Information Security Standard

Prescription Monitoring Information eXchange

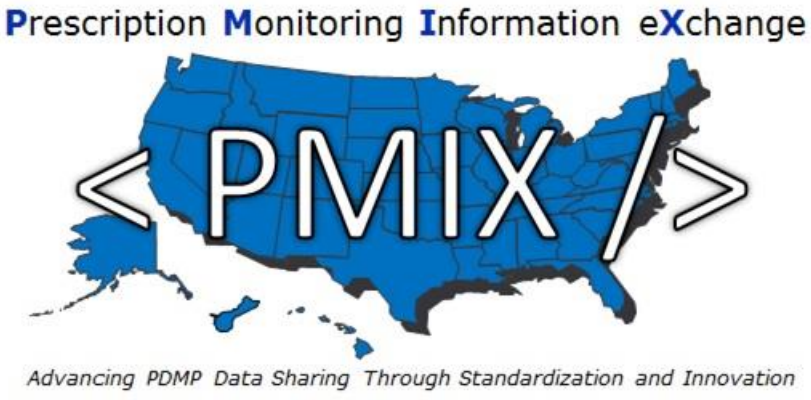

Table of Contents

1. Change Control

Version	Date	Change Summary
1	7/25/17	First Draft
2	8/28/17	Feedback from Executive Committee and the Office of the Chief Information Security Officer of the Office of Justice Programs
3	8/30/17	Updates on Executive Committee Call
4	8/31/17	Additional suggestions from Exec Committee members
5	9/25/17	Clean up definitions and review by the Ad Hoc Security Controls subcommittee.
6	10/10/17	Incorporate suggestion from Security Controls Subcommittee and Heather Gray, Training and Technical Assistance Center, Brandeis University.
7	3/27/18	Incorporated grammatical corrections.
8	3/28/18	Changes to the definition of a Hub/Intermediary and section on compliance.
9	5/9/18	Modification to the definition of a Third Party Intermediary.
Final	5/9/18	Approved by the Executive Committee

2. Background

The Prescription Monitoring Information eXchange (PMIX) Working Group is a standards organization sponsored by the Bureau of Justice Assistance. Its purpose is to support the sharing of Prescription Drug Monitoring Program data among PDMP organizations and their stakeholders by establishing and maintaining the PMIX National Architecture and related guidelines, policies and standards to minimize the cost and complexity of sharing PDMP data across organizational, vendor, geographic and operational boundaries; enable secure, trusted exchanges of PDMP data and promote consistency among PDMPs.

2.1. PMIX National Architecture

The PMIX National Architecture is a nationwide framework designed to enable standards-based sharing of information between Prescription Drug Monitoring Program (PDMP) organizations and their stakeholders.

2.2. Guiding Principles

The Guiding Principles of the PMIX National Architecture foster prescription drug information sharing across all Federal, State, Tribal and approved third party entities in accordance with the PMIX National Architecture are:

- Protect state's full rights and control of Data Ownership.
- Promote the adoption of security standards that protects the confidentiality, integrity, and availability of the data, in transit and at rest.
- Promote uniformity in the selection of a limited set of approved common data standards.
- Promote a standard to which IT solution providers are held that ensures the best value products and/or services to PDMP participating states, while maintaining the public's trust and fulfilling public policy objectives.

2.3. Definitions

2.3.1. Standards

Standards are the rules which must be followed to enable an effective information security program. Compliance with the standards is mandatory, but deviation is possible if approved by the appropriate process. Standards define the minimum, baseline procedures, practices, and configurations for systems, applications, controls, networks, and related topics. They are designed to provide a single reference point for use during software development and adoption, installation of systems and tools, and during the contracts process with vendors and service providers. Standards do not, however, give detailed command-line instructions on how to meet the organization's policies.

2.3.2. Policies

Policies are documents which set out the organization's position regarding business processes and related topics. Policies are a high-level principles and rules created and adopted to help the organization meet its goals, objectives and standards.

2.3.3. Procedures

Procedures define specific methodology to accomplish the standards and policies of the organization.

2.3.4. Plan of Action & Milestones (POA&M)

The POA&M is used to monitor progress in correcting weaknesses or deficiencies noted during the security control assessment. The POA&M identifies: (i) the tasks to be accomplished with a recommendation for completion either before or after information system implementation; (ii) the resources required to accomplish the tasks; (iii) any milestones in meeting the tasks; and (iv) scheduled completion dates for the milestones

2.3.5. Third Party Intermediary (Hub and Other Services)

A service that enables sharing of data between two or more organizations or states by facilitating transactions to and from Prescription Drug Monitoring Programs and/or their stakeholders. This includes, but is not limited to hubs such as PMP Interconnect and RxCheck.

2.3.6. Hub vendor*[1]

An organization or corporation that provides the hub service.

2.3.7. Agent

Agents are those who act on behalf of PDMP or their data sharing partners.

2.3.8. PMIX Working Group*[1]

The governance organization for the PMIX National Architecture and its related standards and guidelines.

