THE WHITE HOUSE

*February 25, 2016*


# Precision Medicine Initiative:
# Data Security Policy Principles and Framework

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. Building from the existing PMI Privacy and Trust Principles, this document offers security policy principles and a framework to guide decision-making by organizations conducting or participating in precision medicine activities. Recognizing that there is no "one size fits all" approach to managing data security, this document provides a framework for protecting participants' data and resources in an appropriate and ethical manner that can be tailored to meet organization-specific requirements.

This document is for the precision medicine community to use as the basis for their own customized data security needs. Data security is a constantly evolving field and new threats are identified every day. Over time, these principles and framework will need to be updated to be responsive to changing circumstances and new threats. Nothing in this document is intended to preclude the public posting of certain non-identifiable, non-individual level information, such as aggregate research data, research findings, and information about ongoing research studies. PMI organizations will comply with all applicable laws and regulations governing privacy, security, and the protection of PMI data at every stage of data collection, storage, analysis, maintenance, use, exchange, and dissemination.

This document was developed through a collaborative interagency process with input from the Office of Science and Technology Policy; National Security Council; U.S. Digital Service; National Institute for Standards and Technology; Federal Trade Commission; Department of Veterans Affairs; Department of Defense; and Department of Health and Human Services, including its Office for Civil Rights, Office of the National Coordinator for Health IT, National Institutes of Health, Food and Drug Administration, and Centers for Medicare and Medicaid Services. These principles and framework were informed by a series of roundtables with security experts from private industry and academia, and a review of existing data security resources.

Security requires a continuous set of evolving processes and controls to address both internal and external threats, and assure the confidentiality, integrity, and availability of data generated and contributed during precision medicine activities. Organizations conducting precision medicine-type research should recognize that ensuring data security will be an ongoing process, and should strive to use current best practices. Given that security best practices are highly dependent on context, each organization will need to conduct its own risk assessment to identify specific security requirements and establish processes to continuously review and make improvements.

Participant-contributed data is the foundational asset of PMI, and participants need assurance that it is being protected and used responsibly. In order to establish trust and encourage widespread participation and donation of health data, PMI organizations should adopt consistent policies and practices, provide clarity about objectives and expectations, and be transparent about systems and data use.

A few unique considerations of precision medicine that guided the development of this document include:

- The types of data used for PMI activities could include, but are not limited to, clinical and insurance claims data, survey and demographic 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. This data is referred to throughout this document as PMI data. PMI data is highly sensitive for participants and requires a high level of security and privacy protection.
- This document is intended to be used by PMI organizations, such as institutions, service providers, or other entities that collect, use, analyze, or share PMI data.
- The primary users of PMI data include individual participants, researchers, developers, citizen scientists,[1] and health care providers.
- PMI organizations have the freedom to take advantage of system architectures that meet their needs, including security needs, such as cloud or enclave approaches.
- This document addresses security measures for PMI data, which includes the data and metadata associated with biospecimens collected as part of PMI activities. There are other requirements related to physical security that PMI organizations should consider that are beyond the scope of this document.
- De-identification is the removal of identifying information (such as name, date of birth, address, social security number) from a dataset so that individual data cannot be linked with specific individuals. De-identification is a significant technical control that can help protect the privacy of a participant. However, an increase in computational power, plus the ability to combine different data sets, means that de-identified data held by a PMI organization could still be matched to an individual. Therefore, PMI organizations should not rely on de-identification alone as a security control.

[1] **In citizen science, the public participates voluntarily in the scientific process, addressing real-world problems in ways that may include formulating research questions, conducting scientific experiments, collecting and analyzing data, interpreting results, making new discoveries, developing technologies and applications, and solving complex problems. Available at: https://www.whitehouse.gov/sites/default/files/microsites/ostp/holdren_citizen_science_memo_09**

## Data Security Policy Principles

The following overarching principles are intended to guide organizations in developing and implementing an appropriate security plan. PMI organizations should, at a minimum:

- Strive to build a system that participants trust. This means having a "participant first" orientation when identifying and addressing data security risks. Participants are the foundational stakeholders of all research activities.
- Recognize that security, medicine, and technology are evolving quickly. As a result, organizations should treat security as a core element of the organization's services and ensure that security elements are adaptable and updatable.
- Seek to preserve data integrity, so that participants, physicians, and researchers can depend on the data.
- Identify key risks, and develop evaluation and management plans that address those risks, while still enabling science and research to advance.
- Provide participants and other relevant parties with clear expectations and transparent security processes.
- Use security practices and controls to protect data, but not as a reason to deny a participant access to his or her data, or as an excuse to limit appropriate research uses of the data.
- Act responsibly. Seek to minimize exposure of participant data, and to keep participants and researchers aware of breaches in order to maintain trust over time.
- Share experiences and challenges so that organizations can learn from each other.

## Achieving the Principles through a Precision Medicine Initiative Data Security Policy Framework

This section is based on a framework developed by the National Institute for Standards and Technology (NIST). The NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, defines a set of activities, outcomes, and references that, when followed, enable five simultaneous and continuous functions—Identify, Protect, Detect, Respond, and Recover—to assess cybersecurity and data security performance, as well as physical and environmental controls.

