July 8, 2015

THE PRECISION MEDICINE INITIATIVE

Precision Medicine Initiative: Proposed Privacy and Trust Principles

As part of its commitment to ensure that privacy is built into the start of the Precision Medicine Initiative (PMI) the White House convened an interagency working group in March 2015 with the charge of developing a set of privacy principles for PMI. This group, co-led by the White House Office of Science and Technology Policy, the Department of Health and Human Services Office for Civil Rights, and the National Institutes of Health, has developed the following Proposed Privacy and Trust Principles for PMI. These principles evolved out of a series of expert roundtables, review of the bioethics literature, an analysis of privacy policies and frameworks used by existing biobanks and large research cohorts, and articulation of a set of fundamental assumptions about the goals and vision of the PMI cohort. The principles provide broad guidance concerning: governance; transparency; reciprocity; respect for participant preferences; data sharing, access and use; data quality and integrity; and security, and are intended to guide future actions that will be undertaken in the design and development of the PMI research cohort. The principles articulate a set of core values and responsible strategies for engendering public trust and maximizing the possible benefits of a large national research cohort, while minimizing the risks inherent in large-scale data collection, analysis, and sharing. The White House is soliciting public comments on these proposed principles through August 7, 2015.

As part of its process, the working group concluded that a parallel process should be undertaken to develop a robust data security framework for PMI with input from experts in security, data science, Health IT, and ethics. This framework should draw on industry best practices in identifying strong administrative, technical, and physical safeguards to ensure the confidentiality and integrity of all PMI cohort specimens and data, and should be reevaluated regularly to keep pace with an ever-advancing technological environment.

Fundamental Assumptions about the PMI Cohort

1. The PMI cohort will be designed to forge a new model for scientific research that emphasizes engaged participants and open, responsible data sharing with strong privacy and security protections.
2. Participants will be partners in research, and their participation will be entirely voluntary.
3. The PMI cohort will be a broad, public resource intended for responsible use by the research and data science communities, including academic, non-profit, and for-profit entities. Data will be used not only for hypothesis-driven research but also for data analyses to formulate questions. Certain information – such as some aggregate data and research results – will be publicly accessible.
4. Participants will play an integral role in the cohort's governance through direct representation on committees established to oversee cohort design and data collection, use, management, security, and dissemination.
5. Participants will be able to voluntarily contribute diverse sources of data – including medical records, genomic data, lifestyle information, environmental data, and personal device and sensor data. The number of data sources and the volume of data will likely increase with time. A minimum data set will be defined and required for participation.
6. The success of the cohort will be enabled by the increasing ability of participants to access their own medical information. A goal of the effort will also be to provide participants access to research data in a respectful and responsible manner.
7. The PMI cohort will include individuals from varied ancestral, demographic, geographic, and health backgrounds who may have different preferences and risk tolerances with respect to privacy.
8. A robust data security framework will be established to ensure that strong administrative, technical, and physical safeguards are implemented to protect all PMI cohort data and that appropriate accountability is established for all parties, in furtherance of the Privacy and Trust Principles.
9. Given the anticipated scope and duration of PMI, single contact consent at the time of participant enrollment will not be sufficient for building and maintaining the level of public trust we aim to achieve. A consent process that is dynamic and ongoing will better serve the initiative's goals of transparency and active participant engagement.
10. Regardless of the PMI cohort's architecture (*e.g.,* centralized, federated, hybrid), a centralized, adaptable governance structure will be required to:

- provide for strong oversight, accountability, and consistency;
- ensure that all data users are bound by the same baseline expectations and norms of behavior;
- establish consent processes and track participant consent;
- determine and manage appropriate communications with participants;
- implement mechanisms for handling complaints concerning data use and identifying and managing breaches; and
- maintain the security of the data.

Proposed Privacy and Trust Principles

Governance

1. The PMI cohort should be planned and conducted in partnership with participants, researchers, health care providers, the Federal Government, and other stakeholders. The central governance system should be highly dynamic and transparent in order to ensure continuous assessment of policies and practices and maintain currency with scientific, technological, and ethics-related developments.
2. Governance mechanisms should include substantive participant and community representation at all levels of program oversight, design, and implementation.
3. In addition to complying with all applicable laws and regulations governing human subjects' research, data privacy, and security, research investigators and institutions, and other authorized data users, should be required to adhere to the rules developed by the established governance system in furtherance of the principles outlined here.
4. Governance mechanisms should ensure accountability, responsible data management, and protect against unauthorized or inappropriate access, use, disclosure, or re-identification of PMI cohort data. Researchers and other data users should be informed of and subject to consequences for failure to adhere to all rules developed in furtherance of these principles.
5. Recognizing that building trust requires that information be provided to PMI participants and communities in an appropriate, responsible, and predictable manner, decisions about how communications with participants are to be handled should be centrally managed. .
6. Risks and potential benefits of research for families and communities should be considered in addition to risks and benefits to individuals. The potential for research conducted using PMI cohort data to lead to stigmatization or other social harms should be identified and evaluated through meaningful and ongoing engagement with relevant communities.

