Georgia State University College of Law in Atlanta, Georgia and Director of the GSU Center for Law, Health & Society.* **Catherine M. Hammack, J.D., M.A.**, *is an Associate in Health Policy and a member of the core faculty of the Center for Biomedical Ethics and Society at Vanderbilt University Medical Center in Nashville, Tennessee.* **Erin Fuse Brown, J.D., M.P.H.**, *is an Associate Professor of Law at the Georgia State University College of Law in Atlanta, Georgia.* **Kathleen M. Brelsford, M.A., Ph.D., M.P.H.**, *is a Research Assistant Professor in the Department of Health Policy and a member of the core faculty of the Center for Biomedical Ethics and Society at Vanderbilt University Medical Center in Nashville, Tennessee.* **Laura M. Beskow, M.P.H., Ph.D.** *is a Professor of Health Policy and the Anne Geddes Stahlman Chair in Medical Ethics in the Center for Biomedical Ethics & Society at the Vanderbilt University Medical Center in Nashville, Tennessee.*

The Journal of Law, Medicine & Ethics, 48 (2020): 126-141. © 2020 The Author(s)
DOI: 10.1177/1073110520917000

the effect of law in practice and to elucidate the actual strengths and limitations of the "web" of legal protections available to research participants. Accordingly, we do not provide a normative analysis, but rather describe what the "web" of legal protections *is*, not what it *should be*.

Our analysis starts in the context of a hypothetical national gene-environment interaction study that incorporates standard confidentiality protections and does not plan to return individual research results.

To understand better how and to what extent existing laws protect research participants in large-scale genomic research, we conducted empirical research that included two separate components: (1) interviews with a diverse group of nationally-recognized thought leaders to explore their views of confidentiality-related topics at the forefront of genome research, and (2) structured legal research assessing research-specific and general federal and state laws that may protect research participants' interests. The primary results of these two endeavors are reported elsewhere. Here, we integrate the findings and apply them to realistic research scenarios involving various privacy threats.

We describe the basic protections available for such a study (Scenario 1), including the Common Rule, HIPAA, and research project governance. We then consider the protections available if:

- Researchers return individual results (Scenario 2), including analysis of the Common Rule, HIPAA, and GINA;
- There is a database breach or hack (Scenario 3), including analysis of HIPAA, GINA, and research project governance; or
- There is a legal demand (such as a subpoena or court order) for data access (Scenario 4), including analysis of Certificates of Confidentiality and HIPAA.

In this paper, we focus on risks and protections for the individual research participant, as laws typically do. However, it is important to note that thought leaders interviewed also emphasized the risks to participants' biological relatives and to socially-identifiable groups.[10] Moreover, the likelihood of risks actually occurring and the severity of any resulting harm depends on numerous contextual factors, including characteristics of the individual participant, study design, and socio-cultural environment.[11]

METHODS

Detailed methodologic information is available elsewhere.[12] We describe the methods briefly below.

Qualitative Interviews

We conducted in-depth interviews (n=60) with a diverse group of prominent experts and scholars in the areas of ethics, genome research, health law, historically-disadvantaged populations, informatics, and participant-centric perspectives, as well as government officials and human subjects protections leaders (Table 1). We identified prospective participants based on leadership positions in prominent organizations, institutions, and studies across the U.S., as well as authorship of highly influential papers on relevant topics.

We developed a semi-structured interview guide centered around privacy and confidentiality issues and solutions in a hypothetical "Million American Study" (MAS) (Box 1). Although the MAS has similarities to the "All of Us" (AoU) Research Program now being conducted by the National Institutes of Health (NIH)[13], we did not design the MAS hypothetical to be identical to AoU. Interview topics included risks and potential benefits and harms; informed consent, including emerging models of dynamic and open consent; and the strengths and limitations of a range of general and specific approaches to protecting confidentiality.

Interviews were conducted by telephone between September 2015 and July 2016. Professional transcriptions of the audio recordings were uploaded into NVivo for coding and analysis using standard iterative processes.[14] The Vanderbilt University and Georgia State University IRBs deemed this research exempt.

The Journal of Law, Medicine & Ethics, 48 (2020): 126-141. © 2020 The Author(s)

Table 1
Participant Characteristics (n = 60)

	n	(%)
Perspective: *		
ELSI research	6	(10.0)
Ethics	7	(11.7)
Federal government	7	(11.7)
Genome research	7	(11.7)
Health law	6	(10.0)
Historically-disadvantaged populations	7	(11.7)
Human subjects protections	7	(11.7)
Informatics	6	(10.0)
Participant-centric approaches	7	(11.7)
Academic Degrees:		
MPH / MSPH	7	(11.7)
Other master's degree (e.g., MA, MS, MBA)	23	(38.3)
JD, LLB / LLM	18	(30.0)
PhD	35	(58.3)
MD	16	(26.7)
RN	2	(3.3)
Based in:		
United States	58	(96.7)
Other (Canada, UK)	2	(3.3)
Gender (self-reported):		
Female	31	(51.7)
Male	29	(48.3)
Race (self-reported):		
American Indian or Alaska Native	2	(3.3)
Asian	5	(8.3)
Black or African American	3	(5.0)
Native Hawaiian or Other Pacific Islander	1	(1.7)
White	49	(81.7)
Ethnicity (self-reported):		
Hispanic or Latino	2	(3.3)

* Primary perspective for which we identified thought leaders; many could easily have been recognized in two or more categories

Legal Analysis

We conducted searches in Westlaw and Lexis-Nexis to identify state laws that had provisions adding to the protections federal laws afford to participants in genomic research. These included laws that would apply to genetic information, tests, and biospecimens, as well as other health information used and held by researchers and biobanks. These also included laws protecting against unwanted use of genetic and other health information by employers, insurers, or "any person" if such information were to be disclosed, breached, hacked, or returned to the participant or their health care provider.

We used formal search strategies and the "book browse" feature to identify enacted statutes and promulgated regulations in effect between January 1, 2015, and December 31, 2017, the period of our research. We then worked in pairs to select all relevant laws across all 50 states and the District of Columbia. Pairs independently coded the selected laws using NVivo and following the codebook the team developed. Any interpretive questions were identified and discussed among the faculty members.

To integrate the findings from these two components of our research, we analyzed each of the research scenarios to determine which federal and state laws offer protections against the risks identified by the thought leaders, including identifying any gaps in legal protection.

SCENARIO 1: THE MILLION AMERICAN STUDY

For thought leaders, the long-term, open-ended nature of the MAS raised concerns beyond those typically associated with more limited or well-defined kinds of research.[15] In particular, they highlighted the risk that information could be used in ways the MAS permitted but were unanticipated and potentially objectionable to some participants because of the research topic, the researcher, or non-research use of the data (Table 2). The primary protections against these kinds of risks and harms include the Common Rule, the HIPAA Privacy Rule, and related state laws, plus research governance features such as data access committees and data use agreements.

The Common Rule and Related Protections

The federal Common Rule aims to protect against some of the risks and harms of research participation, principally through IRB review and individual informed consent.[16] Nearly half of thought leaders found these requirements to be reassuring, primarily citing the Common Rule's commitment to respecting autonomy and privacy (even when it disadvantages research).[17]

The Journal of Law, Medicine & Ethics, 48 (2020): 126-141.

IRB Review

The Common Rule specifies IRB review criteria, including that risks are minimized and reasonable in relation to anticipated benefits, if any.[18] Many thought leaders, however, noted variability among IRBs and said the protection actually afforded depends on IRB quality. They further commented on IRBs' limited abilities to provide meaningful *ongoing* oversight throughout a long-term study.[19] Although the Common Rule often obligates IRBs to provide continuing review,[20] it would be unusual for an IRB to revisit a study's overall design unless a problem occurs.[21]

In addition to the concerns thought leaders raised, there are important gaps in the Common Rule's IRB review requirement. The Rule only applies to federally conducted or funded research.[22] Although the MAS is described as federally funded, secondary research using MAS data may not be.[23] For example, citizen scientists — members of the lay public who actively take part in planning and conducting research[24] — and other non-academic researchers may not be federally funded. In addition, some research by academic investigators may not be federally funded, though their institution may voluntarily apply the Common Rule.

Box 1

The Hypothetical "Million American Study"

The Million American Study (MAS) is a federally-funded, large-scale research endeavor to improve understanding of health and to find new ways to predict, detect, diagnose, treat, and prevent disease. Specifically, the aim is to compile comprehensive information from a cohort of one million Americans in a repository that will serve as a rich research resource for a wide variety of studies for decades to come.

MAS will seek to enroll a representative sample of U.S. adults reflecting diversity in terms of race and ethnicity, age, and sex. Those who agree to participate will give broad consent for:

- Extensive characterization (including whole genome sequencing) of biospecimens, such as blood
- Ongoing access to clinical data (such as medications, test results, and imaging) from electronic health records
- Real-time monitoring of lifestyle and behavioral information, such as physical activity and environmental exposures, through mobile health devices

At the time of consent, participants will be offered choices about whether they are willing to be re-contacted for various purposes (*e.g.,* to provide additional information or specimens). Participants will be able to withdraw consent for future use of their specimens and data, with the exception that data generated in past studies cannot be withdrawn, nor can specimens and data be withdrawn from studies already begun.