NIST Framework Core Functions

- **Identify**. Develop the organizational understanding to anticipate and manage cybersecurity risk to systems, assets, data, and capabilities.
- **Protect**. Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- **Detect**. Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
- **Respond**. Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
- **Recover**. Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

*NIST Cybersecurity Framework: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf*

## Identify

1. **Overall Security Plan.** PMI organizations should develop a comprehensive risk-based security plan that outlines roles and responsibilities related to security, consistent with the principles and framework outlined here. The security plan should identify the governance body for the organization's security program. The governance body will ensure those who use or manage PMI data adhere to the security plan.[2] The security plan should be reviewed by the governance body and updated periodically to incorporate evolving standards and best practices. The plan should describe its approach for:
    - Complying with applicable laws and regulations, and other organization-specific security policies and standards;
    - Designating and maintaining an appropriately resourced and technicallyexperienced information security team;
    - Identifying, assessing, and responding to vulnerabilities and threats;
    - Conducting continuous monitoring;
    - Responding to security incidents and breaches;
    - Ensuring the physical security of areas where PMI data is located; and
    - Ensuring participants, researchers, and technical staff are aware of their security responsibilities.
2. **Risk-Based Approach.** PMI organizations should use risk-management strategies, tools, and techniques to inform and prioritize decisions regarding the protection of PMI data, including; electronic and physical resources within its environment as well as at the point of initial collection. When planning protection of PMI data, the form of the data should be considered (e.g., raw, aggregate, the

[2] **Please also see governance principles outlined in the White House Precision Medicine Privacy and Trust Principles: https://www.whitehouse.gov/sites/default/files/microsites/finalpmiprivacyandtrustprinciples.pdf**

product of a mathematical or statistical process or an analysis report, as well as whether the data are electronic or paper-based).

3. **Independent Third-Party Review.** PMI organizations should have an independent review of their security plans and of the effectiveness of controls on a periodic basis. The reviewer, at a minimum, should perform: a review of the organization's adherence to its security plan; regular vulnerability assessments (e.g., network scans and penetration testing); and evaluation and adjustment of the security program in light of vulnerability assessments and evolving circumstances.
4. **Transparency.** A high-level overview of the organization's security plan and approach should be posted publicly to help enable transparency and congruity with the goals of the Privacy and Trust Principles and this Security Framework. This high-level overview should describe the organization's breach notification process, steps individuals should take to protect themselves, and ways that the public and users of the PMI data can easily submit information about potential vulnerabilities and bugs.

## Protect

### Access Control[3]

1. **Identity Proofing.** PMI organizations should develop a policy for verifying the identity of users and contributors (e.g., participants and healthcare provider organizations), prior to granting credentials for access to or contribution of PMI data.
2. **Credentials.** PMI organizations should use innovative approaches for authentication so that over time they do not rely on username and password alone, and should use strong multi-factor authentication for users of PMI data.
3. **Authentication.** Risk-based authentication controls should flow from the PMI organization's security risk assessment, and should be commensurate with the type of data, level of sensitivity of the information, and user type.
4. **Authorization.** Authorization controls should be granular enough to support participant consent that has been captured by the PMI organization and should limit access, use, or disclosure based on what is necessary to satisfy a particular purpose or carry out a function.

### Awareness and Training

1. **Participant Education.** PMI organizations should provide participants with security awareness materials and education on an ongoing basis. The educational materials should include discussion of how data will be used, the high-level protections that safeguard the data, and the tools available to research participants to protect their own PMI data.
2. **PMI Data User Education.** PMI organizations should provide appropriate training for individuals using PMI data and infrastructure based on the

[3] **Please see the Data Sharing, Access, and Use principles outlined in the White House Precision Medicine Privacy and Trust Principles, which provide for multiple tiers of data access to PMI data – from open to controlled – based on data type, data use, and user qualifications: https://www.whitehouse.gov/sites/default/files/microsites/finalpmiprivacyandtrustprinciples.pdf**

individual's role and responsibilities. This role-based training should include information on appropriate protections for PMI data and security best practices. Appropriate security certifications and continued training in information system security and privacy protection should be encouraged.

**Data Security**

1. **Encryption.** PMI data that is reasonably likely to identify an individual should be protected at-rest and in-motion using strong encryption. Examples of data reasonably likely to identify an individual include direct identifiers such as name, birth date, contact information, and Social Security Number.
2. **Encryption Key Security.** PMI organizations should store encryption keys separately from encrypted data and establish policies for secure encryption key creation, distribution, access, and revocation.
3. **Physical Security.** PMI data should be protected by physical security controls as well as cybersecurity controls.
4. **Service Provider Security.** When PMI organizations employ subcontractors, third parties, or vendors (including hosted, cloud, or application service providers) to create, receive, maintain or transmit PMI data, PMI organizations should obtain the necessary assurances that the service provider will appropriately safeguard PMI data, consistent with the PMI organization's security plan.
5. **Integrity Protection.** PMI organizations should implement integrity protection controls that detect when unauthorized alterations have been made to PMI data.