Transparency

1. To ensure participants remain adequately informed throughout participation in the cohort, information should be provided at the point of initial engagement and periodically thereafter. Information should be communicated to participants clearly and conspicuously concerning: how, when, and what information and specimens will be collected and stored; generally how their data will be used, accessed, and shared; the goals, potential benefits, and risks of participation; the types of studies for which the individual's data may be used; the privacy and security measures that are in place to protect the participant's data; and the participant's ability to withdraw from the cohort at any time, with the understanding that data included in aggregate data sets or used in past studies and studies already begun cannot be withdrawn.
2. Information should be made publicly available concerning PMI cohort data use, protection, and access compliance.
3. Participants should be promptly notified following discovery of a breach of their personal information. Notification should include, to the extent possible, the types of information involved in the breach, steps individuals should take to protect themselves from potential harm, if any, and steps being taken to investigate the breach and mitigate losses.
4. All data users should be expected to publish or post publicly their summary research findings, regardless of the outcomes, as a condition of data use. To enrich the public data resource, mechanisms for data users to integrate their research findings into the PMI cohort should be explored.

Respecting Participant Preferences

1. In order for the PMI cohort to be broadly inclusive, a concerted effort should be made to engage and recruit individuals and communities with varied preferences and risk tolerances concerning data collection, sharing, and use.
2. The PMI cohort should promote participant autonomy and trust through a dynamic information sharing process. This process should enable participants to actively engage in an informed and voluntary manner, and to re-evaluate their own preferences as data sharing and use requirements and technology evolve.
3. Participants should be able to withdraw their consent for future research use and data sharing at any time and for any reason, with the understanding that data included in aggregate data sets or used in past studies and studies already begun cannot be withdrawn.

4. Participants should be provided choices as to whether they would like to be re-contacted for various purposes, such as to receive research data or to collect additional information or specimens for research activities.

Reciprocity

1. The PMI cohort should facilitate participants' access to the medical information they contribute to PMI.
2. Educational resources should be made available to participants to assist them in understanding their health information and to empower them to make informed choices about their health and wellness.
3. Innovative and responsible ways of sharing research data with participants should be explored. This could include sharing aggregate research data, research findings, information about ongoing research studies, as well as data collected about participants.

Data Sharing, Access, and Use

1. Multiple tiers of data access—from open to controlled—based on data type, data use, and user qualifications should be employed to ensure that a broad range of interested communities can utilize cohort data while ensuring that privacy is safeguarded and public trust is maintained.
2. To the degree that data is permitted to be downloaded for use on local systems by data users, such data transfers should be governed by data-sharing agreements and other mechanisms that ensure privacy and security safeguards are maintained.
3. Data access, use, and sharing should be permitted for authorized purposes only. Certain activities should be expressly prohibited, including sale or use of the data for targeted advertising.
4. Unauthorized re-identification and re-contacting of participants will be expressly prohibited and consequences should accompany such actions. Data analyses should be conducted with coded data to the extent feasible.
5. The PMI cohort should maintain a link to participant identities in order to return appropriate information and to link participant data obtained from difference sources.
6. Appropriate measures for protecting individual PMI data from disclosure in civil, criminal, administrative, legislative, or other proceedings—for example, through the issuance of certificates of confidentiality as authorized under section 301(d) of the Public Health Service Act—should be explored.

Data Quality and Integrity

1. The PMI governance structure should include mechanisms to ensure that the quality and integrity of PMI cohort data is maintained and that it is accurate, relevant, complete, and appropriately up-to-date.
2. Mechanisms should be created to ensure data integrity is preserved at all stages: collection, maintenance, use, and dissemination.
3. Participants should be able to easily report any inaccuracies in their demographic or medical information maintained by PMI and request that such inaccuracies be addressed.

Security

1. A robust Data Security Framework should be developed in consultation with experts in data science, security, Health IT, and ethics. The Framework should identify for implementation state-of-the-art administrative, technical, and physical safeguards to ensure the confidentiality and integrity of all PMI cohort specimens and data and to protect against threats to their security. The Framework should be integrated into the architecture of the PMI cohort from the start.
2. Consideration of human factors—in addition to technology—in the design of the Security Framework is essential for identifying the security mechanisms that can be easily implemented and properly maintained by data users.
3. Data security safeguards should be reviewed and subjected to penetration testing and auditing at regular intervals to ensure that they remain reasonable and appropriate in the face of evolving technology and data uses.

###