Specimens will be stored in coded form in a repository at a major academic medical center in one state, while the data will be held at the coordinating center in another state. A robust data security framework will be in place, including administrative, technical, and physical safeguards. There will be a centralized governance process, comprising participant representatives, researchers, health care providers, government officials, and other stakeholders to ensure overall accountability and responsible project management.

Multiple tiers of access to MAS data — from open to controlled — based on data type, data use, and user qualifications will be employed. For example, certain information, such as some aggregate results, will be publicly available. Access to other information will be available to qualified researchers from academic, non-profit, and for-profit entities, in the U.S. and around the world, through application to a Data Access Committee. For approved projects, Data Use Agreements will be used to ensure that data and specimens are used and shared for authorized purposes only, and that privacy and security safeguards are maintained.

Information will be publicly available concerning how MAS cohort data and specimens are being used, including information about ongoing studies and summaries of research findings.

Adapted from F.S. Collins and H. Varmus, "A New Initiative on Precision Medicine," New England Journal of Medicine 372, no. 9 (2015): 793-795; M.J. Khoury and J.P. Evans, "A Public Health Perspective on a National Precision Medicine Cohort: Balancing Long-Term Knowledge Generation with Early Health Benefit," 313, no. 21 (2015): 2117-2118.

The Journal of Law, Medicine & Ethics, 48 (2020): 126-141. © 2020 The Author(s)

The Common Rule also contains several exceptions, the most relevant of which would be secondary research using coded biospecimens and/or data that were collected by the MAS, with no access to identifiers. Such research is not considered to involve human subjects because the Common Rule defines a "human subject" in terms of intervention or interaction with the person or identifiability.[25] In practice, many IRBs review study information to determine whether it meets the definition of "human subjects research," although the regulations do not require it.[26] We found only one state that has a genetic-specific law requiring at least limited IRB review for secondary research when the Common Rule does not.[27]

Informed Consent

Because the MAS involves interaction with participants and is described as prospectively collecting and retaining participants' identifiable biospecimens and private information, the MAS itself would not fall-within one of the Common Rule's exceptions[28] and would require informed consent from participants. This consent requirement provides an opportunity for individuals to be apprised of the procedures, risks, and benefits and to make a voluntary decision about whether to participate in research. Thus, individuals who are generally risk averse, concerned about a specific risk, or feel particularly susceptible to harm can protect themselves by declining to participate.

Nevertheless, this protection may be limited. Many thought leaders noted that the Common Rule's consent requirements can be technically fulfilled despite insufficiencies often found in consent forms (*e.g.*, complex language, excessive length). In other words, the protections provided depend on the quality of the consent materials and processes[29] — including the extent to which they effectively communicate the information identified as most important to prospective participants' decisionmaking.[30]

Moreover, in research endeavors like the MAS, participants consent broadly to their specimens and data being used in unspecified future research.[31] Accordingly, their consent to each specific future study is not required, as long as the description provided when they give consent includes sufficient detail such that reasonable people would expect they were permitting the types of research conducted.[32] Even if broad consent is not obtained, secondary research using only existing coded specimens/data, with no access to identifiers, is not considered "human subjects research" under the Common Rule. Thus, individual participants may not even be notified regarding when or how their materials are used.[33]

However, state laws may require informed consent when the Common Rule does not. A number of states require "any person" conducting genetic tests to obtain consent and define genetic testing broadly enough to apply to research.[34] Because some of these laws refer to *specific* consent, consent to unspecified future research may not be sufficient. To the extent these laws are enforced (several explicitly include a private right of action), participants in these states could theoretically avoid uses they find objectionable by having greater control over each use of their specimens and data.

A critical aspect of informed consent afforded by the Common Rule is disclosure of the right to withdraw.[35] However, as thought leaders noted, there are limits to this protection in endeavors like the MAS insofar as one's materials cannot be called back or removed once they have been shared with other researchers.[36] Some state laws explicitly require the withdrawal and/or

Table 2

Thought leader perspectives on the main risks/ harms of the MAS.

Unanticipated uses
• *Research uses* - Use for an objectionable research topic leads to dignitary or group harm. - Objection may be based on personal values/beliefs (e.g., research that violates commonly-held religious beliefs) or - Objection may be based on a sensitive or non-health-related topic (e.g., research on intelligence, criminality, substance abuse). - Use by an objectionable researcher leads to dignitary harm (e.g., researchers from commercial entities, the government). • *Non-research uses* - Use for commercial purposes leads to psychological harm (e.g., targeted marketing based on sensitive information).
Unknown risks and harms
• Shifting socio-political environments and swiftly evolving research landscape leads to uncertainties and the prospect of unknown risks and harms.
Dissemination
• Research findings may be reported, presented, and/or construed in ways that exacerbate existing stigma and/or health disparities regarding a socially-identifiable group. • Reported research findings by providers, institutions, or insurers may be used to make decisions to withhold or implement interventions/coverage.

The Journal of Law, Medicine & Ethics, 48 (2020): 126-141.

destruction of samples when an individual withdraws consent, with penalties for failure to comply.[37]

HIPAA Privacy Rule and Related Protections

The HIPAA Privacy Rule and similar state laws may give research participants additional control by limiting uses and disclosure of their identifiable health information without individual authorization. The HIPAA Privacy Rule generally prohibits covered entities or their business associates from using or disclosing identifiable health information without individual authorization. However, there are several exceptions allowing for disclosure without authorization, such as for law enforcement purposes, pursuant to a court order or subpoena, or to public health or other governmental authorities.[38] The HIPAA Privacy Rule includes genetic information in the definition of "health information."[39] HIPAA imposes certain obligations on covered entities and business associates, including breach notification, limits on marketing use or sale of protected health information, providing individuals a right of access to their own information, and maintaining the security of protected health information.[40]

The Privacy Rule requires each participant's authorization for the MAS to collect and use medical record data from his or her health care provider, a HIPAA-covered entity.[41] However, this authorization provides little protection against the risk that the participant's information could be used for objectionable research. Despite regulatory language that the authorization "must include a description of *each purpose* of the requested use or disclosure,"[42] agency guidance permits authorizations to unspecified future research if the description is "such that it would be reasonable for the individual to expect that his or her protected health information could be used or disclosed for such future research."[43] Because the requirement that an authorization contain an expiration date may be satisfied by stating "none" or "until authorization is revoked," such authorization can be indefinite.[44]

Most thought leaders were not particularly reassured by the Privacy Rule's protections in the context of the MAS.[45] Although some highlighted the acute awareness and expectations surrounding HIPAA among researchers and institutions, others questioned whether the Privacy Rule would apply to the MAS and its research sites.

Indeed, HIPAA only applies to "covered entities" — primarily health care providers — and their "business associates" that handle identifiable health information.[46] Some academic medical centers may elect to extend covered-entity status to their research activities (including biobanks, data coordination centers, and research sites), while others may not. In large-scale endeavors like the MAS, some research sites may not be covered entities at all.[47] The applicability of HIPAA depends on the entity's status and does not "follow the data" (Figure 1). Thus, as MAS specimens and data are transferred to and from a centralized research laboratory (*e.g.*, for genomic analyses) and to downstream researchers, HIPAA protections would only apply if the particular entity handling the materials is a covered entity or business associate. In contrast, we found a number of states that prohibit *any person* who holds genetic information, personal data, or medical data — which could include researchers — from disclosing the information without individual consent.[48]