**Information Protection and System Maintenance**

1. **Life Cycle.** PMI organizations should implement a system development life cycle, which ensures that appropriate safeguards for PMI data remain in place from receipt or creation through disposition.
2. **Security Patching.** PMI organizations should keep systems updated with the latest security patches and should develop change control and configuration management policies to ensure that system updates are tested, reviewed, and approved prior to implementing.

## Detect

1. **Audit Events.** PMI organizations should define a set of system and network events that capture interactions with PMI data from networks, servers, and application infrastructure, including user access and behavior.
2. **Audit Logs.** System and network events should be logged on a continuous uninterrupted basis in a manner that protects against tampering and provides sufficient detail to identify: the type of action performed on PMI data, the unique identity of who performed the action, the date and time the action occurred, and the subset of data impacted by the action.
3. **Detection and Alerting.** Continuous detection processes and alerting mechanisms should be created to ensure timely and adequate awareness of anomalous events, as well as a process to inform operational staff and stakeholders with relevant situational details.

4. **Threat Information Sharing.** PMI organizations should participate in relevant threat information sharing forums.[4] PMI organizations should also follow existing best practices to provide ways for participants and non-affiliated individuals and entities to report potential vulnerabilities or threats, and respond to reports appropriately.
5. **Anomaly Reporting.** PMI organizations should make reports of security anomalies, alerts, reports, or other relevant events available to the PMI organization's governance boards, and should also provide remediation plans to prevent similar vulnerabilities from occurring in the future.

## Respond

1. **Incident Response.** Not all security incidents result in a breach. PMI organizations should develop a plan to respond to and contain security incidents. This plan should include a process to identify quickly and effectively whether an incident has led to a breach of PMI data. Organizations should coordinate response activities with internal and external parties, as appropriate (e.g., law enforcement, Internet Service Providers, Information Sharing and Analysis Organizations, Information Sharing and Analysis Centers, and vendors).
2. **Incident Response Testing.** PMI organizations should regularly test incident response plans to ensure the highest level of proficiency.
3. **Affected Individual Notification.** When a PMI organization has determined that a security incident has resulted in a breach of PMI data, the organization should notify the affected individuals and appropriate organizations in accordance with applicable breach notification laws, the Privacy and Trust Principles, and the organization's security plan.[5]
4. **Accountable Point of Contact.** PMI organizations should identify an accountable point of contact who will coordinate with appropriate organizations and affected individuals throughout the incident response process. The contact should have the authority to direct actions required in all phases of the incident response.

## Recover

1. **Incident and Breach Recovery Plan.** PMI organizations should establish, maintain, and implement plans for emergency response, backup operations, and

**[4] This sharing should be conducted through existing information sharing and analysis organizations including information sharing and analysis centers (e.g. HI-Trust, NH-ISAC); through the creation of new organizations focused on the specific circumstances of PMI organizations; bilaterally with other trusted organizations; with the Federal government, including through the National Cybersecurity and Communications Integration Center; and the Department of Health and Human Services.**

**[5] As stated in the Privacy and Trust Principles, "Participants should be notified promptly following discovery of a breach of their personal information. Notification should include, to the extent possible, a description of 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, mitigate losses, and protect against further breaches."**

post-incident recovery for PMI data. These plans should address how the PMI organization will stabilize after the incident and restore basic services.

2. **Communication.** As an integral part of the recovery plan, PMI organizations should communicate to stakeholders when a safe and secure environment has been restored.
3. **Lessons Learned.** After recovery from a security incident or breach, PMI organizations should identify lessons learned, including conducting root cause analysis, to identify areas needing improvement, and update security plans based on those lessons learned. Lessons learned should be reported to the PMI organization's governance board, and information that may be helpful to other PMI organizations should be shared with the PMI community as appropriate.

# Appendix A. Glossary

- Network Scan: A network scan identifies all clients and servers on a network, and uses a database of virus definitions to identify vulnerabilities in specific devices and servers in the network. It can also identify other vulnerabilities such as testing for versions of software with known vulnerabilities or misconfigurations.
- Data In-Motion: Data is "in-motion" when it is transferred through communications media, ranging from physical cables and cords to wireless communications like Bluetooth and Wi-Fi. Information in the process of being exchanged between internet users is considered "in-motion."
- Data At-Rest: Data is "at rest" when it is not being read, written to, or sent over a network by a user, and is stored physically in a digital form like a hard drive.
- Encryption: A cryptographic process of encoding data in a way that unauthorized parties cannot access the data.
- Encryption Key: An encryption key is used in an encryption process to render data unreadable. To access the data, a user needs the encryption key to decrypt the data to make it readable again. Keys can be password-based, biometric-based, or randomly generated (e.g., certificates).
- System Development Life Cycle: A multistep process for the development of an information system that begins with initiation, analysis, design, and implementation, and continues through the maintenance and disposal of the system.