World Privacy Forum

Privacy, the Precision Medicine Initiative, & the All of Us Research Program: Will Any Legal Protections Apply?

By Robert Gellman and Pam Dixon

Second Edition, March 2017
Revised, includes 21st Century Cures Act

Background of This Report

This is the second edition of a report originally published by the World Privacy Forum in 2016 about the privacy implications of the Precision Medicine Initiative (PMI), a national volunteer medical research effort. Both editions of the report contain legal analysis about privacy protections applicable to the PMI and recommendations.

The PMI is an ambitious program with a goal of gathering the freely volunteered health and biospecimen data of over a million people to facilitate medical research. The PMI program originally began during the Obama administration and was still in its formative stage when the original 2016 WPF report was published. As of March 2017, the PMI has undergone many changes. First, the PMI was partially renamed, and now includes the All of Us Research Program. The All of Us research program consists of the 1-million person volunteer research volunteer group that will make up the bulk of PMI research program. A second and important change is that the PMI/All of Us program has become an official part of the National Institutes of Health as of January 2017, and the program has now been officially funded. Third, there is now a launch of the PMI/All of Us research program, it is scheduled for April 2017. The April launch will be of the planned pilot research programs, and will involve the enrollment of research participants. With the launch imminent, it is crucial to examine and understand the privacy protections for the PMI and All of Us research program.

The second edition of this report includes updated information about the program and more detail about other aspects of the program that changed in the past year. An important addition to this report is the inclusion of analysis of the recently-enacted 21st Century Cures Act, which specifically impacts the PMI/All of Us program.

Brief Summary of Report

Medical treatments tailored to each individual's physiology and genetic history have long been a dream, but this dream is data-intensive. Until recently, the lack of a broad set of detailed health information from a wide variety of research subjects stymied medical research efforts. The most current effort to turn personalized, tailored medicine into a reality is the Precision Medicine Initiative (PMI), which now includes the All of Us research program. It is this full PMI/All of Us research program, begun in 2015, that hopes to gather an unprecedented amount of detailed biomedical data sets -- including biospecimens and detailed personal health information -- from over one million volunteers, the largest group of medical research volunteers that has been assembled thus far in the United States, if not the world.

Collecting, maintaining, reporting results back to research subjects/participants, and sharing biospecimens and health data from over a million volunteers for research requires meaningful privacy protections. To determine how privacy laws may protect PMI data subjects and their information, this report reviews federal privacy laws potentially applicable to the program. The analysis finds that despite the breadth and sensitivity of planned PMI data, the HIPAA health privacy rule and its protections for individuals will not apply to PMI. Other privacy laws may

apply, such as the Privacy Act of 1974, but there is considerable uncertainty if that law or other privacy laws apply in whole or in part. The lack of applicability will impact everything from access to results, to control over with whom those results are shared, among many other issues.

In December 2016, Congress enacted the 21st Century Cures Act, a long and complex health policy law that, among many other things, addressed PMI and some privacy matters. The 21st Century Cures Act appears to fix some of the shortcomings with Certificates of Confidentiality that provide privacy protections for research records used in research, but the Act did not answer most of the continuing questions about which existing privacy laws apply to PMI.

The PMI program itself includes a set of privacy principles. These principles are not formal laws. Because this report focuses on analysis of actual privacy law that has enforceable rights and procedures, the voluntary and seemingly unenforceable PMI privacy principles are not the focus of attention.

The key privacy concerns raised by the full PMI/All of Us program include:

- **The lack of applicable privacy law to govern its collection and use of individuals' health data**
- **The potential waiver of the patient-physician legal privilege that can shield data from disclosure through litigation**
- **The possibility of law enforcement access to patient records held in the PMI/All of Us databases.**

The PMI program still needs to clarify and strengthen the legal and administrative privacy protections that apply to its activities. People who volunteer their biomedical data sets still must be told clearly what specific legal protections apply and do not apply and what rules exist for law enforcement access to patient records and other biomedical data, such as blood samples.

About the Authors

Robert Gellman is a privacy and information policy consultant in Washington DC. (www.bobgellman.com.) He has written extensively on health, de-identification, Fair Information Practices, and other privacy topics. Pam Dixon is the founder and Executive Director of the World Privacy Forum. She is the author of eight books, hundreds of articles, and numerous privacy studies, including her landmark Medical Identity Theft study. She has testified before Congress on consumer privacy issues as well as before federal agencies. Dixon and Gellman's writing collaborations include the seminal report on predictive algorithms, *The Scoring of America*, and numerous well-regarded privacy-focused research, articles, and policy analyses. They co-authored a reference book on privacy, *Online Privacy: A Reference Handbook,* (ABC-CLIO 2011) and most recently a chapter on privacy regulation and law in *Enforcing Privacy: Regulatory, Legal, and Technological Approaches,* (Springer Nature, 2016.)

About the World Privacy Forum

The World Privacy Forum is a non-profit public interest research and consumer education group that focuses on the research and analysis of privacy-related issues. Founded in 2003, the Forum publishes significant privacy research and policy studies on health privacy, privacy self-regulation, financial privacy and identity issues, biometrics, and data broker privacy practices among other issues. The *Patient's Guide to HIPAA* is a long-standing resource maintained at WPF. WPF members have testified before Congress regarding privacy issues, including health privacy, and have regularly contributed privacy expertise to agency-level workshops at the Federal Trade Commission, the FDA, and HHS. For more, see www.worldprivacyforum.org.

Contents

March, 2017 | Robert Gellman and Pam Dixon
Second edition, Revised, includes 21st Century Cures Act

Privacy, the Precision Medicine Initiative, & the All of Us Research Program: Will Any Legal Protections Apply?

Part I: Introduction and Summary

The goals of the Precision Medicine Initiative and the All About Us Research Program[1] are laudable, but many core privacy questions remain unanswered. These unanswered questions may undercut individuals' willingness to share their data and may create new problems for volunteers. As with many healthcare research activities, some see privacy as an obstacle to scientific advancement. That objection fails to recognize privacy's essential value in and to the health care system. Privacy, rather than being an impediment to medical research, is an essential feature of health care and medical research. Privacy must be addressed in any major health care data activity. If the PMI program does not clarify the privacy protections for its activities, individuals will be more reluctant to volunteer to participate.

[1] Hereafter the Precision Medicine Initiative or PMI refers to the full PMI/All of Us program. Relationship of All of Us Research Program and PMI discussed here: NIH, All of Us Research Program FAQ, https://www.nih.gov/allofus-research-program/frequently-asked-questions or https://www.nih.gov/allofus-research-program/frequently-asked-questions.

The initiative is still in its early stages, with a goal of collecting the health records and biospecimens of one million volunteers.[2] (See Appendices A and B in this report for specifics on the PMI timeline, and what information is to be collected from participants.) National Institutes of Health materials, including a Frequently Asked Questions, and other documents describing what volunteers can expect, discuss briefly how privacy will be handled. Yet despite this, individuals considering participation as well as privacy experts who advocate on their behalf cannot tell how the initiative will be structured, who will hold the data, what privacy laws apply, and how or whether privacy concerns will be addressed adequately.

This document analyzes the published plans for the initiative, raises questions about how the PMI plans to address privacy, and considers in brief the implications for volunteers. Many substantive details about the PMI program are still unknown. The analysis and discussion here reflects current privacy law, which is a known commodity and not likely to change significantly in the near future.

The goal of this paper is to make public the legal analysis undergirding our privacy concerns and to identify issues that the PMI should address in the near future.

Key Findings:

- Medical record data and biospecimen data that consumers donate to the PMI are not covered by the core federal health privacy law while in the hands of the PMI. The health privacy rule issued under the authority of the Health Insurance Portability and Accountability Act (HIPAA) does not apply to the PMI and will not apply to most research activities conducted using information available from the PMI.

- Consumers may have no formal legal right to obtain their own information from the PMI unless a US government agency administers the PMI, something that is not expected. The Privacy Act of 1974, which provides individuals with the ability to review data collected about them by a government agency, applies only if a federal agency operates the PMI. We do not yet know with certainty if a federal agency will operate any part of the PMI. However, if a federal agency operates the PMI, the Privacy Act's disclosure provisions allow agencies considerable authority to disclose records subject to the Act and to define new categories of disclosures at any time through new rules. In particular, the Act allows many types of disclosure to foreign, national, state, and local law enforcement agencies with few procedural prerequisites. We do not yet know what disclosure authority will apply to PMI records or even if they are subject to the Privacy Act. (See Appendix C.)

- Patients who share their health records and biospecimens with the PMI could lose the ability to claim a physician-patient privilege in unrelated judicial proceedings.

[2] The Precision Medicine Initiative Cohort Program – Building a Research Foundation for 21st Century Medicine, Sept. 17, 2015. PMI Working Report to the Advisory Committee to the Director, NIH, p. 1. https://www.nih.gov/sites/default/files/research-training/initiatives/pmi/pmi-working-group-report-20150917-2.pdf.

- A limited amount of patient records shared with PMI may be protected from subsequent disclosure if 42 C.F.R. Part 2 (rules governing substance abuse records) applied to the records at their original source. If so, records disclosed to the PMI from health care providers subject to the substance abuse privacy rules would retain their confidentiality if disclosed to the PMI. This may be the only existing privacy law applicable to the PMI, although it would cover few of the health records in the PMI.

- Certificates of confidentiality for research activities available through the Department of Health and Human Services may offer some legal protections for research records, but there are many uncertainties about the scope and value of the certificates. There are known limitations about the protections this would offer. The December 2016 21st Century Cures Act may result in general improvements to the legal protections afforded by certificates.

- When volunteers enroll in the PMI, they donate a great deal of personal information in the form of medical records and biospecimens. However, collection of cell phone, social media, sensor, and other real-time data are under discussion. How the privacy of these classes of real-time data not traditionally part of health records will be handled is an unknown. Further administrative records about volunteers – as opposed to health information – may be extensive and present their own privacy concerns. Administrative records may include contact information, identification numbers, employment and educational history, location data, and more.

- Nothing in the 21st Century Cures Act enacted in December 2016 resolves any of the uncertainties about the application of existing privacy laws to PMI program and activities.

Key Recommendations:

1. The PMI needs to detail its structure and organization with clarity so that the privacy protections or lack of privacy protections for its records can be assessed. The public needs to be clearly informed what institutions will maintain information in the PMI and where they are located. The PMI must explain how privacy laws, if any, will apply to it. The privacy and security standards issued so far do not answer the questions about what legal protections will apply.

2. The PMI should not begin soliciting information or biospecimens from or about individuals until it clearly describes the applicable privacy protections. The description should include potential uses and disclosures of PMI information for law enforcement and national security purposes. The description of applicable privacy rules should cover health records, administrative records, and any real-time monitoring from mobile or other devices. Volunteers should be told expressly if HIPAA does not apply to the PMI.

3. The E-Government Act of 2002 requires federal agencies to conduct a Privacy Impact Assessment before they develop or procure information technology systems or projects that

collect, maintain or disseminate information in identifiable form from or about members of the public.[3] We have not seen a PIA for the PMI. There is an immediate need for a PIA that includes an opportunity for public comment and debate.

