EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

THE DIRECTOR

October 21, 2016

M-17-02

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Shaun Donovan
Director

SUBJECT: Precision Medicine Initiative Privacy and Security

This memorandum provides assistance to executive departments and agencies (agencies) as they are ensuring privacy and security are fully considered in all agency activities supporting the President's Precision Medicine Initiative (PMI).

Within 60 days from the issuance of this memorandum, agencies involved in PMI activities shall provide to the Office of Management and Budget (OMB) a plan to implement as appropriate, the responsibilities contained in this memorandum in agency activities, including ongoing and future activities and all progress to date. Senior Agency Officials for Privacy (SAOP) are to be lead points of contact on this plan. The plan should include the following information: 1) the mechanisms that will be used to incorporate the Precision Medicine Initiative: Privacy and Trust Principles (*PMI Privacy and Trust Principles*) and the Precision Medicine Initiative: Data Security Policy Principles and Framework (*PMI Security Framework*) into current and future PMI activities and 2) any existing standards, rules, or regulations that your agency operates under that you have identified as fulfilling the principles and framework laid out in the *PMI Privacy and Trust Principles* and *PMI Security Framework*. In particular, agencies should ensure that the *PMI Privacy and Trust Principles* and *PMI Security Framework* will be incorporated into extramural and intramural activities. Intramural activities are all activities, including research, conducted by the agency itself (e.g., the Department of Veterans Affairs' Million Veteran Program, intramural researchers at the National Institutes of Health doing projects with any PMI database).

Background

PMI is a research and development initiative which aims to improve health and the treatment of disease by taking into account individual differences in people's genes, environments, and lifestyles. Advances in precision medicine have already led to new discoveries, including the development of a number of treatments tailored to specific characteristics of an individual, such as genetic makeup, or environmental or health history.

Translating this initial success to a larger scale will require a coordinated and sustained national effort including leveraging emerging methods for managing and analyzing large data sets, incorporating improvements in health information technology, incorporating advances in genomics to accelerate biomedical discoveries, and translating those discoveries into improvements in care.

This initiative requires many different types of data about individuals, such as information about lifestyle, environment, and health, and will include diverse efforts by multiple Federal agencies, academic institutions, medical centers, research organizations, and industry. Some efforts will be run by Federal agencies which will collect, store, maintain and process individuals' information. In other cases, Federal agencies will fund academic and other outside institutions, or facilitate research with other Federal agencies, which will, in turn, collect and store information and facilitate research by the broader scientific community.

Participant-contributed data is the foundation of PMI activities, and all participants deserve assurance that the information they contribute is being protected and used responsibly, regardless of the agency or organization conducting the activity. PMI's long-term success depends on establishing and maintaining trust through an ongoing commitment by the Federal Government and entities funded by the Federal Government regarding the privacy and security of the information participants provide and the information that is generated about them. Following from the President's charge to ensure that privacy was built into the start of this initiative, the White House convened an interagency working group to develop privacy principles to guide agencies in PMI activities. The working group members, with public input, concluded that a parallel process should be undertaken with subject matter experts in security, data science, Health IT, and ethics to develop a robust data security framework for PMI. Those two working groups each produced a document, with public input, to guide PMI agencies as they consider privacy and security in the context of PMI. The *PMI Privacy and Trust Principles* document outlines a set of core values and responsible strategies for protecting the privacy interests of participants and properly managing personal information, including health information, such as genomic data. The *PMI Security Framework* articulates policy principles and a framework for protecting the security of participants' data and resources in an appropriate and ethical manner.

For purposes of this memorandum, PMI activities include all efforts conducted in furtherance of PMI that involve the collection, transmission, storage, curation, use, and return of PMI data. These efforts could include, but are not limited to, activities conducted through grants, contracts, cooperative agreements, Other Transactions Authority awards, and intramural activities. PMI data can include, but is not limited to, clinical and insurance claims data, survey and demographic data, geographical and location data, genomic and other biospecimen-derived data, and mobile, implantable, or other equipment or device data, all of which may be stored electronically or on paper. Additionally, for purposes of this memorandum and its implementation, agencies should act only within the bounds of their legal authorities and consistent with all applicable Federal laws, such as the Federal Information Security Modernization Act of 2014, the Paperwork Reduction Act, the Health Insurance Portability and Accountability Act, the E-Government Act of 2002, the Genetic Information Nondiscrimination Act, and the Privacy Act – and applicable implementing regulations.