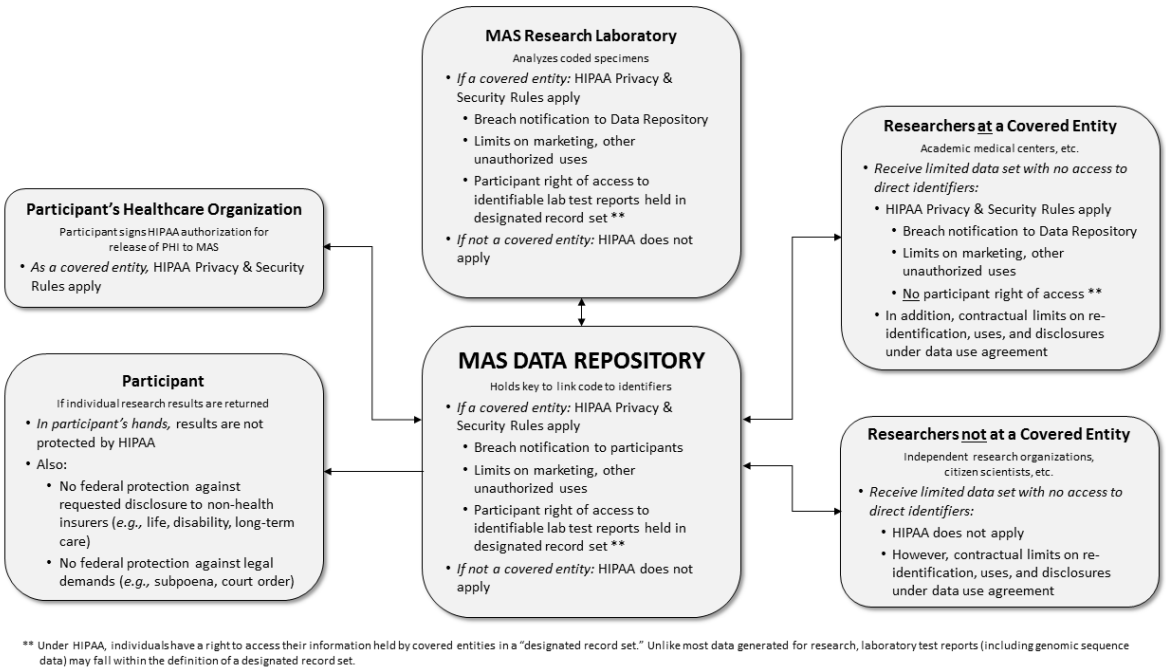
For HIPAA-covered entities, the Privacy Rule's requirements establish strong standards and deterrents against unauthorized use and disclosure and may serve as an industry standard for non-covered entities. Some thought leaders were reassured by the Privacy Rule's high standards for de-identification, although many noted these standards are not infallible and that re-identification is possible.[49] Moreover, much of the MAS data used by researchers would be identifiable, even if in a limited dataset. A limited dataset excludes direct identifiers but, given the richness of data collected and generated by endeavors like the MAS (including genomic data), it may contain information that could be used in combination to identify individuals. Although limited datasets are not considered de-identified under the Privacy Rule, they may be used without authorization for research purposes pursuant to a data use agreement that contractually obligates the recipient to safeguard the data, refrain from re-identification or further disclosure except as provided by the agreement, and notify the covered entity of uses or disclosures not permitted by the agreement.[50]

The HIPAA Privacy Rule does, however, require an individual's authorization for uses or disclosures of their identifiable information for marketing, ameliorating some risks thought leaders raised regarding unwanted non-research uses (Table 2).[51] Non-covered entities that receive MAS data would not be bound by the Privacy Rule's proscriptions on uses or disclosures of the participant's data, but may be contractually bound to similar limitations under a data use agreement (Figure 1).

While some thought leaders referenced HIPAA's penalties as a potential deterrent against intentional or reckless violations, others noted the prominent role of human error, particularly when many people have access to the data.[52] Reported HIPAA breaches support this concern, evidencing both inadvertent breaches by people with authorized access as well as attacks by people without authorized access.[53] If data

The Journal of Law, Medicine & Ethics, 48 (2020): 126-141.

Figure 1
HIPAA in the hypothetical "Million American Study."



** Under HIPAA, individuals have a right to access their information held by covered entities in a "designated record set." Unlike most data generated for research, laboratory test reports (including genomic sequence data) may fall within the definition of a designated record set.

are disclosed to entities that are not HIPAA-covered, HIPAA's protections do not apply.

A further limit on the Privacy Rule's protections is that it does not offer a private right of action to individuals whose information is disclosed without authorization.[54] Aggrieved individuals' only recourse under HIPAA is to file a complaint with the Office for Civil Rights to conduct an investigation. Although this may result in corrective action or administrative penalties against the covered entity or business associate, it will not compensate the individual.

Research Project Governance

In addition to statutory and regulatory limits on data access, research platforms like the MAS often adopt rules and procedures to govern access to data and specimens, as well as to protect against misuse. This kind of research project governance, including data access committees and data use agreements, has a crucial role to play because participants who give broad consent are, in essence, entrusting decisions about and oversight of secondary research to these entities and processes.[55] As described in Box 1, researchers would apply to use MAS specimens/data. If approved by a data access committee, the MAS would provide a limited dataset under a data use agreement. This agreement would give contractual protections against re-identification, disclosure, or misuse of participant data, whether or not the recipient of the dataset is a covered entity (Figure 1).

Thought leaders generally perceived data access committees and data use agreements as either weak,or helpful but insufficient.[56] They highlighted several limitations that echo concerns they expressed about HIPAA,[57] including reliance on human behavior; barriers to monitoring, enforcement, and pursuing penalties; reactiveness (rather than prevention); and limitations associated with delegated decision making (*i.e.*, entities making decisions about data access and use on behalf of research participants). Protections provided by data access committees and data use agreements rely on the integrity and commitments of the individuals involved.

Given the important role of research project governance in protecting participants and maintaining trust in the research enterprise, empirical research is needed to address thought leaders' concerns and identify and strengthen best practices.

SCENARIO 2: RETURNING INDIVIDUAL RESEARCH RESULTS

If the MAS did *not* contemplate return of individual research results, thought leaders described the risks of participation as low. They believed that a decision to return results could provide direct health benefit for a small proportion of participants — but would increase

The Journal of Law, Medicine & Ethics, 48 (2020): 126-141.

the risks and potential harms for the majority (Table 3).[58] They suggested that if the MAS were seeking to minimize risks and potential harms, it should either not return individual results or, alternatively, limit return to results that are clinically-actionable.[59] They also discussed return of results as the mechanism by which information could eventually be used outside participants' control in ways that might be unanticipated and/or unwanted.[60]

The primary protections against these kinds of risks and harms include the Common Rule, the HIPAA Privacy Rule, and GINA, as well as related state laws and research project governance.

The Common Rule and Related Protections

The Common Rule, when it applies, requires researchers to disclose *whether* clinically relevant results will be returned.[61] Presumably, the impact of returning results and plans for doing so would be incorporated into the IRB's assessment of risks when reviewing a project like the MAS.

Given their perceptions of risk, it is unsurprising that many thought leaders addressed the importance of not simply notifying participants, but providing them with the opportunity to decide whether or not they want to receive results.[62] Thus, during the consent process, participants who had concerns could decline to receive results or decline participation altogether.

Whether the potentially adverse consequences of receiving unwanted/unexpected results are in fact minimized depends on the quality of the IRB oversight and consent process. For example, some thought leaders foresaw participants saying "yes" without understanding that decision, or receiving results due to a perceived or actual duty on the part of the MAS to inform despite the participant saying "no."[63] To mitigate this concern, some suggested the MAS should establish a governance process to determine what types of results would be returned and detailed procedures for disclosure (*e.g.*, providing consultation, education, referral).[64]

The HIPAA Privacy Rule and Related Protections

The HIPAA Privacy Rule provides individuals a right to access their own information held by covered entities in a "designated record set," which may allow participants to access their genomic results, regardless of the approved research protocol.[65] Unlike most data generated for research,[66] the 2014 amendments to CLIA and HIPAA Privacy Rules provide that laboratory test reports (including genomic sequence data) may fall within the definition of "designated record set." If the research laboratory that conducts genome sequencing for the MAS were a HIPAA-covered entity, it would have to comply with the HIPAA right of access and provide the participant with his or her identifiable genomic data upon request (Figure 1).[67] Typically, the research laboratory would work with coded specimens, so in practice, the requested access would be provided by the MAS data repository, which holds the key to link the coded test reports to the individual's identity. In other words, even if the MAS did not plan to return of results as part of its design, allowing participants to access to their genomic data may be required if the research laboratory used is a covered entity under HIPAA.[68]

In addition to HIPAA's access rights, a limited number of states create rights to access genetic information that could be used to override researchers' decisions about whether and what kinds of results to return.[69] For example, one state's law explicitly applies to research participants and grants them the right to access their genetic information.[70] Several other states broadly grant individuals the right to access their genetic information.[71] Some have created "property

Table 3

Thought leader perspectives on the main risks/ harms if MAS returns individual research results.

There are risks and potential harms even if results remain within a participant's self-defined sphere of personal privacy (including their own medical care), each of which may be magnified by results of uncertain or no clinical utility as well as by other issues associated with unknowns of genetic information:

- Results may contain unwanted or unexpected information leading to psychological harm to the participant and their biological relatives (e.g., future health status, parentage, self-/group-identity).
- Participants may not understand the results or have access to resources to confirm or act upon them.
- Participants may take unwarranted medical action based on results, and providers (e.g., physicians, insurers) may make premature or erroneous treatment/coverage decisions, leading to physical and/or economic harm.

Additional risks and potential harms arise if results leave a participant's self-defined sphere of personal privacy via required, voluntary, or unintended disclosure:

- Current or potential employers (< 15 employees); life, disability, or long-term care insurers; or other entities may use results, leading to economic harm.
- Participants may voluntarily share results which may be further shared by others (e.g., social media) and/or leave data vulnerable to unintended disclosure through inadequate security on devices or the internet.