4. If the Privacy Act of 1974 applies to PMI or any significant part of it, then the National Institutes of Health should publish a system of records notice and allow adequate time for public comment.

5. If the Privacy Act of 1974 does not apply to the PMI, then it is possible that no health privacy or other privacy law will apply to most data and biospecimens. As a result, patient data could be vulnerable to a host of unrelated public and private demands and activities. If so, then PMI may need its own privacy law in place before it starts.

Part II: Discussion and Legal Analysis of the Precision Medicine Initiative

Background and Purpose of the Precision Medicine Initiative and the All of Us Research Program

President Obama announced what was then just called the Precision Medicine Initiative (PMI) in January 2015. At the time, many hailed the PMI as the beginning of many medical research dreams come true. The core of the program is creating a large national database for medical research consisting of medical records information, survey information, and biospecimens.

According to the original Obama White House documents:

> The mission of the President's Precision Medicine Initiative (PMI) is to enable a new era of medicine through research, technology, and policies that empower patients, researchers, and providers to work together toward the development of individualized treatments.[4]

To accomplish these goals, the PMI will develop "a voluntary national research cohort of a million or more volunteers to propel our understanding of health and disease and set the

[3] See Office of Management and Budget, Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (2003)(M-03-22), https://obamawhitehouse.archives.gov/omb/memoranda_m03-22/.
[4] White House, *Precision Medicine Initiative: Data Security Policy Principles and Framework* (May 25, 2016), https://obamawhitehouse.archives.gov/sites/obamawhitehouse.archives.gov/files/documents/PMI_Security_Principles_Framework_v2.pdf.

foundation for a new way of doing research through engaged participants and open, responsible data sharing."[5]

Volunteers will share a robust data set with the initiative. What we know so far is from the National Institutes of Health, which states:

> What would be expected of me if I enroll in the Precision Medicine Initiative Cohort Program?
>
> Volunteers will be asked to share data including data from their electronic health records and health survey information. Participants may be asked to provide health data on lifestyle habits and environmental exposures as well. Participants will also undergo a standard baseline physical exam and provide a biological sample such as blood, urine, or saliva.[6]

We also know that volunteers may be asked for a great deal of additional information, which may eventually include information from their mobile phones and other sensors, as well as social media and perhaps even records of over the counter drug purchases. (Appendix B.) In this document, we do not question the intent or the goal of the PMI. At present, we accept as a given that the initiative is properly motivated and seeks to achieve an admirable public policy goal using a reasonable approach.

Still, any activity that expects to collect detailed health information and biospecimens from at least a million volunteers requires careful consideration of the privacy consequences. In addition to the health records and biospecimens, the PMI will have administrative records about volunteers that are not themselves health records per se. An administrative record may have identification and contact information for the volunteer, data about sources of information (e.g., physicians, other health care providers, and insurers), data about health devices used by the volunteer, work and education histories, financial information, and possibly more. Administrative information could be held in one or in multiple databases, and the databases could be maintained by different organizations in different locations.

A million administrative records about volunteers present major privacy and security concerns of their own, apart from any substantive health information. How these records will be organized, who will hold the records, and what privacy regime (if any) applies to the administrative records is not clear. Many important privacy-related questions arise – certainly, the protection of information and confidentiality. But another important aspect of PMI is if research participants will be able to see their own results, and control who else (like an insurance company or a physician) learns those results. Many difficult to solve privacy issues arise from this program.

---

[5] https://obamawhitehouse.archives.gov/the-press-office/2015/01/30/fact-sheet-president-obama-s-precision-medicine-initiative.

[6] NIH FAQ https://www.nih.gov/precision-medicine-initiative-cohort-program/precision-medicine-initiative-cohort-program-frequently-asked-questions. Or https://www.nih.gov/allofus-research-program/frequently-asked-questions.

Beyond federal law, it is also not clear if PMI records held in different states will be subject to different state privacy laws.[7]

The Obama White House initiative paid some attention to both privacy and security. For example, two key White House documents outline the privacy and security policies and principles.[8] While many of the principles acknowledge the need to address privacy, the principles are quite general and lack important legal and administrative details. The principles appear to be voluntary, are changeable at will, and may not create any enforceable legal rights.

One of the transparency principles states:

> Information should be made publicly available concerning PMI data protections and use, and compliance with governance rules.[9]

We applaud this policy, but this principle does not supply the details of those data protections or when they will be available. The statement's use of passive voice only underscores the problem. We do not know who should make information available or who should comply with governance rules. Additionally, many core documents directed to researchers do not address privacy in any meaningful way, instead, focusing on security issues.[10] When dealing with a richly detailed health database, the details matter, and the law matters.

The lack of specificity about privacy is troubling, especially considering that the program has already been funded.[11] Additionally, a significant unknown going forward is what kind of support the program will have under the Trump Administration. However, this report focuses only on applicable privacy law. It is extremely important to distinguish between privacy **principles** that are voluntary and perhaps unenforceable on one hand, and actual privacy **law** that has enforceable rights and procedures.

We accept that the PMI has voluntary privacy principles, but we cannot analyze the privacy principles at this time, recognizing that they lack specificity and may not carry the force of law.[12]

---

[7] For example, some states have specific laws regarding release of patient information. Many additional state laws can impact medical research issues. See for example *Privacy and Security Solutions for Interoperable Health Information Exchange* (Aug. 2009), https://www.healthit.gov/sites/default/files/disclosure-report-1.pdf.

[8] See White House, *Precision Medicine Initiative: Data Security Policy Principles and Framework* (May 25, 2016), https://obamawhitehouse.archives.gov/sites/obamawhitehouse.archives.gov/files/documents/PMI_Security_Principles_Framework_v2.pdf; *Precision Medicine Initiative: Privacy and Trust Principles* (Nov. 9, 2015), https://obamawhitehouse.archives.gov/sites/default/files/microsites/finalpmiprivacyandtrustprinciples.pdf.

[9] *Precision Medicine Initiative: Privacy and Trust Principle*s (Nov. 9, 2015), https://obamawhitehouse.archives.gov/sites/default/files/microsites/finalpmiprivacyandtrustprinciples.pdf.

[10] See for example, FAQ for Other Transaction Awards, https://www.nih.gov/precision-medicine-initiative-cohort-program/frequently-asked-questions-other-transaction-awards.

[11] See https://www.nih.gov/research-training/allofus-research-program/funding and https://www.nih.gov/sites/default/files/research-training/initiatives/pmi/20151118-ot-award-policy-guide.pdf.

[12] Under the FTC Act § 5, 15 U.S.C. § 45, https://www.law.cornell.edu/uscode/text/15/45, the privacy principles could be enforced by the Federal Trade Commission in certain circumstances, for example, when there was an unfair or a deceptive business practice. This type of enforcement is quite different than the affirmative rights conferred to

We do not know how the principles will be made operational. [13] An October 2, 2016, memorandum from the Office of Management and Budget requiring relevant agencies to develop privacy and security plans may ultimately help.[14] However, there is insufficient information on the public record to answer the most important questions. It is possible that the process started by OMB will eventually produce clarity on how privacy rules will apply to PMI. Whether the activities required by the OMB memo will be affected by the presidential transition in 2017 is unknown.

The issue that we raise in this report is how the PMI will actually protect privacy and what specific privacy laws apply. We consider different possible structures for the Initiative and evaluate how existing privacy laws may apply.

Organizational Structure of the PMI Data and Data Managers

Summary: The structure of the PMI program has an impact on how privacy protections function. This section reviews the privacy consequences of having a federal or a non-federal manager.

A major organizational decision with important implications for privacy in the PMI is who will hold the data and biospecimens and take responsibility for privacy. We recognize that there may be multiple databases (for patient data, for specimens, etc.), multiple data controllers, and different management and technical structures for the PMI. For example, the September 2015 report of a PMI Working Group includes this paragraph suggesting a hub-and-spoke model.

> To facilitate data access, data normalization, and participant engagement, the Working Group recommends that the PMI-CP follow a "hub-and-spoke" model that has a Coordinating Center to provide a single point of contact for coordinating data, biospecimens, participant communication and engagement, and research studies. The Working Group encourages NIH to consider novel collaborations with not-for-profit and commercial organizations to achieve state-of-the-art analysis methods, scientific rigor, elastic storage and compute capabilities, and technological expertise. For data storage and access, the Working Group

---

individuals under, for example, HIPAA. Further, FTC jurisdictional limits mean that many PMI research institutions are not subject to FTC enforcement powers.

[13] For example, a key PMI funding document does not discuss how to specifically implement the privacy principles. https://www.nih.gov/sites/default/files/research-training/initiatives/pmi/20151116-pmi-pilot-phase-studies-ota-sow.pdf. The document states "All partners in the President's PMI are expected to adhere to the PMI privacy and trust principles developed by the White House" with no substantive elaboration. The Genetic Information Nondiscrimination Act of 2008 is mentioned briefly, but its relevance is uncertain as we do not anticipate that the PMI Cohort Program will provide genetic information to health insurance companies or employers.

[14] Office of Management and Budget, Memorandum for the Heads of Executive Departments and Agencies, Precision Medicine Initiative Privacy and Security (October 21, 2016) (M-17-02), https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-02.pdf.

> recommends the PMI-CP pursue a hybrid data and analytics architecture that leverages both centralized data storage of core data while preserving federated access to additional data at the nodes across the network, as needed by specific studies. This hybrid model would accelerate execution of many research queries but still allow detailed data access for queries not addressable through the current data common data models.[15]

The current discussions of governance structure can be seen in Appendix C. To make our discussion here manageable, we make a simple assumption that there is a single manager for any PMI database, and that manager has responsibility for establishing privacy standards and for complying with any applicable privacy laws. Further, we assume that the PMI manager may either be a federal agency (e.g., NIH) or a non-federal agency (e.g., a federal contractor or grantee). The NIH has awarded a first round of grants for the PMI, including to Vanderbilt Medical Center for a pilot project.[16]

This discussion reviews the privacy consequences of having a federal or a non-federal manager.

HIPAA and the Precision Medicine Initiative: HIPAA Protections Will Not Apply to the PMI

Summary: HIPAA will not protect any data held by the PMI manager or used downstream by researchers.

The HIPAA privacy rule[17] applies to three categories of health care institutions: most health care providers, most health plans (insurers), and health care clearinghouses. These institutions are known as *HIPAA covered entities*. The HIPAA privacy rule does not apply to health information held by others. Thus, the rule does not cover any identifiable health information held by data brokers, websites, credit bureaus, disease registries, health researchers, disease advocacy organizations, law enforcement agencies, or others. This is true even if the information originated with a HIPAA covered entity. Once a HIPAA covered entity shares health information protected under HIPAA with anyone who is not a HIPAA covered entity, the information generally passes outside the scope of the HIPAA privacy rule and beyond the jurisdiction of HIPAA oversight and enforcement. This is true whether a federal agency or a private entity acquires HIPAA protected health information.

---

[15] Precision Medicine Initiative (PMI) Working Group Report to the Advisory Committee to the Director, National Institutes of Health, The Precision Medicine Initiative Cohort Program – Building a Research Foundation for 21st Century Medicine 4 (Sep. 17, 2015) (internal cross references omitted), http://acd.od.nih.gov/reports/DRAFT-PMI-WG-Report-9-11-2015-508.pdf.