Agency Responsibilities

1. *Compliance with PMI Privacy and Trust Principles and PMI Data Security Framework.* In all PMI activities, agencies should address, as appropriate, the *PMI Privacy and Trust Principles* and the *PMI Security Framework.* The principles and framework articulated in these documents represent the minimum privacy and security measures that agencies should address when implementing PMI activities. Agencies can, and should, impose additional privacy and security measures consistent with their missions, specific authorities, circumstances, and risks that reflect the principles and framework laid out in the *PMI Privacy and Trust Principles* and *PMI Data Security Framework* documents. All actions should be regularly evaluated to identify new risks, implement controls to mitigate those risks, and to ensure controls operate as intended, and are updated, as appropriate.

2. *Grants.* Prior to making a final funding decision, agencies should require grantees to comply with the *PMI Privacy and Trust Principles* and *PMI Security Framework* as appropriate, for their role in PMI and should require applicants to describe their ability to act consistent with and adhere to these principles and framework during the funding decision process. For Federal grants and cooperative agreements that support PMI activities, awarding agencies should consider including terms and conditions in grants which require recipients to adhere to their submitted plans for compliance with the *PMI Privacy and Trust Principles* and *PMI Security Framework* during all stages of award, including, but not limited to, the collection, transmission, storage, curation, use, and return of PMI data. For awards that include milestones, agencies may consider the grantees' past compliance with the principles and framework when making decisions about continued or supplemental funding.

3. *Contracts.* Agencies should require offerors to develop, and successful contractors to implement and maintain a plan that explains how the entity will align its PMI program activities with the objectives set forth in the *PMI Privacy and Trust Principles* and *PMI Security Framework* based on the contractor's role in PMI. As appropriate, agencies can and should require that this plan describe the processes and procedures that will be followed to ensure appropriate privacy safeguards for IT systems and PMI data at stages relevant to the contract work. These stages include processes and procedures required of subcontractors, such as data collection, transmission, storage, curation, use, and return of PMI data. Agencies should determine the extent to which a plan is required based on the nature of the planned work (e.g., a contract for collecting and managing data and metadata to support research on genomic sequences will require a more comprehensive plan than a contract to scan forms for medical data used to support PMI research) and the extent to which a previously developed contractor plan may satisfy the requirements of a pending contract. The contractor's plan could be incorporated by reference into the contracts or task orders when a contractor will be safeguarding PMI-related information or performing other work involving PMI information as explained in the solicitation's statement of work and as directed by the resulting Federal contract.

4. *Other Transactions Authority*. Any relevant agency with authority to enter into transactions (other than contracts, cooperative agreements, or grants) to carry out PMI activities should incorporate and require adherence to the *PMI Privacy and Trust Principles* and *PMI Security Framework* in those transactions. Agencies should include a requirement in funding opportunity announcements that applicants develop, and implement plans and procedures consistent with the *PMI Privacy and Trust Principles* and *PMI Security Framework,* as appropriate for the applicant's role in PMI. When reviewing applications, agencies should require an applicant's plans to comply with the *PMI Privacy and Trust Principles* and *PMI Security Framework,* where appropriate, and incorporate those considerations into funding decisions. Also, as agencies review an applicant's progress on a given project, they should ensure the project is operating consistent with the principles and framework when determining whether to continue or supplement funding.

5. *Interagency Agreements.* Agencies that enter into agreements that involve the sharing of PMI data with other agencies, should incorporate the *PMI Privacy and Trust Principles* and *PMI Security Framework* into such agreements and into subsequent agency PMI activities.

6. *Intramural Activities and Research*. Agencies should develop and implement policies to ensure that intramural activities, including research, using PMI data or biospecimens, are conducted in accordance with the *PMI Privacy and Trust Principles* and the *PMI Security Framework*. These policies should be updated and evaluated annually to ensure appropriate application to PMI activities.

7. *SAOP Coordination for PMI Activities*. The PMI effort is complex, requiring the Senior Agency Official for Privacy to coordinate with the agency's Chief Information Officer as well as procurement and grant staff. The Senior Agency Official for Privacy will also need to reach outside his or her agency for support and expertise, as appropriate, from the Federal Privacy Council, the PMI community, the Chief Information Officers Council, the Chief Acquisition Officers Council, and the larger PMI and grant-making community.

Agencies shall implement this memorandum consistent with applicable law. This memorandum is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.