The Journal of Law, Medicine & Ethics, 48 (2020): 126-141. © 2020 The Author(s)

rights" in DNA, although many of these do not make clear whether this includes the right to access genomic research results.[72]

Genetic Information Nondiscrimination Act

Thought leaders also discussed several risks and possible harms arising from subsequent disclosures of research results that have been returned, including discrimination in employment and insurance (Table 3).[73]

With respect to employment, GINA only prohibits large employers (≥15 employees) from requesting, requiring, or using genetic information for employment decisions, which leaves approximately 15% of all U.S. workers unprotected.[74] In contrast, six state genetic discrimination laws apply to employers with five or fewer employees and eleven apply to those with only one employee.[75] An individual can sue for employment discrimination under GINA after exhausting administrative remedies, but recovery is limited based on employer size.[76] Some states have adopted provisions, such as treble damages, statutory minimum damages, and attorneys' fees and costs, which can facilitate pursuit of a claim.[77] Other states explicitly authorize aggrieved individuals to bring a lawsuit, without damage limits.

In addition, under GINA, health insurers cannot deny coverage or charge different premiums on the basis of genetic information.[78] The Affordable Care Act (ACA) greatly expanded these protections by prohibiting health insurers from charging more or denying coverage based on pre-existing conditions or other health status factors.[79] The ACA does not, however, provide a private right of action to enforce these health insurance rules, which are largely left to government enforcement.[80] A few thought leaders cautioned against long-term reliance on the ACA's protections against discrimination in health insurance in the current political climate, and many of these concerns persist as ACA opponents attempt to repeal or roll back its protections.[81]

Thought leaders also discussed that returning research results opens up the individual to having to disclose genetic and other health information to life, disability, and long-term care insurers, for which GINA offers no protection (Table 3). One of GINA's known gaps is that it does not prevent life, disability, or long-term care insurers from making coverage or premium decisions based on genetic information. If these insurers ask about genetic test results, participants that have received their research results would be required to disclose them.

Unlike GINA, some states prohibit use of genetic information in underwriting in long-term care insurance, disability insurance, and life insurance.[82] Some of these restrict use of genetic information in underwriting unless it is "based on sound actuarial principles or actual or reasonably anticipated claims experience."[83] As many research results will not have been validated and have uncertain clinical implications, these laws *may* limit long-term care, disability, and life insurers from using such information. Several states create broader protections against unwanted access to and uses of genetic information by *any* person, not just employers or insurers. For example, several states have criminal laws that penalize acquiring medical information (which is defined broadly enough to include genetic information) without authorization.[84] These laws may provide a mechanism for redress should the harm thought leaders identified be realized.

Many thought leaders were reassured by GINA; although they acknowledged gaps in protection, some perceived the risk of genetic discrimination in health insurance coverage as low and/or mostly theoretical.[85] Those who were less reassured pointed to the gaps as well as enforcement challenges, given the difficulty of people knowing — much less proving — they have been discriminated against in employment or insurance decisions based on genetic information. These thought leaders variously described GINA as aspirational, misleading, or promoting genetic exceptionalism.[86]

SCENARIO 3: UNINTENDED RELEASE OF DATA WITH POTENTIAL FOR RE-IDENTIFICATION

Thought leaders considered unintended release of data that have potential for re-identification as an important risk of the MAS (Table 4).[87] Such releases can result from an internal failure (*i.e.,* a breach), such as a lost laptop, or from an external attack (*i.e.,* a hack). In either case, the concern is that the multifaceted richness of MAS data makes it susceptible to being re-identified and used in ways that harm participants. Thought leaders foresaw this risk growing over time, given advances in "big data" science and increases in the availability of data that would enable sophisticated triangulation.

The HIPAA Security Rule and Related Protections

The HIPAA Security Rule,[88] which prescribes technological, physical, and organizational requirements for maintaining the security of protected health information, serves as the primary legal tool for protecting against data breaches and hacks. Like the Privacy Rule, the Security Rule does not apply to a researcher or biobank that is not a covered entity or business associate and does not apply to non-electronic information (*e.g.,* biospecimens).[89] Nevertheless, the

The Journal of Law, Medicine & Ethics, 48 (2020): 126-141.

HIPAA Security Rule is seen as establishing an industry standard for securing sensitive electronic data that non-covered entities may follow to reduce the chance of unintended release.[90]

Thought leaders generally described technical data security measures, such as those required by the HIPAA Security Rule, as necessary but insufficient.[91] They noted several limitations, such as relying on humans to understand, implement, and enforce them and on mechanisms like audit trails that discover violations only after the fact.[92] Moreover, widespread data sharing, which is encouraged (and often required) for scientific purposes, increases the number of times data are transmitted, people who have legitimate access, and places data are stored — with correspondingly increased opportunities for unintended access and potential harm. The likelihood of harm depends on actors' motives, for example, criminal intent versus "white hat" researchers[93] (although participants may be concerned regardless of the actor), and the quality of technical security measures and oversight.[94]

Thought leaders did not address specific protective measures *after* a breach or hack, perhaps because they are limited. The HIPAA Privacy Rule requires covered entities to notify affected individuals of a breach and offers the possibility of administrative penalties against the covered entity or business associate who experienced the breach.[95] Some states have laws that allow individuals to sue for violation of their genetic privacy.[96] These provide a mechanism to seek relief from the entity from which data were released as well as any third party who misappropriates, rediscloses, or misuses genomic data — particularly when the laws also establish statutory minimum damages.[97] In addition, one state prohibits re-identification or attempts at re-identification of individuals based on their protected health information.[98] Another has an identity theft law that specifically includes genetic information that could provide a mechanism for redress.[99]

As noted in Scenario 2, GINA would prevent larger employers and health insurers from discriminating against an individual based on genetic information that had been released via a breach or hack, but it would offer no protection against genetic discrimination by other types of entities or insurers.

Research Project Governance

For researchers who receive data from platforms like the MAS, data use agreements may limit the risk of unintended release by setting standards of behavior. In the event of a breach, non-covered entity researchers would not be required to engage in breach notification under HIPAA, but could be contractually obligated to notify the MAS under the data use agreement (Figure 1).[100] Such agreements would be theoretically enforceable against researchers who sign them to receive MAS data — although thought leaders were skeptical whether and how enforcement would occur — and could also be used as evidence of standards of care.[101]

Table 4

Thought leader perspectives on the main risks/harms if MAS data were unintentionally released.

There are several risks and harms from breach, hack, and triangulation, the likelihood and severity of which may increase over time due to technological innovations (e.g., developing genomic technologies, identifiability of data): • Risk of economic harm from medical or regular identity theft or employment/insurance/other discrimination • Risk of psychological harm related to concerns about re-identification, disclosure, and misuse The likelihood and severity of risks/harms from unintended access also depend on a recipient's motivation to use it; researchers may attempt to re-identify data merely to evaluate identifiability of data or the strength of protections (particularly of genomic data), while malicious actors may have financial or other harmful motives.

SCENARIO 4: SUBPOENA, COURT ORDER, OR OTHER LEGAL DEMAND

Thought leaders anticipated government and law-enforcement interest in MAS data, leading to the potential for legal harm (*e.g.,* surveillance, criminal tracking, immigration, national security).[102] In particular, data amassed by the MAS — through collection of existing information (*e.g.,* from medical records) as well as generation of new information (*e.g.,* survey questions, genomic analysis) — could be the subject of a legal demand or a request from law enforcement (Table 5). The latter possibility has gained prominence since ancestry DNA databases were used to solve the "Golden State Killer" and other cold cases.[103] Although none of these cases involved a research databank, it is not difficult to imagine law enforcement requesting access to research data, especially as rich a resource as the MAS.

In addition to law enforcement, there may be other legal interest in data from endeavors like the MAS. Most legal demands for research data have occurred in civil matters, such as personal injury (including environmental exposures) or family law cases.[104] As described by thought leaders, access for these kinds of purposes could lead to consequences ranging from legal jeopardy to psychological distress (Table 5).[105]

The Journal of Law, Medicine & Ethics, 48 (2020): 126-141. © 2020 The Author(s)

Certificates of Confidentiality

Certificates of Confidentiality are congressionally authorized legal tools that provide protection against compelled disclosure of sensitive, identifiable research data "in any Federal, State, or local civil, criminal, administrative, legislative, or other proceeding."[106] Historically, researchers had to apply for this protection. Although the study did not have to be federally funded to receive a Certificate, issuance was discretionary and not guaranteed. As discussed in more detail below, the 21st Century Cures Act (enacted after our thought leader interviews were conducted) changed some of these provisions.[107]

Thought leaders described Certificates as an extra layer of protection but no guarantee against compelled disclosure, noting uncertainty about their legal effect.[108] They were especially uncertain of Certificates' protections in the context of multi-site research, including whether the protections apply to data once it is shared and whether all research sites would enforce the protections.