[16] See "Funded Research" section, https://www.nih.gov/AllofUs-research-program/funding-opportunities.

[17] The Department of Health and Human Services issued the health privacy rule under the authority of the Health Insurance Portability and Accountability Act, Public Law 104-191. There are also HIPAA security and data breach rules, and these rules have the same applicability as the privacy rule. The focus here is only on the privacy rule. See generally http://www.hhs.gov/hipaa/for-professionals/index.html#1954.

The National Institutes of Health and HIPAA

The National Institutes of Health (NIH) is perhaps the only significant health care provider not subject to the HIPAA privacy rule. Why? "NIH does not meet the definition of a 'covered entity' and is therefore not covered by HIPAA because it does not bill for health care received at the Clinical Center." NIH buried this disclosure in a Frequently Asked Questions document from the NIH Senior Counsel for Privacy (March 2013) at page 4, question 16 ("Who can I contact if a person or organization covered by the Privacy Rule violates my health information privacy rights?").[18]

HHS could easily have written the HIPAA privacy rule to cover NIH but chose not to do so. If HIPAA applied to NIH, however, it would probably not matter for the PMI because PMI is not a treatment activity. NIH would almost certainly have defined itself as a *hybrid entity* under HIPAA so that its many non-treatment activities would fall outside of HIPAA. Many health care providers have functions that are not treatment activities. For example, a supermarket may be a hybrid entity, with a pharmacy that is a covered entity and its other activities not subject to HIPAA.[19]

Disclosures Allowable under HIPAA

Even if the HIPAA privacy rule applied to the PMI, its protections against disclosures leave much to be desired. For example, the rule allows six broad categories of disclosures of HIPAA protected health information for law enforcement purposes, with the most open-ended allowing disclosures in response to "administrative requests."[20] The rule's standards and procedures for these requests are weak, and a large number of federal, state, and local agencies qualify as law enforcement agencies. The HIPAA provision for national security disclosures has even weaker standards for disclosure. The rule allows unrestricted disclosures of health information to any national security or intelligence agency. HIPAA imposes no conditions or procedures prior to a national security disclosure. Any HIPAA-covered entity can, without violating HIPAA, disclose any patient information to a national security agency without a court order, without a subpoena, and, remarkably, even without a request from the agency.[21]

---

[18] National Institutes of Health, Frequently Asked Questions, Question 16 (Match 2013), ("Who can I contact if a person or organization covered by the Privacy Rule violates my health information privacy rights?"). https://oma.od.nih.gov/forms/Privacy Documents/Documents/NIH Privacy FAQs March 2013.pdf.

[19] For more detailed explanations about hybrid entities, see World Privacy Forum, *Patient's Guide to HIPAA, FAQ 9: Which Entities Must Comply with HIPAA?* https://www.worldprivacyforum.org/2013/09/hipaaguide9-2/ . For more on NIH and HIPAA see World Privacy Forum, *Patient's Guide to HIPAA, FAQ 3*: *What Laws are Relevant to Health Privacy*? https://www.worldprivacyforum.org/2013/09/hipaaguide3/ .

[20] 45 C.F.R. § 164.512(f)(1)(ii)(C).

[21] Comments of the World Privacy Forum for the Universal Periodic Review, UN Human Rights Council. *The Right to Health Privacy: Human Rights and the Surveillance and Interception of Medical and Health Records by Security Agencies*, October 14, 2014. http://www.worldprivacyforum.org/wp content/uploads/2014/10/WPF_UPR_UScomments_October2014_fs.pdf.

Will the Privacy Act of 1974 Protect the PMI Data?

Summary: The Privacy Act of 1974 applies only if a federal agency operates PMI. However, the Act's disclosure provisions allow agencies considerable authority to recognize new disclosures. In particular, the Act allows many types of disclosure to foreign, national, state, and local law enforcement agencies with few procedural prerequisites. We do not yet know what disclosure authority will apply to PMI records under the Privacy Act.

The Privacy Act of 1974[22] applies to federal agencies and some federal contractors. It does not apply to recipients of federal funds, federal grantees, or tax-exempt organizations. Thus, if a non-federal entity operates PMI, that entity is not subject to the Privacy Act of 1974, and the Act offers no protections to data subjects of the PMI.[23] In that case, the Act offers no protections to data subjects of PMI. We underscore that the Privacy Act of 1974 will not apply if NIH uses a grant instrument to fund PMI operations by a third party. Use of a contract rather than a grant does not assure application of the Privacy Act of 1974, and we think that a contract would not bring PMI activities under the Act.[24] We also note that in the currently funded PMI pilot programs the existing agreements appear not to be government contracts that could be subject to the Privacy Act.[25]

The Privacy Act of 1974 has good and bad elements. It implements all elements of Fair Information Practices,[26] but the Act is old and quite out-of-date. While many of its provisions provide useful privacy protections (e.g., access and correction rights, notice, and accountability), the Act's disclosure provisions have been controversial for decades.

If a federal agency maintains any health records for PMI, those records are subject to the Privacy Act of 1974 provided that 1) the records are under the control of the agency; and 2) the agency retrieves information by name, identifying number, or other identifying particular assigned to the

---

[22] 5 U.S.C. § 552a.

[23] If a federal agency used a contract to hire a non-federal entity, it is possible that the Privacy Act of 1974 could apply, but only if the contract provided for the maintenance of personal information *to accomplish an agency function*. 5 U.S.C. § 552a(m). However, it is highly unlikely that any federal funds used to support PMI would be conveyed by a contract. It is much more likely that a federal agency would use a grant instrument rather than a contract, and federal grantees are not subject to the Privacy Act of 1974.

[24] If a federal agency used a contract to hire a non-federal entity, it is possible that the Privacy Act of 1974 could apply, but only if the contract provided for the maintenance of personal information *to accomplish an agency function*. 5 U.S.C. § 552a(m). However, it is highly unlikely that any federal funds used to support PMI would be conveyed through a contract. It is much more likely that a federal agency would use a grant instrument rather than a contract, and federal grantees are not subject to the Privacy Act of 1974.

[25] https://www.nih.gov/AllofUs-research-program/frequently-asked-questions-other-transaction-awards.

[26] See generally Robert Gellman, *Fair Information Practices: A Basic History* (Version 2.15, 2015), http://bobgellman.com/rg-docs/rg-FIPshistory.pdf.

individual.[27] We do not see any loophole in the Privacy Act of 1974 that would allow any agency to maintain PMI health records without complying with the Act. However, if an agency avoided the Privacy Act of 1974 (e.g., by awarding a grant for operation of the PMI) then no general health privacy law would apply at all. All personal records would be usable and disclosable without statutory restrictions whatsoever. Needless to say, we do not see that as a good option.

If the Privacy Act of 1974 applies, however, we can guess how it might work. We assume here that if a federal agency operated PMI, that agency would be the National Institutes of Health. In order to assess how the Privacy Act of 1974 would apply, we can look at existing systems of records that NIH maintains and see how NIH can use and disclose those records.[28] The NIH already has a system of records that bears a lot of similarity to what we might expect for the PMI. That system is *Clinical Research: Candidate Healthy Volunteer Records*.[29] The system contains records on "normally healthy individuals who volunteer to participate in NIH studies."

We focus here on how an agency can use or disclose records for law enforcement purposes. The discussion, perhaps unfortunately, requires a review of the entrails of the Privacy Act. The Act's law enforcement disclosure provisions are better in some ways and worse in some way than the comparable provisions in the HIPAA health privacy rule.

There are several ways that the Privacy Act of 1974 authorizes agencies to disclose personal information. The statute itself sets out twelve "conditions of disclosure" that define allowable disclosures for all Privacy Act systems of records.[30] One class of allowable disclosures is:

> to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought.[31]

Under this authority, an agency may share any Privacy Act record with any federal, state, or local law enforcement agency upon written request by the head of the agency. Disclosures are not mandatory, and an agency need not disclose a requested record if it chooses not to do so. Still, the authority here is quite broad (any law enforcement activity "authorized by law"), tempered only by the procedural requirement that the request come from the head of the agency.

Another condition of disclosure of the Privacy Act allows an agency to disclose information pursuant to a *routine use*.[32] A routine use is a disclosure "compatible with the purpose for which

---

[27] See the definition of *system of records* at 5 U.S.C. § 552a(a)(5).
[28] A system of records is a group of agency records about individuals, and the Privacy Act of 1974 (for the most part) applies to systems of records. 5 U.S.C. § 552a(b)(5).
[29] https://oma.od.nih.gov/forms/Privacy%20Documents/PAfiles/0012.htm. Whether a collection of records is a *system of records* under the Privacy Act of 1974 turns on a *factual* test about retrievability.
[30] 5 U.S.C. § 552a(b).
[31] 5 U.S.C. § 552a(b)(7).
[32] 5 U.S.C. § 552a(b)(3).

[the record] was collected."[33] In modern privacy parlance, use generally refers to internal use by an organization that holds a record, and a disclosure means sharing a record with someone outside the organization. The Privacy Act is confusing in that a *routine use* is an external disclosure. An agency defines one or more routines uses for each system of records through a process similar to a rulemaking.[34]

The statutory standard for establishing a routine use is vague, and agencies often have expansive routine uses. Agencies frequently create routine uses to expand upon the disclosures for law enforcement purposes allowed by the statutory provision quoted above. The statutory provision just discussed requires a request from the head of the agency. Agencies have a routine use so they can initiate a disclosure without a request.

This type of routine use typically allows disclosures to federal and foreign law enforcement agencies if a record "indicates" any violation or potential violation of law. A similar routine use may allow disclosures to state and local law enforcement agencies. Here's an example.

> In the event that a system of records maintained by this agency or carry out its functions indicates a violation or potential violation of law, whether civil, criminal or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule or order issued pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the appropriate agency, whether federal, or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation or order issued pursuant thereto.[35]

Essentially, this routine use allows nearly standardless disclosure of any record to a civil or criminal law enforcement agency. Again, disclosures are discretionary and not mandatory. The authority, however, is quite broad. The routine use allows a disclosure in response to a request from an agency that does not meet the statutory condition of disclosure that requires a written request from the head of an agency.

This specific example of a law enforcement routine use quoted above comes from the agency-wide routine uses established by the Department of Health and Human Services. There are eight other HHS agency-wide routine uses covering other disclosures. Many agencies define agency-wide routine uses that apply to all agency systems of records for convenience. It is not entirely clear if the nine HHS routines uses applicable to more than one system of records actually apply to all agency records. Some legal details remain murky, and the specifics are not worth exploring here. Our best reading is that these apply to most HHS systems, including those maintained by NIH, which is a component of HHS. If NIH establishes a new system for PMI, it could define

---

[33] 5 U.S.C. § 552a(a)(7).
[34] 5 U.S.C. § 552a(3)(11).
[35] Department of Health and Human Services, Privacy Act Regulation, 45 C.F.R. Part 5b, Appendix B, Routine Uses Applicable to More Than One System of Records Maintained by HHS, http://www.ecfr.gov/cgi-bin/text-idx?SID=8391cb1e1e023df7b045749be77396c9&mc=true&node=pt45.1.5b&rgn=div5#ap45.1.5b_113.b.

routine uses for that system, and it might find a way to avoid some of the agency-wide routine uses established by HHS.

The point is that the Privacy Act of 1974 gives agencies broad authority to establish a basis for disclosing records from a Privacy Act system of records. Most agencies use that authority to provide for expansive law enforcement disclosures. This could happen to any PMI system. It is possible that disclosures could be even broader. Remember that the HIPAA health privacy rule promulgated by HHS allows disclosures of any health record to any national security agency without any standards or process. The same policy might (or might not) apply to PMI records.

Further, Congress can, without changing the Privacy Act of 1974, require agencies to disclose records for additional purposes, making those purposes legislatively compatible with the purpose for which the records were originally collected. For example, in the Personal Responsibility and Work Opportunity Reconciliation Act of 1996, Congress directed each federal agency to disclose some agency records to a directory of new hires aimed at finding individuals with outstanding child support obligations. The Office of Management and Budget directed each agency to establish a new routine use for its payroll records.[36] Under exigent political circumstances, Congress could make any federal record available for new law enforcement, national security, or other activity.[37]

The Privacy Act of 1974's provisions on use and disclosure leave much to be desired. As documented above, the Act allows many types of disclosures to foreign, national, state, and local law enforcement agencies with few procedural prerequisites. We will not know what disclosures will be allowed for PMI until we see a system of records notice for a PMI system. Developing a system of records notice and obtaining approval can take months, and there is no draft notice yet available.

Finally, we observe that the Privacy Act of 1974 applies to federal agencies. If an agency discloses a Privacy Act record to another federal agency, the record may end up in a different system of records subject to an entirely different set of routine uses. However, if an agency discloses a Privacy Act record to anyone other than a federal agency, the rules of the Privacy Act do not follow the record, and the record may be subject to another or to no privacy law at all. This is similar to the way that HIPAA works.

[36] See Sally Katzen, Administrator of the Office of Information and Regulatory Affairs, Office of Management and Budget, https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/inforeg/katzen_prwora.pdf (1997).
[37] Under HIPAA, stronger state laws take precedence, so if a state law prohibited a disclosure allowed by HIPAA, the disclosure would be illegal. This is not the case with the Privacy Act of 1974. If another law requires a disclosure, a federal agency just creates a new routine use.

Will Physician-Patient Privilege Survive if an Individual Donates their Health Records and Biospecimens to the PMI Database?

Summary: A patient who consents to the disclosure of health records to PMI could lose the ability to claim a physician-patient privilege to shield documents and information from disclosure in judicial proceedings.

The law in many states recognizes a physician-patient testimonial privilege that serves to protect patient privacy by limiting what a physician's ability to testify about confidential communications between the patient and the physician. The privilege exists in most states, and it varies considerably in scope, application, and exemption across the states.[38] While the privilege has a limited value in many ways, it can be protective of privacy at times. The details of state law privileges are beyond the scope of this analysis.

What is important here is that the privilege can be lost under different circumstances. For example, a privilege may be lost if an otherwise confidential communication happened in the presence of a third person. The privilege can be lost by disclosure of privileged information to a third party. If a patient consents to the disclosure of his health record, the privilege may be waived. Once waived the privilege is lost. In the case of PMI, where a patient consents to a health record disclosure to PMI and, perhaps to an unknown and indefinite number of researchers in the future, there may be a strong argument that the patient waived any available privilege.

Because the physician-patient privilege is statutory, it could be reshaped by law to preserve the privilege. Whether a federal law could accomplish this type of change to state law rules of evidence is uncertain. It is also uncertain if the PMI initiative plans to address the privilege issue, either through notice to those who volunteer their records or through legislative proposals. The PMI Privacy and Trust Principles state that "[m]easures for protecting PMI data from disclosure in civil, criminal, administrative, legislative, or other proceedings should be explored." That suggestion does not appear to address clearly the privilege issue, an issue that affects records in their original location and not records in the hands of PMI. In any event, a promise to explore the issue at some indefinite time in the future has little value today.

[38] See generally, Robert Gellman, *Prescribing Privacy: The Uncertain Role of the Physician in the Protection of Patient Privacy*, 62 North Carolina Law Review 255 (1984), http://scholarship.law.unc.edu/cgi/viewcontent.cgi?article=2944&context=nclr.

Will the Legal Protections Afforded to Alcohol and Drug Abuse Patient Records Apply to the PMI Database?

Summary: Records disclosed to PMI from health care providers subject to federal substance abuse confidentiality rules would retain their confidentiality if disclosed to PMI.

A separate privacy regime applies to records maintained by most alcohol and drug abuse health care providers. The Substance Abuse and Mental Health Services Administration (SAMHSA) maintains the Confidentiality of Alcohol and Drug Abuse Patient Records regulations.[39] The rules are often referred to as *Part 2*.

The Part 2 rules have perhaps the strictest privacy rules of any American privacy law. The rationale is that patients in substance abuse programs may seek treatment for activities that violate drug abuse or other laws. Without some protections against law enforcement access to the records, patients might refuse to seek treatment. The Part 2 rules impose meaningful limits on disclosures to law enforcement by health care providers subject to Part 2. The details are beyond the scope of this analysis. However, it is unquestionable that the Part 2 protections against law enforcement disclosure are much better than those available under either HIPAA or the Privacy Act of 1974.

Part 2 has another interesting provision absent from the other laws already discussed. The Part 2 rules generally follow the record when disclosed by a substance abuse program. This means that the sensitive information in the record remains protected despite its disclosure. This may be the only American privacy law where privacy rules follow the records. Remarkably, this policy applies even when a patient consents to the disclosure of the patient's record.[40]

If a patient agrees to the disclosure of a HIPAA record to PMI, the HIPAA rules do not accompany the disclosure unless the record goes to a covered entity subject to HIPAA. If a patient agrees to the disclosure of a Privacy Act of 1974 record, the privacy rules of the Act may apply (but in different ways) if the recipient is a federal agency, but the privacy rules do not apply if the recipient is not a federal agency. However, if a patient consents to the disclosure to the PMI of substance abuse records subject to Part 2, the Part 2 restrictions follow the record. Needless to say, this presents significant administrative challenges when a recipient accepts Part

[39] 42 C.F.R. Part 2. SAMHSA is in the process of revising the rules. See 81 Federal Register 6988 (February 9, 2016), https://www.gpo.gov/fdsys/pkg/FR-2016-02-09/pdf/2016-01841.pdf. SAMHSA issued a final rule on January 18, 2017, 82 Federal Register 6052, https://www.federalregister.gov/d/2017-00742, but the revised rule does not appear to change the analysis presented in this report.

[40] 42 C.F.R. § 2.32. The notice that accompanies a disclosed record must include this statement: "This information has been disclosed to you from records protected by Federal confidentiality rules (42 CFR Part 2). The Federal rules prohibit you from making any further disclosure of this information unless further disclosure is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted by 42 CFR Part 2. A general authorization for the release of medical or other information is NOT sufficient for this purpose. The Federal rules restrict any use of the information to criminally investigate or prosecute any alcohol or drug abuse patient."

2 records because the applicable confidentiality regime is different and stricter than any other potentially applicable law.

Do Certificates of Confidentiality Provide Enough Protection for PMI Data and Biospecimen Donors?

Summary: Certificates of confidentiality provide researchers a defense against compelled disclosures. While there are some uncertainties about the value of certificates, PMI data covered by a certificate would likely have some protection against subpoenas and the like. The recently enacted 21st Century Cures Act will resolve some of the uncertainties.

A certificate of confidentiality authorized by some federal statutes provides some protection against compelled disclosure of records held by researchers. The certificate authorizes a researcher to resist compulsory legal demands (such as a court order or subpoena) for identifiable research information about individuals. The Public Health Service Act establishes one of the broadest certificate programs.[41] The law allows the Secretary of HHS to issue a certificate of confidentiality not only to federally-supported research, but to other research as well. The Secretary requires that a research project seeking a certification obtain institutional review board approval of the research protocol.

PMI records used by researchers – and the PMI records themselves held by a PMI manager – could well qualify a certificate of confidentiality. NIH operates the certificate program, and there seems little doubt that it could lawfully grant certificates for many PMI data activities. If so, then certificates of confidentiality would provide a degree of protection against compelled disclosure.

The actual value of a certificate is questionable, however. First, it protects against *compelled* disclosures, but it say nothing about volunteered disclosures. A researcher faced with a long,

---

[41] 42 U.S.C. § 241(d) ("The Secretary [of Health and Human Services] may authorize persons engaged in biomedical, behavioral, clinical, or other research (including research on mental health, including research on the use and effect of alcohol and other psychoactive drugs) to protect the privacy of individuals who are the subject of such research by withholding from all persons not connected with the conduct of such research the names or other identifying characteristics of such individuals. Persons so authorized to protect the privacy of such individuals may not be compelled in any Federal, State, or local civil, criminal, administrative, legislative, or other proceedings to identify such individuals."). These certificates are available on project-by-project basis from NIH, the Food and Drug Administration, the Substance Abuse and Mental Health Services Administration, the Centers for Disease Control, the Indian Health Service, and the Health Resources and Services Administration. For more information on certificates and the process for obtaining them, see NIH's Certificates of Confidentiality Kiosk at https://humansubjects.nih.gov/coc/index.

Other statutes that provide for certificates of confidentiality or the equivalent include: 42 U.S.C. § 242m(d); 42 U.S.C. § 299c-3(c); 42 U.S.C. § 290aa(n); 42 U.S.C. § 3789g(a); 42 U.S.C. § 10604(d); and 44 U.S.C. § 3501 note. Some state laws may also provide comparable protections for some research activities.

expensive, and unfunded battle to protect records could voluntarily disclose the records and avoid the battle altogether. Second, and similarly, a certificate holder is not required to resist demands for records. The law provides that certificate holders are *authorized* to resist demands, but they are not compelled to do so. Third, the actual value of the certificate of confidentiality is somewhat in doubt. The uncertainty is wonderfully summarized in a recent journal article that provides examples of cases where a court meaningfully upheld a certificate or essentially disregarded it.[42] The lesson is that you do not know the value of a certificate until a judge issues a ruling in a particular case before a court. Fourth, certificates are only available for research activities. If PMI allows or tolerates non-research uses of PMI data, a certificate may not be available or may offer no protection.

The shortcomings of laws establishing certificate of confidentiality programs are beyond the scope of this analysis. However, it is probably fair to assume that NIH would take steps to place most or all PMI activities under certificate protection. NIH could also require those using PMI data to sign a data use agreement compelling users to resist compelled disclosures and to refuse to make voluntary disclosures (at least those without data subject consent). If so, then research activities that receive certificates would be in a better position to protect the records against compelled disclosure. Without certificates, however, PMI records could be vulnerable just like any other record to compelled disclosure for civil and criminal purposes. Still, the value of a certificate remains uncertain and could vary from case to case as happened in the past.