These concerns are partially supported by our previous research. The few written court opinions involving challenges to Certificates reveal mixed success in protecting identifiable research data. *People v. Newman* provides the strongest support for avoiding data disclosure in a scenario like the Golden State Killer; the *Newman* court refused to compel disclosure of patient photographs to identify a potential murderer because of the Certificate's protections.[109] However, other cases have allowed disclosure of research data, including a case involving a criminal defendant seeking data to dispute the prosecution's case and another arising in the context of child abuse and neglect.[110] This variation in outcomes may reflect judges' and attorneys' unfamiliarity with Certificates and the conflict between Certificates' protections and the typically liberal discovery rules in civil litigation and criminal defendants' Constitutional rights.[111]

The 21st Century Cures Act implemented several changes to the Certificate authorizing statute that address some of the thought leaders' concerns.[112] Issuance of a Certificate is now mandatory for federally-funded research, although it remains discretionary for non-federally funded research. Thus, NIH now automatically issues Certificates for research involving human subjects that it funds. Protections also now extend to all copies of the data in perpetuity, such as MAS data that are shared widely for research. The new provisions prohibit protected data from being admitted in evidence or otherwise used in any legal proceeding. However, due to automatic issuance, researchers who have not applied for a Certificate may be unaware of the protections and, thus, may not assert them when necessary.

The disclosure prohibition of the Certificate statute does not apply to disclosures required by federal, state, and local law. NIH discussed this provision in the context of compliance with mandatory public health reporting laws,[113] but this exception is not limited to these circumstances. Given the myriad of federal, state, and local laws, there are likely to be other required disclosures, such as to protect vulnerable populations, the environment, or public safety. Once data leaves the research realm in accordance with this exception, it is unlikely that the Certificate's protections — including the provisions about admissibility — apply.[114]

Table 5

Thought leader perspectives on risks/harms if there is a court order or other legal request for MAS data.

Legal demand
• MAS data may be used in criminal investigations or civil disputes (e.g., immigration, custody battles), the legal implications of which could be serious and the consequences severe for participants as well as their biological relatives. A Certificate can protect against such legal demands, but relies on researchers as well as courts to understand, assert, and uphold its protections.
Legal requirement
• MAS data may be disclosed to government or public health authorities for mandatory public health reporting, government audits, or in accordance with other legal requirements, potentially causing embarrassment and/or familial disruption, particularly if sensitive information is released.

HIPAA Privacy Rule and Related Protections

For research that, unlike the MAS, does not have a Certificate, the next level of protection — provided by the HIPAA Privacy Rule and state privacy laws — is thin.[115] These laws generally allow disclosure to law enforcement to help identify a suspect or in response to a legal demand, without an individual's authorization.[116] Although such laws do not *require* disclosure, it is not difficult to imagine that, absent another legal obligation (*e.g.*, a Certificate), researchers would want to disclose information that could help identify a notorious murderer like the Golden State Killer. HIPAA permits disclosure of limited information to help identify a suspect without an individual's authorization or a legal demand.[117] Under certain circumstances, it also allows covered entities to disclose protected health information in response to a civil legal demand for information, such as in a family law

The Journal of Law, Medicine & Ethics, 48 (2020): 126-141.

or a workplace injury case, without an individual's authorization.[118]

CONCLUSION

Our analysis of the "web" of protections created by federal and state laws shows that there are areas of strength — particularly where federal protections are further reinforced by state laws — but also gaps where neither federal nor (most) state law protect. Accordingly, researchers and IRBs need to be aware of those protections and gaps to be able to determine the impact of research design on the risks a study presents, as well as what information ought to be conveyed to participants during the consent process. Their task is complicated because there is uncertainty about which state laws apply in the context of national endeavors like the hypothetical MAS, where participants, researchers, and data may be located in different states that potentially afford substantively different protections and fill in gaps in the federal protections.[119] Clearly and accurately conveying the information participants need or want to know so as not to provide false reassurance is challenging.[120]

The thought leaders we interviewed were generally well aware of the protections federal laws provide and the limitations of those laws. They rarely addressed state laws, but this may reflect the primary focus of our interview guide on federal law. Additional research is needed to identify the extent to which stakeholders are aware of state laws and how they are implemented in practice, as well as the ways that stakeholders are anticipating, addressing, and resolving choice of law questions that arise in research settings. Such research could help others navigate these complex issues, as well as provide insights into crafting consent forms that take into account differences in state law.

Regardless of the apparent strength of the protections afforded by law, such protections ultimately depend on humans to understand, implement, obey, and enforce them. Thought leaders frequently commented on this reliance as the weak link. Additional research may be required to eludicate how well individuals with access to research data understand their legal obligations to protect it and how best to enforce those laws to maximize compliance. There may be educational, technological, oversight, governance, or other mechanisms to make fulfilling and enforcing these obligations easier, potentially decreasing the reliance on individuals and increasing consistency. Efforts to identify and implement effective measures and best practices are necessary to realizing the full scope of protections the laws are intended to provide.

Our analysis of the "web" of protections created by federal and state laws shows that there are areas of strength — particularly where federal protections are further reinforced by state laws — but also gaps where neither federal nor (most) state law protect. Accordingly, researchers and IRBs need to be aware of those protections and gaps to be able to determine the impact of research design on the risks a study presents, as well as what information ought to be conveyed to participants during the consent process.

Note

Other than the grant support acknowledged below, the authors have no conflicts to declare.

Acknowledgments

This work was supported by a grant from the National Human Genome Research Institute (R01-HG-007733, PI: Laura M. Beskow). Professor Wolf's time was supported in part by a grant from the National Human Genome Research Institute and National Cancer Institute (R01-HG-008605, PIs: Susan M. Wolf, Ellen Wright Clayton, and Frances Lawrenz). The content is solely the responsibility of the authors and does not necessarily represent the official views of NHGRI, NCI, or NIH. The authors thank Barbara Evans and the peer reviewers for their helpful feedback.

References

1. S. Landau, "Control Use of Data to Protect Privacy," *Science* 347, no. 6221(2015): 504-506.
2. F. S. Collins and H. Varmus, "A New Initiative on Precision Medicine," *New England Journal of Medicine* 372, no. 9 (2015): 793-795; AACR Project GENIE Consortium, "AACR Project GENIE: Powering Precision Medicine through an International Consortium," *Cancer Discovery* 7, no. 8 (2017): 818-831; E. E. Schadt, "The Changing Privacy Landscape in the Era of Big Data," *Molecular Systems Biology* 8 (2012): 612-614.
3. Schadt, *supra* note 2; L. L. Rodriguez, "The Complexities of Genomic Identifiability," *Science* 339, no. 6117 (2013): 275-276; J. Kulynych and H. T. Greely, "Clinical Genomics, Big Data, and Electronic Medical Records: Reconciling Patient Rights with Research when Privacy and Science Collide," *Journal of Law and the Biosciences* 4, no. 1 (2017): 94-132; M. A. Rothstein, "Ethical Issues in Big Data Health Research," *Journal of Law, Medicine & Ethics* 43, no. 2 (2015): 425-429; M.

The Journal of Law, Medicine & Ethics, 48 (2020): 126-141.

A. Rothstein, "Some Lingering Concerns about the Precision Medicine Initiative," *Journal of Law, Medicine & Technology* 44, no. 3 (2016): 520-525.