Enacted at the end of 2016, the 21st Century Cures Act[43] may resolve some of the uncertainties identified here. The Act directs changes to certificate programs that will broaden availability of certificates and strengthen the protections for patient records, including the protection against compelled disclosure of records covered by a certificate.[44] While a stronger certificate of

---

[42] Leslie E. Wolf, Mayank J. Patel, Brett A. Williams, Jeffrey L. Austin, Lauren A. Dame, Certificates of Confidentiality: Protecting Human Subject Research Data in Law and Practice, 14 Minnesota Journal of Law, Science, and Technology 11 (2013). http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2217833.

[43] Act of December 13, 2016, Public Law 114-255.

[44] The text of the new certificate provision is:

SEC. 2012. PRIVACY PROTECTION FOR HUMAN RESEARCH SUBJECTS.

(a) IN GENERAL.—Subsection (d) of section 301 of the Public Health Service Act (42 U.S.C. 241) is amended to read as follows:

> (d)(1)(A) If a person is engaged in biomedical, behavioral, clinical, or other research, in which identifiable, sensitive information is collected (including research on mental health and research on the use and effect of alcohol and other psychoactive drugs), the Secretary, in coordination with other agencies, as applicable—
>
> (i) shall issue to such person a certificate of confidentiality to protect the privacy of individuals who are the subjects of such research if the research is funded wholly or in part by the Federal Government; and
>
> (ii) may, upon application by a person engaged in research, issue to such person a certificate of confidentiality to protect the privacy of such individuals if the research is not so funded.
>
> (B) Except as provided in subparagraph (C), any person to whom a certificate is issued under subparagraph (A) to protect the privacy of individuals described in such subparagraph shall not disclose or provide to any other person not connected with the research the name of such an individual or any information, document, or biospecimen that contains identifiable, sensitive information about such an individual and that was created or compiled for purposes of the research.

confidentiality for research is welcome, certificates of confidentiality are not a complete privacy rule, and other uncertainties about privacy requirements for PMI records remain.

(C) The disclosure prohibition in subparagraph (B) shall not apply to disclosure or use that is—

(i) required by Federal, State, or local laws, excluding instances described in subparagraph (D);

(ii) necessary for the medical treatment of the individual to whom the information, document, or biospecimen pertains and made with the consent of such individual;

(iii) made with the consent of the individual to whom the information, document, or biospecimen pertains; or

(iv) made for the purposes of other scientific research that is in compliance with applicable Federal regulations governing the protection of human subjects in research.

(D) Any person to whom a certificate is issued under subparagraph (A) to protect the privacy of an individual described in such subparagraph shall not, in any Federal, State, or local civil, criminal, administrative, legislative, or other proceeding, disclose or provide the name of such individual or any such information, document, or biospecimen that contains identifiable, sensitive information about the individual and that was created or compiled for purposes of the research, except in the circumstance described in subparagraph (C)(iii).

(E) Identifiable, sensitive information protected under subparagraph (A), and all copies thereof, shall be immune from the legal process, and shall not, without the consent of the individual to whom the information pertains, be admissible as evidence or used for any purpose in any action, suit, or other judicial, legislative, or administrative proceeding.

(F) Identifiable, sensitive information collected by a person to whom a certificate has been issued under subparagraph (A), and all copies thereof, shall be subject to the protections afforded by this section for perpetuity.

(G) The Secretary shall take steps to minimize the burden to researchers, streamline the process, and reduce the time it takes to comply with the requirements of this subsection.

(2) The Secretary shall coordinate with the heads of other applicable Federal agencies to ensure that such departments have policies in place with respect to the issuance of a certificate of confidentiality pursuant to paragraph (1) and other requirements of this subsection.

(3) Nothing in this subsection shall be construed to limit the access of an individual who is a subject of research to information about himself or herself collected during such individual's participation in the research.

(4) For purposes of this subsection, the term 'identifiable, sensitive information' means information that is about an individual and that is gathered or used during the course of research described in paragraph (1)(A) and—

(A) through which an individual is identified; or

(B) for which there is at least a very small risk, as determined by current scientific practices or statistical methods, that some combination of the information, a request for the information, and other available data sources could be used to deduce the identity of an individual.

(b) APPLICABILITY.—Beginning 180 days after the date of enactment of this Act, all persons engaged in research and authorized by the Secretary of Health and Human Services to protect information under section 301(d) of the Public Health Service Act (42 U.S.C. 241(d)) prior to the date of enactment of this Act shall be subject to the requirements of such section (as amended by this Act).

Issues Relating to Consensual Disclosures

Summary: Third parties may seek access to PMI health records with the consent of the data subjects. PMI rules governing third party access are unknown.

Under some circumstances, individuals give consent for the sharing of their health records with third parties. With an appropriately signed consent form, health record holders, including HIPAA covered entities, can share records with those third parties.[45] PMI records may be attractive to some users and more preferable than other health records. Much will depend on the scope and currency of the records. For example, someone may seek PMI records rather than other records about a patient if PMI collects in one place records from diverse sources and multiple health care providers. PMI may also have records that are unavailable from the original source in some cases.

For example, an individual seeking a security clearance in order to have access to classified information must sign a broad consent form allowing any source of information about the individual to disclose the information with a federal investigator. In addition, the applicant for a security clearance signs a specific authorization consistent with HIPAA.[46] The consent granted under Standard Form 86 (Questionnaire for National Security Positions) appears broad enough to cover records held by PMI.

For example, an individual applying for life insurance is typically signs a broad consent form that allows disclosure of personal information from both HIPAA and non-HIPAA sources. If the consent form currently in use is not broad enough to cover PMI, it could be easily amended. The advantage to insurers might be a faster response and obtaining in one place records that originated from more than one source.

Whether PMI would respond to requests from third parties armed with data subject consents is unknown. There are good arguments for and against allowing consensual disclosures to third parties. Data subject access is a basic privacy practice and part of the PMI Privacy and Trust Principles. The details of how access would be provided remain unknown. If PMI followed the policy in the HIPAA privacy rule, it might well allow third parties to exercise the access right that an individual has with the consent of the individual.[47] The Privacy Act of 1974 provides for data subject access, but it is not clear if that access right can be exercised by a third party with consent. The Act provides that an individual inspecting personal records can bring a third party to accompany him.[48] We do not know which, if any, existing model the PMI would follow.

---

[45] HIPAA allows disclosures with an authorization from the patient. 45 C.F.R. § 164.508. Under a separate procedure, a patient's may designate another person to have a copy of his record under the provision that allows a patient access to his own record, and a covered entity must disclose the record. 45 C.F.R. §528(c)(3)(ii). The Privacy Act of 1974 allows disclosures pursuant to a written request from the data subject. 5 U.S.C. 552a(b).
[46] Standard Form 86 (2010) at page 21, https://www.opm.gov/forms/pdf_fill/sf86-non508.pdf.
[47] 45 C.F.R. §528(c)(3)(ii).
[48] 5 U.S.C. § 552a(d)(1).

The creation of any new compilation of information may bring with it new and possibly unexpected requests and demands for access to the information. Remote data users may find value in an information resource and, when armed with individual consent, may seek records that they might not be able to obtain otherwise. Consider, for example, if a direct marketer or database vendor, found a way to induce an individual to share access to that individual's health record. Without a clearly stated set of rules and policies, the availability of records in PMI will remain uncertain and patient privacy could be threatened.

The 21st Century Cures Act Does Not Solve the Privacy Problem with PMI

Section 2011 of the 21st Century Cures Act[49] adds a new section to the Public Health Service Act[50] addressing the Precision Medicine Initiative. In general, the new section[51] authorizes[52] the

[49] Act of December 13, 2016, Public law 114-255. The text of the Act appears at https://www.congress.gov/114/bills/hr34/BILLS-114hr34enr.pdf.

[50] 42 U.S.C. § 289 et seq., https://www.law.cornell.edu/uscode/text/42/289.

[51] The full text of the provision is:

42 U.S.C. § 498E. PRECISION MEDICINE INITIATIVE.

(a) IN GENERAL.—The Secretary is encouraged to establish and carry out an initiative, to be known as the 'Precision Medicine Initiative' (in this section referred to as the 'Initiative'), to augment efforts to address disease prevention, diagnosis, and treatment.

(b) COMPONENTS.—The Initiative described under subsection (a) may include—

(1) developing a network of scientists to assist in carrying out the purposes of the Initiative;

(2) developing new approaches for addressing scientific, medical, public health, and regulatory science issues;

(3) applying genomic technologies, such as whole genomic sequencing, to provide data on the molecular basis of disease;

(4) collecting information voluntarily provided by a diverse cohort of individuals that can be used to better understand health and disease; and

(5) other activities to advance the goals of the Initiative, as the Secretary determines appropriate.

(c) AUTHORITY OF THE SECRETARY.—In carrying out this section, the Secretary may—

(1) coordinate with the Secretary of Energy, private industry, and others, as the Secretary determines appropriate, to identify and address the advanced supercomputing and other advanced technology needs for the Initiative;

(2) develop and utilize public-private partnerships; and

(3) leverage existing data sources.

(d) REQUIREMENTS.—In the implementation of the Initiative under subsection (a), the Secretary shall—

(1) ensure the collaboration of the National Institutes of Health, the Food and Drug Administration, the Office of the National Coordinator for Health Information Technology, and the Office for Civil Rights of the Department of Health and Human Services;

(2) comply with existing laws and regulations for the protection of human subjects involved in research, including the protection of participant privacy;

(3) implement policies and mechanisms for appropriate secure data sharing across systems that include protections for privacy and security of data;

(4) consider the diversity of the cohort to ensure inclusion of a broad range of participants, including consideration of biological, social, and other determinants of health that contribute to health disparities;

(5) ensure that only authorized individuals may access controlled or sensitive, identifiable biological material and associated information collected or stored in connection with the Initiative; and

(6) on the appropriate Internet website of the Department of Health and Human Services, identify any entities with access to such information and provide information with respect to the purpose of such access, a

Secretary of HHS to establish and carry out a PMI initiative to "augment efforts to address disease prevention, diagnosis, and treatment."

The main issue raised in original May 2016 version of this report is what privacy law applies to the PMI. In a nutshell, the original conclusion was that it was not clear what privacy law or whether any privacy law applies to the PMI itself or to any activities conducted under the PMI. The actual answer depends on the structure of the PMI and who carries out activities under the PMI. No information available on the public record provides a clear answer.

The new legislation has a privacy provision, but it does not establish standards or apply any existing law to PMI information or activities. The new language says that in implementing the program, the Secretary shall

> (2) comply with existing laws and regulations for the protection of human subjects involved in research, including the protection of participant privacy.[53]

Human subjects protection rules will also certainly apply to some and perhaps all of the research conducted by researchers using PMI data. The Common Rule contains the main human subject protection rules for federal and federally sponsored research.[54] The Common Rule does little to address privacy rights and interests of individuals. The only provision directly mentioning privacy requires Institutional Review Boards (IRBs) to determine that research projects meet specified requirements, including:

> (7) When appropriate, there are adequate provisions to protect the privacy of subjects and to maintain the confidentiality of data.

It is generally beyond the ability of IRBs to determine the privacy rights of individuals with respect to the main elements of privacy reflected in HIPAA or in basic privacy standards found in Fair Information Practices. At best, human subject protection rules as currently implemented offer incomplete privacy protections, and the protections can vary depending on how individual

---

summary of the research project for which such access is granted, as applicable, and a description of the biological material and associated information to which the entity has access.
(e) REPORT.—Not later than 1 year after the date of enactment of the 21st Century Cures Act, the Secretary shall submit a report on the relevant data access policies and procedures to the Committee on Health, Education, Labor, and Pensions of the Senate and the Committee on Energy and Commerce of the House of Representatives. Such report shall include steps the Secretary has taken to consult with experts or other heads of departments or agencies of the Federal Government in the development of such policies.

[52] It is technically not an authorization in the usual legislative sense. The exact words of the statute are "The Secretary is encouraged to establish and carry out an initiative…." 42 U.S.C. § 498E(a). Presumably, a Secretary could decide not to carry out the PMI because there is no requirement to do so in the new law. However, any PMI initiative must comply with the mandatory requirements in subsection (d). There seems to be enough wiggle room in the law so that the Secretary could establish a similar or different initiative that is not the PMI and conduct that similar initiative without regard to the authority and requirements of the 21st Century Cures Act. The PMI itself originated during the Obama Administration without any express legislation direction or specific authority.

[53] 42 U.S.C. § 498E(d).

[54] 45 C.F.R. Part 46, http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title45/45cfr46_main_02.tpl.

IRBs require research projects to implement the Common Rule's general requirement and on how research projects follow the dictates of IRBs.[55]

There are three other provisions in the new section that address privacy somewhat, but they do not answer any of the questions raised here. Paragraph (d)(3) says that policies and mechanisms for data sharing across systems must include protections for privacy and security of data. It does not say which, if any, existing protections apply. Paragraph (d)(5) says that the PMI must ensure that only authorized individuals may access controlled or sensitive biological material and associated information. All privacy and security regimes include access restrictions, but it remains unclear which regime, if any, applies. Finally, paragraph (d)(6) requires the Secretary to identify on a website who has access to PMI information and why. That requirement says nothing about which privacy rules apply to recipients of data. It remains possible that no privacy law may apply.

Notwithstanding the requirement in the Act that the PMI comply with privacy rules for the protection of human subjects, we still do not know which privacy laws or regulations apply because the new law does not expressly apply HIPAA, the Privacy Act of 1974, or any other existing law or regulation. It merely says that the program must "comply with existing laws and regulations" for the protection of human subjects, including the protection of privacy. Under that broad framework, any of the laws discussed in this report might apply depending on the structure of the PMI and who carries out its activities.

The 21st Century Cures Act also strengthened one of the federal laws addressing human subjects protection for research on mental health and use of the use and effect of alcohol and other psychoactive drugs.[56] We do not know how or if these rules will apply to PMI, but it seems likely that the rules will apply to some but not all PMI records.

---

[55] The federal departments and agencies responsible for the Common Rule published a notice of proposed rulemaking to amend the Common Rule and strengthen privacy and security protections for covered research activities. The proposal appeared in the Federal Register in September 2015, https://www.federalregister.gov/documents/2015/09/08/2015-21756/federal-policy-for-the-protection-of-human-subjects. See World Privacy Forum comments on the NPRM at https://www.worldprivacyforum.org/2016/01/wpf-files-comments-on-federal-proposal-for-human-subject-research-common-rule/. The Department of Health and Human Services, along with other federal agencies, changed the Common Rule in January 2017, just before the end of the Obama Administration. 82 Federal Register 7149 (January 19, 2017), https://www.federalregister.gov/documents/2017/01/19/2017-01058/federal-policy-for-the-protection-of-human-subjects. Based on a limited review of the revised Common Rule (which mostly does not take effect until January 2018), it does not appear that the revision affect the conclusions of this report.

[56] As amended by section 2012 of the 21st Century Cures Act, 42 U.S.C. § 241 will read:
(d)(1)(A) If a person is engaged in biomedical, behavioral, clinical, or other research, in which identifiable, sensitive information is collected (including research on mental health and research on the use and effect of alcohol and other psychoactive drugs), the Secretary, in coordination with other agencies, as applicable—

(i) shall issue to such person a certificate of confidentiality to protect the privacy of individuals who are the subjects of such research if the research is funded wholly or in part by the Federal Government; and

(ii) may, upon application by a person engaged in research, issue to such person a certificate of confidentiality to protect the privacy of such individuals if the research is not so funded.

(B) Except as provided in subparagraph (C), any person to whom a certificate is issued under subparagraph (A) to protect the privacy of individuals described in such subparagraph shall not disclose or provide to any other person not connected with the research the name of such an individual or any information, document, or

Part III: Recommendations

1. The PMI needs to detail its structure and organization with clarity so that the privacy protections or lack of privacy protections for its records can be assessed. The public needs to know what institutions will maintain information in the PMI and where they are located. The PMI must explain how privacy laws, if any, will apply to it. The privacy and

---

biospecimen that contains identifiable, sensitive information about such an individual and that was created or compiled for purposes of the research.

(C) The disclosure prohibition in subparagraph (B) shall not apply to disclosure or use that is—

(i) required by Federal, State, or local laws, excluding instances described in subparagraph (D);

(ii) necessary for the medical treatment of the individual to whom the information, document, or biospecimen pertains and made with the consent of such individual;

(iii) made with the consent of the individual to whom the information, document, or biospecimen pertains; or

(iv) made for the purposes of other scientific research that is in compliance with applicable Federal regulations governing the protection of human subjects in research.

(D) Any person to whom a certificate is issued under subparagraph (A) to protect the privacy of an individual described in such subparagraph shall not, in any Federal, State, or local civil, criminal, administrative, legislative, or other proceeding, disclose or provide the name of such individual or any such information, document, or biospecimen that contains identifiable, sensitive information about the individual and that was created or compiled for purposes of the research, except in the circumstance described in subparagraph (C)(iii).

(E) Identifiable, sensitive information protected under subparagraph (A), and all copies thereof, shall be immune from the legal process, and shall not, without the consent of the individual to whom the information pertains, be admissible as evidence or used for any purpose in any action, suit, or other judicial, legislative, or administrative proceeding.

(F) Identifiable, sensitive information collected by a person to whom a certificate has been issued under subparagraph (A), and all copies thereof, shall be subject to the protections afforded by this section for perpetuity.

(G) The Secretary shall take steps to minimize the burden to researchers, streamline the process, and reduce the time it takes to comply with the requirements of this subsection.

(2) The Secretary shall coordinate with the heads of other applicable Federal agencies to ensure that such departments have policies in place with respect to the issuance of a certificate of confidentiality pursuant to paragraph (1) and other requirements of this subsection.

(3) Nothing in this subsection shall be construed to limit the access of an individual who is a subject of research to information about himself or herself collected during such individual's participation in the research.

(4) For purposes of this subsection, the term 'identifiable, sensitive information' means information that is about an individual and that is gathered or used during the course of research described in paragraph (1)(A) and—

(A) through which an individual is identified; or

(B) for which there is at least a very small risk, as determined by current scientific practices or statistical methods, that some combination of the information, a request for the information, and other available data sources could be used to deduce the identity of an individual.''.

(b) APPLICABILITY.—Beginning 180 days after the date of enactment of this Act, all persons engaged in research and authorized by the Secretary of Health and Human Services to protect information under section 301(d) of the Public Health Service Act (42 U.S.C. 241(d)) prior to the date of enactment of this Act shall be subject to the requirements of such section (as amended by this Act).

security standards issued so far do not answer the questions about what legal protections will apply.

2. The PMI should not begin soliciting information or biospecimens from or about individuals until it clearly describes the applicable privacy protections. The description should include potential uses and disclosures of PMI information for law enforcement and national security purposes. The description of applicable privacy rules should cover health records, administrative records, and any real-time monitoring from mobile or other devices. Volunteers should be told expressly if HIPAA does not apply to the PMI.

3. The E-Government Act of 2002 requires agencies to conduct a Privacy Impact Assessment before they develop or procure information technology systems or projects that collect, maintain or disseminate information in identifiable form from or about members of the public.[57] We have not seen a PIA for the PMI. There is an immediate need for a PIA that includes an opportunity for public comment and debate.

4. If the Privacy Act of 1974 applies to PMI or any significant part of it, then the National Institutes of Health should publish a system of records notice and allow adequate time for public comment

5. If the Privacy Act of 1974 does not apply to PMI, then it is possible that no health privacy or other privacy law will apply to most of the data or biospecimens. As a result, the data could be vulnerable to a host of unrelated public and private demands and activities. If so, then PMI may need its own privacy law in place before it starts.

Conclusion

Creating a national database of health and genetic information for medical research is a laudable goal. However, creating a large new health information database and biomedical data ecosystem without clear, enforceable privacy laws and rules that protect individuals' medical data and gives them enforceable rights has the potential for negative consequences for individual donors. Sloppy use and disclosure of PMI records could also damage the PMI effort itself. Privacy principles are fine, but they are not the law. Privacy principles do not provide volunteers with firm and enforceable legal protections.

Privacy is a complex, multi-layered issue and encompasses many aspects of choice, autonomy, and fair information practices. PMI volunteers will be much more likely to provide their health information and biomedical datasets in support of the long-term goals of medical research if they have enforceable legal privacy protections.

[57] See Office of Management and Budget, Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (2003)(M-03-22), https://obamawhitehouse.archives.gov/omb/memoranda_m03-22/.

About this Report and Credits

Authors: Robert Gellman, privacy consultant, and Pam Dixon, Executive Director, World Privacy Forum.

Editing, proofing, and reading: Tim Sparapani, Linda Ackerman.

Cover illustration: for Second Edition: John Emerson, Backspace

Publication date for Second Edition: March 2017. First edition published May 2016.

Published at www.worldprivacyforum.org.

URL for Second Edition (March 2017): https://www.worldprivacyforum.org/2017/03/report-privacy-the-precision-medicine-initiative-and-all-of-us-research-program-will-any-legal-protections-apply/

Archival URL, first edition (May 2016): https://www.worldprivacyforum.org/2016/05/wpf-report-the-precision-medicine-initiative-what-laws-apply/

Background information and research for this report was collected from extensive public, official sources available regarding the PMI and the About Us research program.

Appendix A: Timeline of the Precision Medicine Initiative

Chronology of PMI/All of Us research program from January 2015-March 2017.

Jan. 20, 2015: President Obama announced the Precision Medicine Initiative in his State of the Union Address.

Jan. 30, 2015: White House event with patients, advocates, scientists, and industry leaders. President Obama shared his vision for the Initiative to enhance innovation in biomedical research with the ultimate goal of moving the U.S. into an era where medical treatment can be tailored to each patient.

Feb. 11-12, 2015: National Institutes of Health conducts the first workshop on PMI.

March 30, 2015: ACD PMI working group established.

April 28-29, 2015: Public Workshop on Unique Scientific Opportunities for the National Research Cohort Workshop (NIH).

May 5, 2015: Senate hearing, Continuing America's Leadership: Realizing the Promise of Precision Medicine for Patients.

May 28-29, 2015: Digital Health Data in a Million-Person PMI Cohort Workshop (Vanderbilt University).

July 1-2 2015: Participant Engagement and Health Equity Workshop (NIH).