4. S. A. Tovino, "The HIPAA Privacy Rule and the EU GDPR: Illustrative Comparisons," *Seton Hall Law Review* 47, no. 4 (2017): 973-993, at 975.
5. 45 C.F.R. part 46 (2018). There are twenty federal agencies that have adopted these Department of Health and Human Services regulations, either as signatories or by executive order or statutory mandate, hence the moniker "Common Rule." U.S. Department of Health and Human Services, Federal Policy for the Protection of Human Subjects ('Common Rule'), *available at* <https://www.hhs.gov/ohrp/regulations-and-policy/regulations/common-rule/index.html> (last visited February 3, 2020). The Food and Drug Administration has its own rules (21 C.F.R. parts 50 & 56 (2019)) that apply to research within its authority (*e.g.,* for drug or device approval) that are substantially similar, but not identical, to the Common Rule. U.S. Food and Drug Administration. Comparison of FDA and HHS Human Subject Protection Regulations, *available at* <https://www.fda.gov/scienceresearch/specialtopics/runningclinicaltrials/educationalmaterials/ucm112910.htm> (last visited February 3, 2020). Revisions to the Common Rule were published in the Federal Register in January 2017, after our thought leader interviews were completed and, after some delay, were implemented in January 2019. U.S. Department of Health and Human Resources Office for Human Research Protections, Revised Common Rule, *available at* <https://www.hhs.gov/ohrp/regulations-and-policy/regulations/finalized-revisions-common-rule/index.html> (last visited February 3, 2020). However, the changes do not significantly alter the provisions relevant to our project.
6. 45 C.F.R. § 160 (2018); 45 C.F.R. § 164 (2018).
7. 29 U.S.C. § 1182(b) (2018) (prohibiting discrimination in employer-based insurance); 42 U.S.C. § 300gg-3(b)(1)(B) (2011) (regarding group health insurance); 42 U.S.C. § 2000ff-1 (2018) (prohibiting employment discrimination on the basis of genetic information).
8. See L. E. Wolf, E. Fuse Brown et al., "The Web of Legal Protections for Participants in Genomic Research," *Health Matrix* 29, no. 1 (2019): 1-112.
9. For thought leader interviews, see L. M. Beskow, C. M. Hammack, and K. M. Brelsford, "Thought Leader Perspectives on Benefits and Harms in Precision Medicine Research," *PLoS One* 13, no. 11: e0207842 (2018); L. M. Beskow et al., "Thought Leader Perspectives on Risks in Precision Medicine Research," in I. G. Cohen, H. F. Lynch, and E. Vayena, eds., *Big Data, Health Law, and Bioethics* (Cambridge, UK: Cambridge University Press, 2018): 161-174; C. M. Hammack, K. M. Brelsford, and L. M. Beskow, "Thought Leader Perspectives on Participant Protections in Precision Medicine Research," *Journal of Law, Medicine & Ethics* 47, no. 1 (2019): 134-148. For the legal analysis, see Wolf et al., *supra* note 8.
10. Beskow et al., "Thought Leader Perspectives on Risks in Precision Medicine Research," *supra* note 9, at 170-71.
11. Beskow et al., "Thought Leader Perspectives on Benefits and Harms in Precision Medicine Research," *supra* note 9.
12. For thought leader interviews, see Beskow et al., "Thought Leader Perspectives on Benefits and Harms in Precision Medicine Research," *supra* note 9; Beskow et al., "Thought Leader Perspectives on Risks in Precision Medicine Research," *supra* note 9; Hammack et al., "Thought Leader Perspectives on Participant Protections in Precision Medicine Research," *supra* note 9. For the legal analysis, see Wolf et al., *supra* note 8.
13. U.S. Department of Health and Human Services, National Institutes of Health, All of Us Research Program, *available at* <https://allofus.nih.gov/> (last visited February 3, 2020).
14. K. M. MacQueen et al., "Codebook Development for Team-Based Qualitative Analysis," *Cultural Anthropology Methods* 10, no. 2 (1998): 31-36.
15. Beskow et al., "Thought Leader Perspectives on Risks in Precision Medicine Research," *supra* note 9, at 167-72; Beskow et al., "Thought Leader Perspectives on Benefits and Harms in Precision Medicine Research," *supra* note 9.
16. 45 C.F.R. §§ 46.109 & .116 (2018).
17. Hammack et al., "Thought Leader Perspectives on Participant Protections in Precision Medicine Research," *supra* note 9, at 141-43.
18. 45 C.F.R. §§ 46.111(a)(1) & (2) (2018).
19. Hammack et al., "Thought Leader Perspectives on Participant Protections in Precision Medicine Research," *supra* note 9, at 141-43.
20. 45 C.F.R. § 46.109(e) (2018)("An IRB shall conduct continuing review of research requiring review... at intervals appropriate to the degree of risk, not less than once per year," although the post-2018 rules now exclude some low-risk studies from this requirement.).
21. S. Davis, "Monitoring of Approved Studies: A Difficult Tightrope Walk by Ethics Review Committees," *Perspectives in Clinical Research* 9, no. 2 (2018): 91-94; S. Hoffman, "Continued Concern: Human Subject Protection, the Institutional Review Board, and Continuing Review," *Tennessee Law Review* 68, no. 4 (2001): 725-770.
22. According to a recent report, federal funding accounts for less than 25% of funding for medical and health research and development. Research America, U.S. Investments in Medical and Health Research and Development, 2013-2015 (2016), *available at* <https://www.researchamerica.org/sites/default/files/2016US_Invest_R&D_report.pdf> (last visited February 3, 2020). This is consistent other data indicating that, as of 2017, the federal government funded less than half of basic research. J. Mervis, "Data Check: U.S. Government Share of Basic Research Hits New Low," *Science 335*, no. 6329 (2017): 1005. Although institutions may — and many do — apply the Common Rule provisions to all research in which they are involved, they are not legally required to do so.
23. See L. E. Wolf, "Advancing Research on Stored Biological Materials: Reconciling Law, Ethics, and Practice," *Minnesota Journal of Law, Science and Technology* 11, no. 1 (2010): 99-156, at 128-33. These exceptions remain under the new Common Rule.
24. J. P. Wolley et al., "Citizen Science or Scientific Citizenship? Disentangling the Uses of Public Engagement Rhetoric in National Research Intiatives," *BMC Medical Ethics* 17, no. 1 (2016): 33, at 2-4; M. V. Eitzel et al., "Citizen Science Terminology Matters: Exploring Key Terms," *Citizen Science: Theory and Practice* 2, no. 1 (2017): 1-20.
25. See 45 C.F.R. § 46.102(f) (2016)[pre-2018 Common Rule], 45 C.F.R. § 46.102(e)(1) (2018)[2018 Common Rule] and Office for Human Research Protections, U.S. Department of Health and Human Services, Coded Private Information or Specimens Use in Research, Guidance (2008), *available at* <https://www.hhs.gov/ohrp/regulations-and-policy/guidance/research-involving-coded-private-information/index.html> (last visited February 3, 2020).
26. U.S. Department of Health and Human Services, Office for Human Research Protections, Exempt Research Determination FAQs, *available at* <https://www.hhs.gov/ohrp/regulations-and-policy/guidance/faq/exempt-research-determination/index.html> (last visited February 3, 2020).
27. The law mandates IRB review of *all* genetic research for "explicit prior approval or an explicit determination that the research is anonymous or otherwise exempt," that includes "disclos[ure of] ...the intended use of [the biospecimens] for every proposed research project, even anonymous or otherwise exempt research." Ore. Admin. R. § 333-025-0100 et seq. (2019). There are a few states that have human subjects laws that apply when the Common Rule does not (*e.g.,* to non-federally funded research). See Cal. Health & Safety Code § 24170 et seq. (West 1999), Md. Code Ann. Health-Gen. § 13-2001 et seq. (West 2018), N.Y. Pub. Health Law § 2440 et seq. (McKinney 2019), and Va. Code Ann. § 32.1-162.16 et seq. (2018). However, as these mimic the Common Rule's exemptions, they

The Journal of Law, Medicine & Ethics, 48 (2020): 126-141. © 2020 The Author(s)

do not extend protections for secondary research. See Wolf et al., *supra* note 8, at 27-28.