July 27-28, 2015: Mobile Technologies in a Precision Medicine Initiative Cohort (Intel).

Sept. 17, 2015: ACD PMI Working Group Report.

Sept. 25, 2015: NIH Stakeholder Briefing on the PMI Working Group Final Report.

Dec. 17, 2015: PMI Cohort Program Advisory Panel Meeting.

Jan. 14, 2016: Pre-Application Technical Assistance Webinar for the Precision Medicine Initiative (PMI) Cohort Program Requests for Applications.

Jan. 15, 2016: PMI Cohort Program Advisory Panel Meeting.

Feb. 2016: Vanderbilt University Medical Center is announced as first PMI funding recipient.

Summer 2016: The NIH announces it will award cooperative agreements for the full implementation phase of the PMI. This includes establishing a coordinating center to oversee direct volunteer recruitment, healthcare provider organizations to enroll more participants, and a Biobank capable of storing and managing blood, urine and saliva samples for analysis. (http://news.vanderbilt.edu/2016/02/vumc-to-lead-pilot-program-for-precision-medicine-initiative-cohort-program/).

September 27, 2016: NIH funds Precision Medicine Consortium programs, California Precision Medicine Consortium, New England PMC, Trans American Consortium for the Health Care Systems Research Network, Henry Ford Health System, and Geisinger Health System. See https://www.nih.gov/research-training/precision-medicine-initiative/funding.

October 2016: PMI Cohort Program changes name to ***All of Us Research Program***. https://www.nih.gov/AllofUs-research-program/pmi-cohort-program-announces-new-name-all-us-research-program.

October 21, 2016: The Office of Management and Budget issues a memorandum on PMI to all agencies titled *Precision Medicine Initiative Privacy and Security*, https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-02.pdf.. The memo directs agencies involved in the PMI to address, as appropriate, the PMI Privacy and Trust Principles and the PMI Security Framework. Among other things, the memo assigns Senior Agency Officials for Privacy (SAOP) are to be lead points of contact on developing an agency plan for implementing privacy and security requirements.

January 11, 2017: All of Us Research Program Advisory Panel Meeting. (PMI Cohort Program) https://www.nih.gov/allofus-research-program/events.

February 2017: All of Us Research Program announces funding opportunity for community partners. https://www.nih.gov/news-events/news-releases/all-us-research-program-announces-funding-opportunity-community-partners.

February 22, 2017: All of Us Research Program names a "Chief Engagement Officer" for the All of Us Research Program. **"**All of Us aims to build one of the largest biomedical data sets in the world, involving participants from diverse communities across the United States.**"** https://www.nih.gov/research-training/allofus-research-program/dara-richardson-heron-md-named-chief-engagement-officer-all-us-research-program.

March 6-7, 2017: Return of genetic results for the All of Us Research Program. https://www.nih.gov/sites/default/files/research-training/initiatives/pmi/return-of-results-agenda-0306-0717.pdf.

2017: Planned: ~79,000 engaged participants fully consented and enrolled in the Cohort and collection of biospecimens from at least 25,000 participants.

Appendix B: Donated Information from Individuals and Patients

Participants in the PMI will donate a variety of information, including blood and other biospecimen samples, along with health records and other data, see Illustration 1. Early discussions planned for additional data collections that include geolocation, cell phone data, social networking data, and potentially even over-the-counter medication purchases. See Illustration 2. As of 2017, discussions continue regarding the eventuality of adding the datasets outlined in Illustration 2, with continuing discussion of sensors and data from mobile phones.

1. Initial core data set to be collected from volunteers

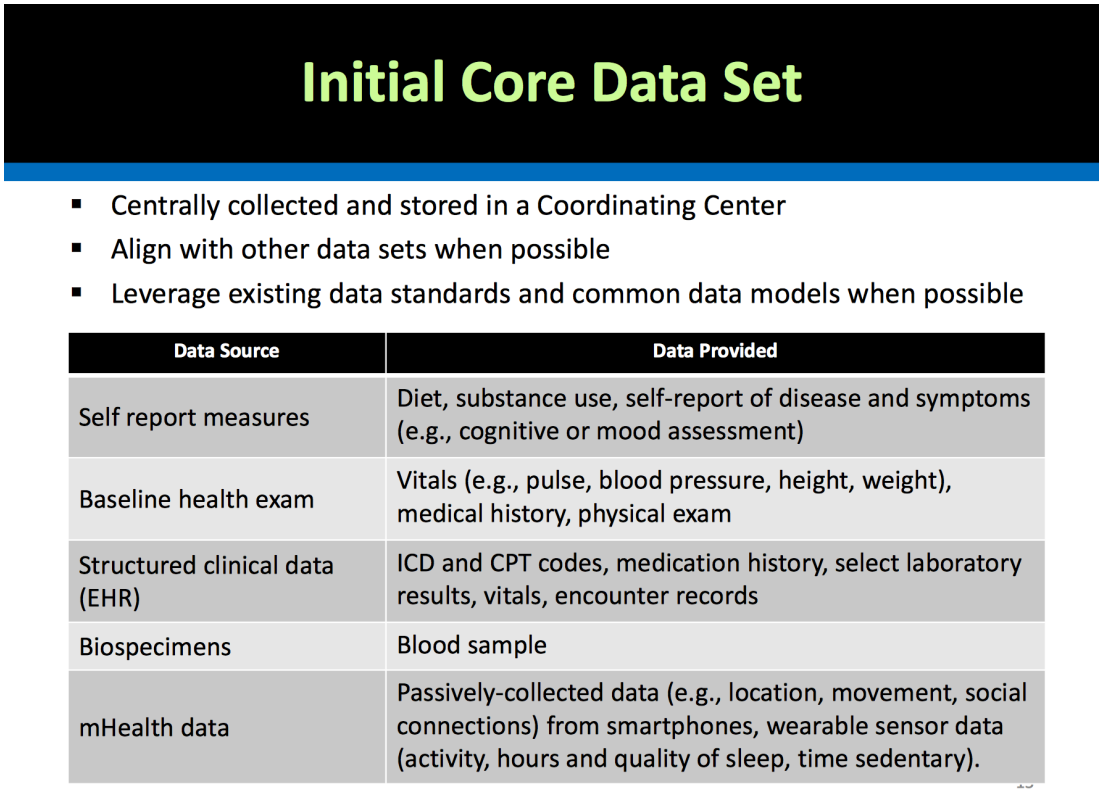
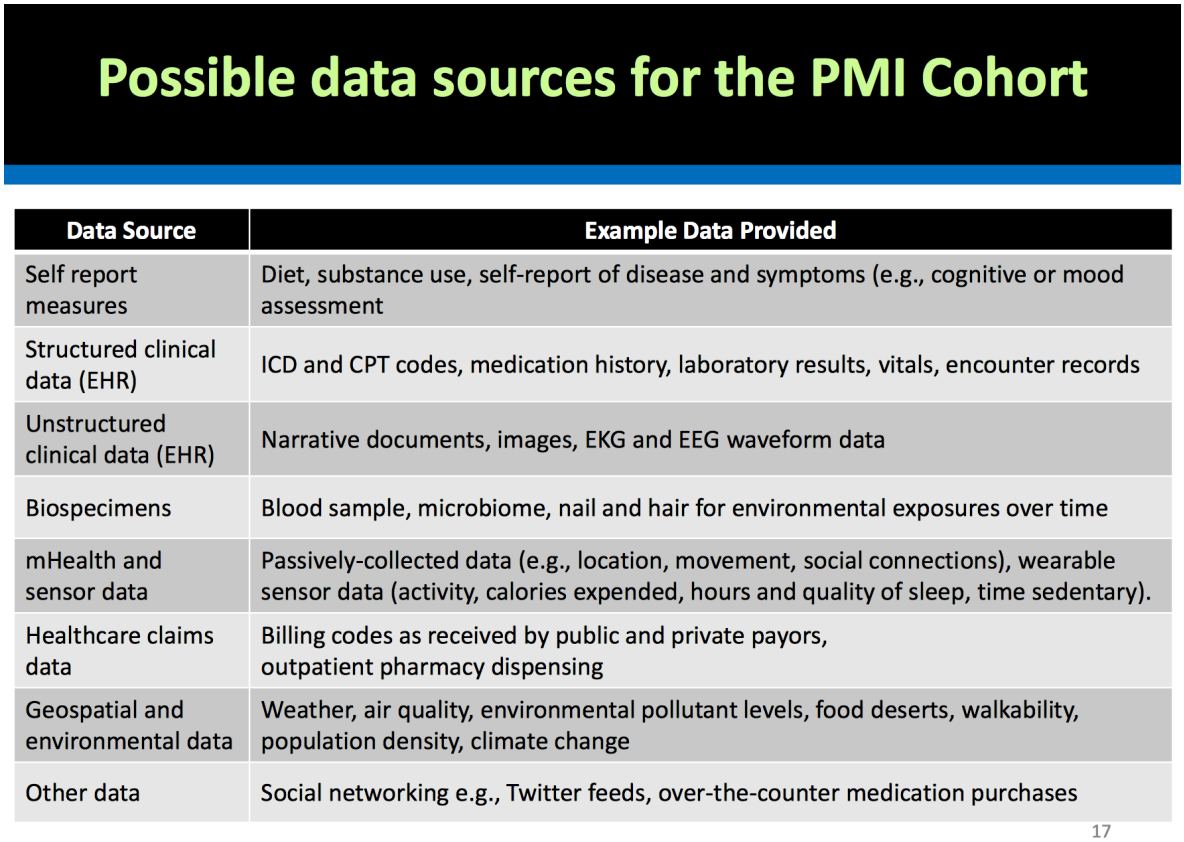


Illustration 1: Initial Core Data Sets from Data Donors to the PMI

Source: https://www.nih.gov/sites/default/files/research-training/initiatives/pmi/pmi-advisorypanel-slides-20160115.pdf.

2. Potential data to be collected from or about volunteers, and data sources



Possible data sources for the PMI Cohort

Data Source	Example Data Provided
Self report measures	Diet, substance use, self-report of disease and symptoms (e.g., cognitive or mood assessment
Structured clinical data (EHR)	ICD and CPT codes, medication history, laboratory results, vitals, encounter records
Unstructured clinical data (EHR)	Narrative documents, images, EKG and EEG waveform data
Biospecimens	Blood sample, microbiome, nail and hair for environmental exposures over time
mHealth and sensor data	Passively-collected data (e.g., location, movement, social connections), wearable sensor data (activity, calories expended, hours and quality of sleep, time sedentary).
Healthcare claims data	Billing codes as received by public and private payors, outpatient pharmacy dispensing
Geospatial and environmental data	Weather, air quality, environmental pollutant levels, food deserts, walkability, population density, climate change
Other data	Social networking e.g., Twitter feeds, over-the-counter medication purchases

17

Illustration 2: Potential donor data sets to contribute to PMI data.

Source: https://www.nih.gov/sites/default/files/research-training/initiatives/pmi/pmi-advisorypanel-slides-20160115.pdf.