28. As described above, some research involving biological specimens is not considered "human subjects" research and, thus, falls outside the Common Rule. Research involving biological specimens may also fall within one of the exemptions under the Common Rule or may qualify for a waiver of consent. H. F. Lynch, L. E. Wolf, and M. Barnes, "Implementing Regulatory Broad Consent Under the Revised Common Rule: Clarifying Key Points and the Need for Evidence," *Journal of Law, Medicine & Ethics* 47, no 2 (2019): 213-231, at 215-221. Identifiability is key to these exceptions to the Common Rule; as the agencies are required under the revisions to reconsider periodically what is "identifiable," these options could be limited in the future. H. F. Lynch and M. N. Meyer, "Regulating Research with Biospecimens under the Revised Common Rule," *Hastings Center Report* 47, no. 3 (2017): 3-4, at 4.
29. Hammack et al., "Thought Leader Perspectives on Participant Protections in Precision Medicine Research," *supra* note 9, at 141-43.
30. See L. M. Beskow et al., "Simplifying Informed Consent for Biorepositories: Stakeholder Perspectives," *Genetics in Medicine* 12, no. 9 (2010): 567-572.
31. This "broad consent" has facilitated the development of genomics and other research databases. C. Grady et al., "Broad Consent for Research with Biological Samples: Workshop Conclusions," *American Journal of Bioethics* 15, no. 9 (2015): 34-42. The 2018 Common Rule introduced a new regulatory broad consent option, although it is unclear what impact it will have. Lynch et al., *supra* note 28, at 226.
32. 45 C.F.R. § 46.116(d)(2) (2018).
33. If identifiers were shared, consent may still not be required if the research meets the regulatory criteria for waiver. See 45 C.F.R. § 46.116(d) (2016)[pre-2018 Common Rule] and 45 C.F.R. § 46.116(f)(3) (2018)[2018 Common Rule].
34. Wolf et al., *supra* note 8, at 39-43.
35. 45 C.F.R. § 46.116(a)(8)(2016) and (2018) [both pre-2018 and 2018 Common Rule].
36. Beskow et al., "Thought Leader Perspectives on Risks in Precision Medicine Research," *supra* note 9, at 171-72; Wolf et al., *supra* note 8, at 22-23.
37. Wolf et al., *supra* note 8, at 31-33.
38. 45 C.F.R. § 164.512 (2018)(specifying disclosures for which authorizations are not required).
39. 45 C.F.R. § 160.103 (2018), defining health information as "any information, *including genetic information*, whether oral or recorded in any form or medium, that: (1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and (2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual." (emphasis added).
40. 45 C.F.R. §§ 164.400 to 164.414 (2018) (breach notification); 45 C.F.R. § 164.508 (2018) (marketing and sale of PHI); 45 C.F.R. § 164.524 (2018) (right of access); 45 C.F.R. Part 164, subpart C (2018) (Security Rule).
41. Specifically, the authorization must provide the participant with descriptions of (1) the information that will be used or disclosed; (2) each purpose of the requested use or disclosure; (3) an expiration date; (4) the individual's right to revoke the authorization and how to revoke the authorization; and (5) the potential of information to be redisclosed to a recipient not subject to the HIPAA Privacy Rule. 45 C.F.R. § 164.508(c) (2018). This authorization may be combined with the research consent. 45 C.F.R. § 164.508(b)(3) (2018).
42. 45 C.F.R. § 164.508(c)(1)(iv) (2018) (emphasis added).
43. U.S. Department of Health and Human Services., Office of Civil Rights, Guidance on HIPAA and Individual Authorization of Uses and Disclosures of Protected Health Information for Research (June 2018), at 3, *available at* <https://www.hhs.gov/sites/default/files/hipaa-future-research-authorization-guidance-06122018%20v2.pdf> (last visited February 3, 2020).
44. 45 C.F.R. § 164.508(c)(1)(5) (2018); Office of Civil Rights, *supra* note 43, at 3. The HIPAA Privacy Rule also requires an individual's authorization for uses or disclosures of their PHI for marketing, avoiding some risks thought leaders raised. 45 C.F.R. § 164.508 (2018). There are some exceptions that are not applicable in the research context.
45. Hammack et al., "Thought Leader Perspectives on Participant Protections in Precision Medicine Research," *supra* note 9, at 143-44.
46. 45 C.F.R. §§ 160.102, 160.103, 164.500 (2018).
47. U.S. Department of Health and Human Services, How Can Covered Entities Use and Disclose Protected Health Information for Research and Comply with the Privacy Rule, *available at* <https://privacyruleandresearch.nih.gov/pr_08.asp> (last visited February 3, 2020); U.S. Department of Health and Human Services FAQ 315: When Does a Covered Entity Have Discretion to Determine Whether a Research Component of the Entity Is Part of Their Covered Functions, and Therefore Subject to the HIPAA Privacy Rule? (Mar. 14, 2006), *available at* <https://www.hhs.gov/hipaa/for-professionals/faq/315/when-does-a-covered-entity-have-discretion-to-determine-covered-functions/index.html> (last visited February 3, 2020).
48. Wolf et al., *supra* note 8, at 43-47.
49. Hammack et al., "Thought Leader Perspectives on Participant Protections in Precision Medicine Research," *supra* note 9, at 143-44.
50. 45 C.F.R. § 164.514(e)(2) (2018).
51. Beskow et al., "Thought Leader Perspectives on Risks in Precision Medicine Research," *supra* note 9, at 167-70.
52. Hammack et al., "Thought Leader Perspectives on Participant Protections in Precision Medicine Research," *supra* note 9, at 143-44.
53. See U.S. Department of Health and Human Services Office for Civil Rights, Breach Portal: Notice to Secretary of HHS Breach of Unsecured Protected Health Information, *available at* <https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf> (last visited February 3, 2020) for a list of breaches affecting 500 or more individuals.
54. Wolf et al., *supra* note 8, at n. 236.
55. Grady et al., *supra* note 31.
56. Hammack et al., "Thought Leader Perspectives on Participant Protections in Precision Medicine Research," *supra* note 9, at 137-41.
57. *Id.*
58. Beskow et al., "Thought Leader Perspectives on Benefits and Harms in Precision Medicine Research," *supra* note 9.
59. *Id.*
60. *Id.*
61. 45 C.F.R. § 46.116(c)(8) (2018).
62. Beskow et al., "Thought Leader Perspectives on Benefits and Harms in Precision Medicine Research," *supra* note 9.
63. *Id.*
64. *Id.*
65. 45 C.F.R. § 164.524 (2018). A designated record set includes medical, insurance, and billing records and any records "used in whole or in part, by or for the covered entity to make decisions about individuals." The Privacy Rule's clinical trial exception allowing suspension of participant access to their information would not apply to the MAS, where treatment is not provided as part of the research. 45 C.F.R. § 164.524(a)(2)(iii) (2018).
66. Department of Health and Human Services, FAQ 311: What does the HIPAA Privacy Rule Say About a Research Participant's Right of Access to Research Results? (updated Mar. 14, 2006), *available at* <https://www.hhs.gov/hipaa/for-professionals/faq/311/what-does-hipaa-say-about-research-participants-right-of-access/index.html> (last visited February 3, 2020); National Institutes of Health, Clinical Research and the HIPAA Privacy Rule, *available at* <https://privacyrule-

The Journal of Law, Medicine & Ethics, 48 (2020): 126-141. © 2020 The Author(s)

andresearch.nih.gov/clin_research.asp> (updated June 22, 2004)(last visited February 3, 2020) ("[R]esearch data would not be considered part of the designated record set if, for example, the research data is not used to make decisions about the individual and not part of the medical record. In that case, the individual would not have a right to access the data.").
67. 79 Fed. Reg. 7290, 7291 (Feb. 6, 2014); B. Evans et al., "Regulatory Changes Raise Troubling Questions for Genomic Testing," *Genetics in Medicine* 16, no. 11 (2014): 799-803, at 800.
68. A laboratory may be a HIPAA-covered entity if, for example, it submits any bills to an insurance company for payment or if it is part of an academic medical center that extends covered entity status to the research lab. Evans et al., *supra* note 67, at 802. See also B. J. Evans, "HIPAA's Individual Right of Access to Genomic Data: Reconciling Safety and Civil Rights," *American Journal of Human Genetics* 102, no. 1 (2018): 5-10, at 5.
69. Wolf et al., *supra* note 8, at 69-73.
70. Or. Rev. Stat. Ann. § 192.537(7) (2019)("An individual or an individual's representative, promptly upon request, may inspect, request correction of and obtain genetic information from the records of the individual").
71. Del. Code Ann. Titl 16, § 1204 (2019); Fla. Stat. Ann. § 760.40 (2018)(through physician); Nev. Rev. Stat. Ann. § 629.141 (2017); N.J. Stat. Ann. § 10:5-46 (West 2018); S.D. § 34-14-22 (2019). A few other states allows patients similar rights to their records. Md. Code Ann. Health-Gen. 13-109 (2018) (refers to "unambiguous diagnostic results"); 10A N.C. Admin Code 47C.0101 et seq. (2019); Wash Rev. Code Ann. § 70.02.005 et seq. (2019). See Wolf et al., *supra* note 8, at 69-73.
72. Alaska Stat. Ann. § 18.13.010 (2018); Colo. Rev. Stat. Ann. § 10-3-1104.6 and 10-3-1104.7 (2018); Ga. Code Ann. § 33-54-1 et seq. (2019); Fla. Stat. Ann. § 760.40. (2018); La. Rev. Stat. Ann. § 22: 1023 (2018) & 37 La. Admin Code Pt XIII, 4515 (2018). See Wolf et al., *supra* note 8, at 74-75; J. L. Roberts, "Progressive Genetic Ownership," *Notre Dame Law Review* 93, no. 3: 1105-1172, at 1110 (2018).
73. Beskow et al., "Thought Leader Perspectives on Risks in Precision Medicine Research," *supra* note 9, at 163-67.
74. Wolf et al., *supra* note 8, at 36 (citing 2015 U.S. Census data).
75. Wolf et al., *supra* note 8, at 54-56. As thought leaders indicated, the ADA, which is broader than GINA, may provide some additional protections, but the legal arguments are complex and uncertain and, practically, may be easily thwarted. *Id.* at 90-98.
76. *Id.* at 63.
77. *Id.* at 63-69.
78. *Id.* at 35-36.
79. 42 U.S.C. §§ 300gg, 300gg-4 (2018).
80. C. H. Monahan, "Private Enforcement of the Affordable Care Act: Toward an 'Implied Warranty of Legality' in Health Insurance," *Yale Law Journal* 126, no. 4 (2017): 1118-1179, at 1123. The exception is Section 1557 of the ACA, providing a private right of action to enforce the prohibition on discrimination on the basis of race, color, national origin, sex, age, or disability by health programs that receive federal financial assistance, including ACA plans sold on the Exchanges.
81. Beskow et al., "Thought Leader Perspectives on Benefits and Harms in Precision Medicine Research," *supra* note 9, at 144-46. There have been multiple efforts to repeal or limit the effect of the ACA. These include executive orders to delay provisions of the ACA, removal of information regarding enrollment, limiting outreaching, advertising, and the enrollment period, and multiple votes on alternative health care bills. J. Rovner, "Timeline: Despite GOP's Failure to Repeal Obamacare, The ACA Has Changed," *Kaiser Health News,* April 4, 2018, *available at* <https://khn.org/news/timeline-roadblocks-to-affordable-care-act-enrollment/> (last visited February 5, 2020). After the ACA survived multiple Republican attempts in Congress to repeal the statute, a federal district judge in Texas held in December 2018 in a lawsuit filed by Republican govenors and state attorneys general, that because the individual mandate had been struck down, the rest of the Affordable Care Act was unconstitutional. In December 2019, the Fifth Circuit upheld the ruling that the ACA's individual mandate is unconstitutional but remanded the case to the District Court to decide whether the vest of the statute is severable from the individual mandate. *Texas v. US*, 945 F3d 355 (5th Cir. 2019). The fate of the ACA remains in limbo at the time of this writing.
82. Wolf et al., *supra* note 8, at 56-60.
83. *Id.*
84. *Id.* at 78-82.
85. Beskow et al., "Thought Leader Perspectives on Benefits and Harms in Precision Medicine Research," *supra* note 9, at 144-46.
86. Hammack et al., "Thought Leader Perspectives on Participant Protections in Precision Medicine Research," *supra* note 9, at 144.
87. Beskow et al., "Thought Leader Perspectives on Risks in Precision Medicine Research," *supra* note 9, at 163-67.
88. 45 C.F.R. Part 164, subpart C (2018).
89. Wolf et al., *supra* note 8, at 43.
90. B. Cohen, "The Evolving Legal Framework Regulating Commercial Data Security Standards," *Maryland Bar Journal* (2014), at 30, 31, *available at* <https://www.hldataprotection.com/files/2014/01/Md.-Bar-J.-Cohen-The-Evolving-Legal-Framework-Regulating-Commercial-Data-Security-Standards-Jan.-2014.pdf> (last visited March 5, 2020).
91. Beskow et al., "Thought Leader Perspectives on Benefits and Harms in Precision Medicine Research," *supra* note 9, at 137-38.
92. *Id.*
93. Beskow et al., "Thought Leader Perspectives on Risks in Precision Medicine Research," *supra* note 9, at 163-67.
94. Hammack et al., "Thought Leader Perspectives on Participant Protections in Precision Medicine Research," *supra* note 9, at 137-41.
95. 45 C.F.R. §§ 164.400 to 164.414 (2018).
96. Wolf et al., *supra* note 8, at 64-69 (discussing private rights of actions under genetic privacy laws).
97. *Id.* (discussing statutory damages for violation of genetic or health information privacy laws).
98. "A person may not reidentify or attempt to reidentify an individual who is the subject of any protected health information without obtaining the individual's consent or authorization [if required by law]." Tex. Health & Safety Code § 181.151 (West 2018). A few states have identity theft laws specific to health information that could provide some remedy. *See, e.g.*, Colo. Rev. Stat. Ann. § 18-4-412 (2019); Mont. Code Ann. § 50-16-551 (2018); Neb. Rev. Stat. Ann. § 81-674 (2018); Nev. Rev. Stat. § 439.590 (2019); Wis. Stat. Ann. § 146.84(1)(bm) (2018).
99. See, e.g., Iowa Code Ann. § 715A.8 (2019).
100. 45 C.F.R. § 164.514(e)(4) (2018).
101. Hammack et al., "Thought Leader Perspectives on Participant Protections in Precision Medicine Research," *supra* note 9, at 139-41.
102. Beskow et al., "Thought Leader Perspectives on Benefits and Harms in Precision Medicine Research," *supra* note 9.
103. T. Fuller, "How a Genealogy Site Led to the Front Door of the Golden State Killer Suspect," *New York Times*, April 26, 2018, *available at* <https://www.nytimes.com/2018/04/26/us/golden-state-killer.html> (last visited February 5, 2020; K. Swenson, "Undercover cops grabbed a DJ's chewing gum. It helped crack a teacher's 1992 murder, police say," *Washington Post*, June 26, 2018, *available at* <https://www.washingtonpost.com/news/morning-mix/wp/2018/06/26/undercover-cops-grabbed-a-djs-chewing-gum-it-helped-crack-a-teachers-1992-murder-police-say/> (last visited February 5, 2020); K. Swenson, "After 30 Years, Police Say They've Captured A Child-Killer Who Left A Sickening Trail of Taunts," *Washington Post*, July 16, 2018, *available at* <https://www.washingtonpost.com/news/morning-mix/wp/2018/07/16/i-

The Journal of Law, Medicine & Ethics, 48 (2020): 126-141. © 2020 The Author(s)

been-watching-you-a-child-killer-taunted-little-girls-with-terrifying-notes-police-say-after-30-years-dna-led-to-an-arrest/> (last visited February 5, 2020). L. E. Wolf and L. M. Beskow, "Genomic Databases, Subpoenas, and Certificates of Confidentiality," *Genetics in Medicine* (2019), *available at* <https://doi.org/10.1038/s41436-019-0592-0> (last visited March 23, 2020).

104. L. E. Wolf et al., "Certificates of Confidentiality: Legal Counsels' Experiences with and Perspectives on Legal Demands for Research Data," *Journal of Empirical Research on Human Research Ethics* 7, no. 4 (2012): 1-9, at 3.
105. Beskow et al., "Thought Leader Perspectives on Benefits and Harms in Precision Medicine Research," *supra* note 9; Beskow et al., "Thought Leader Perspectives on Risks in Precision Medicine Research," *supra* note 9, at 170-71.
106. 42 U.S.C. § 241(d) (2017).
107. See L. E. Wolf and L. M. Beskow, "New and Improved? 21st Century Cures Act Revisions to Certificates of Confidentiality," *American Journal of Law & Medicine* 44, no. 2-3 (2018): 343-358. for a detailed analysis of these changes.
108. Hammack et al., "Thought Leader Perspectives on Participant Protections in Precision Medicine Research," *supra* note 9, at 138-39.
109. *People v. Newman*, 32 N.Y.3d 379 (1973), *cert. denied*, 414 U.S. 1163 (1974). For a discussion of this and other cases involving Certificates, see L. E. Wolf et al., "Certificates of Confidentiality: Protecting Human Subject Research Data in Law and Practice," *Journal of Law, Medicine & Ethics* 43, no. 3 (2015): 594-609, at 596-600.
10. *North Carolina v. Bradley*, 634 S.E.2d 258 (2006) and juvenile court case discussed in Wolf et al., *supra* note 109, at 597-600.
111. See Wolf et al., *supra* note 109, at 602-03.
112. See, e.g., Wolf and Beskow, *supra* note 107.
113. U.S. Department of Health and Human Services, National Institutes of Health, Frequently Asked Questions, VII.A.5, *available at* <https://grants.nih.gov/policy/hs/faqs.htm#5817> (last visited February 5, 2020).
114. Wolf and Beskow, *supra* note 107, at 351-352.
115. A small number of states have laws that provide Certificate-like protections, but these apply only to specific circumstances, such as genetic research (Ark. Code Ann. § 20-35-103 (2018) and Okla. Stat. Ann. Tit. 36, § 3614.4 (2019)) or to data held by researchers at publicly funded universities (La. Rev. Stat. Ann. § 44.7 (2018)) and apply only to *civil* litigation. Other statutes that apply to genetic information have many exceptions. Wolf et al., *supra* note 8, at 49-52.
116. 45 C.F.R. § 164.512(f) (2018). This includes information "related to the individual's DNA or DNA analysis … samples or analysis of body fluids or tissue" in response to a court order, warrant, or subpoena without individual authorization or notice. 45 C.F.R. § 164.512(f)(1); Department of Health and Human Services., FAQ 505: When does the Privacy Rule allow covered entities to disclose protected health information to law enforcement officials? (July 23, 2004), *available at* <https://www.hhs.gov/hipaa/for-professionals/faq/505/what-does-the-privacy-rule-allow-covered-entities-to-disclose-to-law-enforcement-officials/index.html> (last visited February 5, 2020).
117. 45 C.F.R. § 164.512(f)(2) (2018). The information that researchers could disclose to help law enforcement identify a suspect without a legal demand would be limited to name and address, date and place of birth, social security number, ABO blood type and rh factor, type of injury, date and time of treatment, date and time of death, and a description of distinguishing physical characteristics.
118. This includes receiving evidence that there were reasonable efforts to notify the individual about the request that would allow the individual to object and to seek a protective order from the court. Such evidence would be in the form of a written statement and documentation of either (1) the requestor's notice to the individual with information about the litigation and instructions for raising objections, or (2) an agreement between the parties or a request to the court for a qualified protective order. Department of Health and Human Services, FAQ 706: What "satisfactory assurances" must a covered entity that is not a party to the litigation receive before it may respond to a subpoena without a court order? (Jan. 7, 2005), *available at* <https://www.hhs.gov/hipaa/for-professionals/faq/706/what-satisfactory-assurances-must-a-covered-entity-receive-before-it-responds-to-a-subpoena/index.html> (last visited February 5, 2020).
119. Wolf et al., *supra* note 8, at 101-102.
120. See J. A. Catania et al., "Research Participants' Perceptions of the Certificate of Confidentiality's Assurances and Limitations," *Journal of Empirical Research on Human Research Ethics* 2, no. 4 (2007): 53-59; D. K. Check et al., "Certificates of Confidentiality and Informed Consent: Perspectives of IRB Chairs and Institutional Legal Counsel," *IRB: Ethics and Human Research* 36, no. 1 (2014): 1-8.

The Journal of Law, Medicine & Ethics, 48 (2020): 126-141. © 2020 The Author(s)