Appendix C: Governance Chart for the PMI

The governance of the PMI was initially just a proposal, which can be seen in Illustration 3. As of January 2017, the PMI cohort is now called All of Us Research Program, and it is officially part of the National Institutes of Health. All of Us receives baseline NIH funding now that it is a formal part of NIH, as can been seen in Illustration 4. The governance of the PMI may undergo further iterative changes, but as of January 2017 it is now a formal entity.

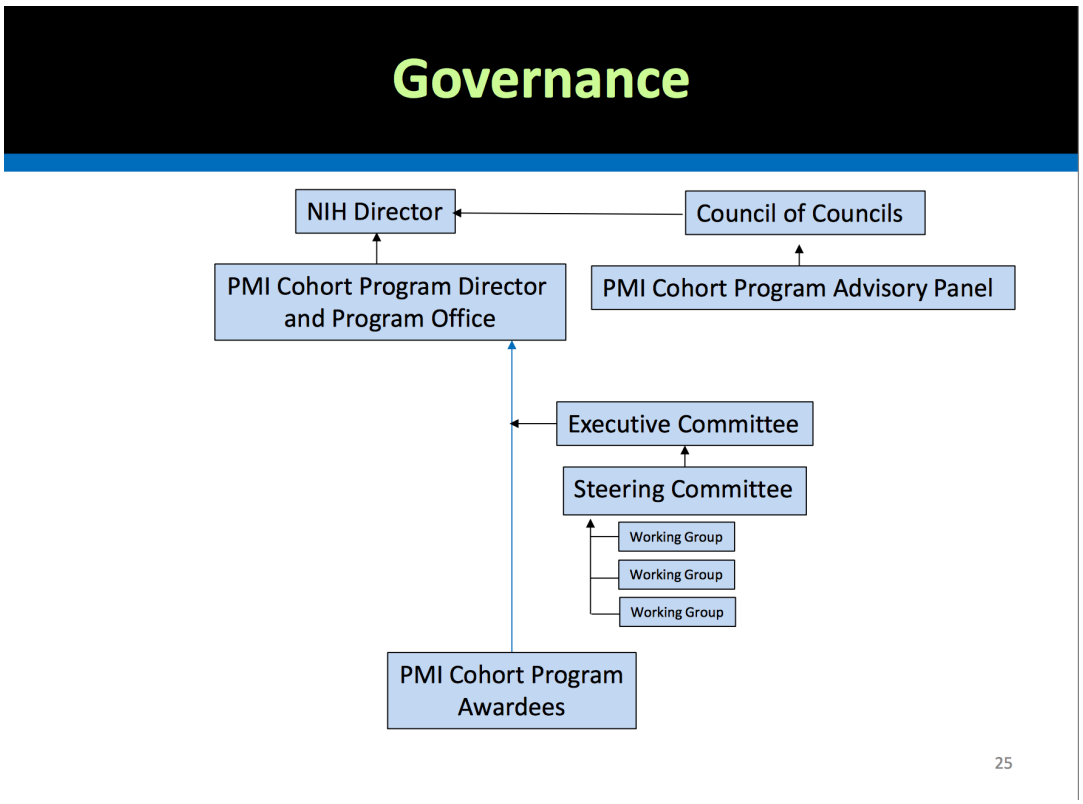


Illustration 3: Governance chart of the PMI.

Source: https://www.nih.gov/sites/default/files/research-training/initiatives/pmi/pmi-advisorypanel-slides-20160115.pdf.

Illustration 4: 2017 Governance chart of the All of Us Research Program (PMI), now an official part of the NIH.

Source: https://www.videocast.nih.gov/summary.asp?live=19067&bhcp=1.

Appendix D Privacy and Security Frameworks of the PMI/All of Us program

The PMI/All of Us research program has published two key documents relating to privacy and security. These are the final versions of those documents, one focused on security, and one focused on privacy and trust.

Precision Medicine Initiative: Data Security Policy Principles and Framework

(May 25, 2016),
https://obamawhitehouse.archives.gov/sites/obamawhitehouse.archives.gov/files/documents/PMI_Security_Principles_Framework_v2.pdf.

Precision Medicine Initiative: Privacy and Trust Principles

(Nov. 2015)
https://obamawhitehouse.archives.gov/sites/default/files/microsites/finalpmiprivacyandtrustprinciples.pdf

Appendix E: Visual Overview of PMI/All of Us Program and Consortium

The slides in this appendix were presented by the National Institutes of Health on January 11, 2017 during the public portion of the All of Us Research Program Advisory Panel Meeting. The original slides can be viewed on the meeting webcast, available at https://www.videocast.nih.gov/summary.asp?live=19067&bhcp=1.

Additional slides from this meeting may be viewed at https://www.nih.gov/sites/default/files/research-training/initiatives/pmi/fo-webinar-slideshow.pdf.

Illustration 5 is an overview of the All of Us program. Illustration 6 is a visual representation of the All of Us consortia.

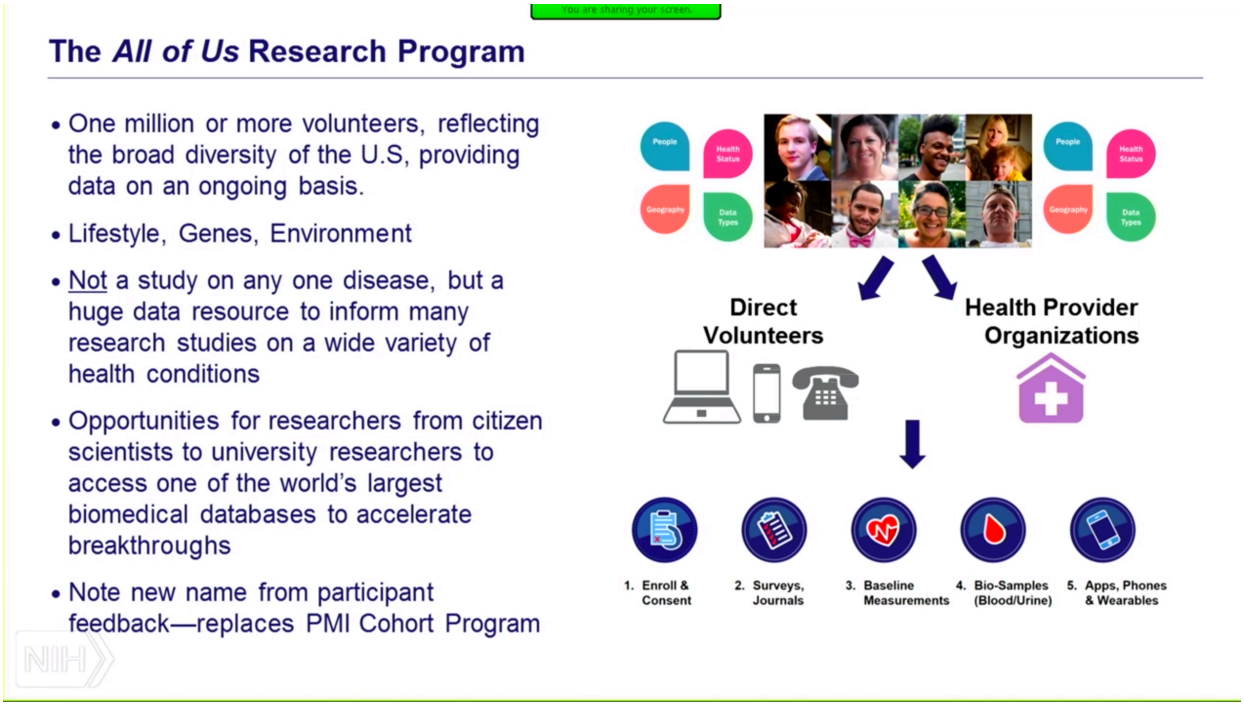


Illustration 5: NIH overview of All of Us Research Program.

Source: January 2017 presentation available at https://www.videocast.nih.gov/summary.asp?live=19067&bhcp=1.

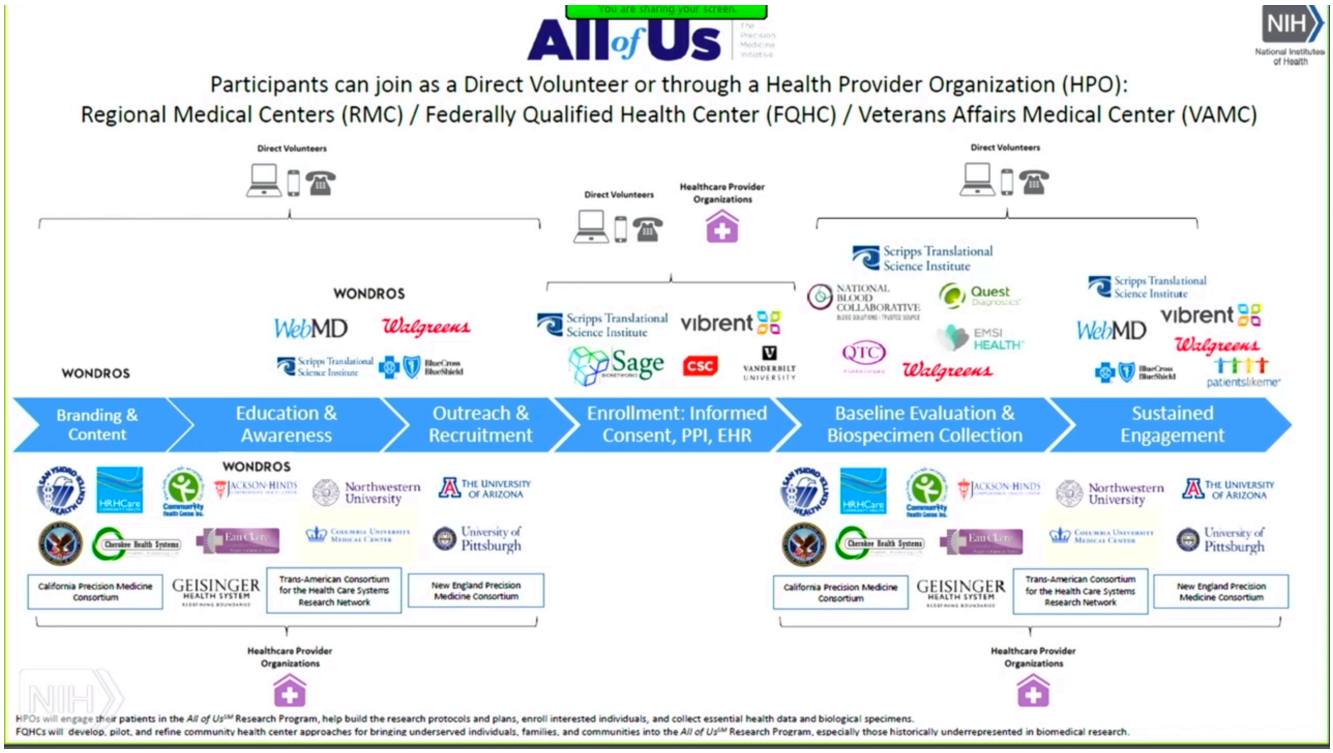


Illustration 6: NIH visualization of PMI/All of Us Research Program.

Source: January 2017 presentation available at https://www.videocast.nih.gov/summary.asp?live=19067&bhcp=1.