2.3.9. PMIX National Architecture*[1]

The Prescription Monitoring Information eXchange (PMIX) National Architecture is an information exchange standard and related guidelines that enables interoperability between systems PDMPs use for interstate exchange of PDMP data. The architecture is comprised of a formal set of technical requirements that apply to state PDMP systems, data sharing 'hubs', and other exchange partners or intermediaries.

2.3.10. PDMP*[1]

A Prescription Drug Monitoring Program is an electronic database which collects and distributes designated data on prescription drugs dispensed in a state, commonwealth, district or territory.

2.3.11. PDMP Organizations*[1]

A PDMP Organization is a specific United States state, commonwealth, district or territorial regulatory, administrative or law enforcement agency that houses the PDMP. The housing agency distributes data from the database to individuals who are authorized under state law to receive the information for purposes of their profession.

2.3.12. PDMP Systems*[1]

The software system that houses the electronic database for a PDMP Organization.

2.3.13. PDMP Data*[1]

Controlled substance and drugs of concern dispensing data submitted by pharmacies and other dispensers in a state to a PDMP.

3. Standards Implementation

3.1. Audience

This document applies to all entities involved in the exchange of prescription data between Prescription Drug Monitoring programs and their stakeholder organizations as well as data sharing hubs, and other exchange partners or intermediaries. This document applies to all of the programs and vendors supporting this exchange of information.

3.2. Use of the Standards Document

This standards document is a reference point for use by business units, technology implementers, and service providers to ensure a consistent framework of protections is in place. Implementing these standards involves:

- Review of existing controls, procedures, and tools against the standards
- Documenting compliance or deviations
- Gap analysis to determine where improvements are needed
- A risk analysis to validate that the improvements are justified against the costs of the controls and the value of the information involved
- Creation of a plan to close the gaps OR request and approval of an exemption
- Documentation of the new controls, procedures, tools

This standard defines a minimum level of compliance. Vendors and organizations may choose to implement a higher level of protection than what is outlined in this document. No signoff or approval is needed for a higher level of protection.

3.3. Compliance with State Statute or Regulation

This document does not supersede or amend any requirements imposed by the laws, rules, or policies of an individual state or the federal government. This standard was developed, approved, and adopted by Prescription Drug Monitoring Programs and this representative standards organization. Compliance with this standard does not confirm or indicate compliance with any such laws, rules, or policies. Please consult with the individual PDMP organization that oversees the data being exchanged to ensure that the exchange complies with their applicable laws, rules, and policies.

4. Prescription Monitoring Information eXchange Security Standard

The Prescription Monitoring Information eXchange standard for the security of information is the most recent edition of the United States Department of Commerce's National Institute of Standards and Technology (NIST) Special Publication 800-171, *"Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations"*. This document can be found at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf . The Executive Committee and its Subcommittees shall conduct an evaluation of changes in any new release of the NIST Special Publication 800-171. The Plan of Action and Exemption processes may be invoked by the Executive Committee for changes in any new release of the NIST Special Publication 800-171.

4.1. Compliance

State Prescription Drug Monitoring Programs, their agents and third party intermediaries shall be responsible for ensuring the security of other state's data entrusted to their care through an interstate exchange of information. Each state, their agents and intermediaries shall be responsible for providing information security protections commensurate with the risk and magnitude of harm resulting from unauthorized use, disclosure, disruption, modification, or destruction of information shared between organizations. Compliance certification will allow states, agents and third party intermediaries to attest to their level of security capability. States, agents and third party intermediaries who wish to certify compliance shall provide evaluation documentation per section 4.2.

4.2. Evaluation

4.2.1. Evaluation by Participating States and Their Agents

Each biennial, each state shall certify compliance by the state and their agents with the applicable PMIX Security Standards, apply for a waiver for any standards with which they will not comply or apply for a Plan of Action for any standards with which they plan to comply.

4.2.2. Evaluation by Intermediaries

Each year, each entity shall perform an independent audit of the information security program and practices of that entity to determine their compliance with the PMIX Security Standard. Each audit shall include testing of the effectiveness of information security policies, procedures and practices of a representative subset of the intermediary's information systems, an assessment of compliance with the PMIX Security Standard based on the results of the testing and a plan of action to remediate any issues of non-compliance. This audit and its corresponding plans of action, if applicable, shall be presented to the Executive Committee of the PMIX Working Group for review and acceptance. The audit may be based on in whole or in part an audit performed for the organization for other purposes as long as the PMIX Security Standards were specifically addressed in the audit process.

4.2.3. Evaluation Compliance

Each state, their agents and intermediaries shall perform evaluations as defined here in to demonstrate compliance with the PMIX standard. States and Intermediaries must submit the evaluation of their PMIX Security Standard compliance to the PMIX Executive Committee, and/or its designee. Evaluations shall be approved by a simple majority of the Executive Committee.

4.3. Plan of Action & Milestones

States and third party intermediaries may submit a plan of action to the PMIX Working Group Executive Committee, and/or its designee for any areas of non-compliance with the PMIX Security Standard. The Plan of Action shall identify (i) the tasks to be accomplished with a recommendation for completion; (ii) the resources required to accomplish the tasks; (iii) any milestones in meeting the tasks; and (iv) the scheduled completion dates for the milestones. A POA&M will reviewed by the Executive Committee, and/or its designees. A final POA&M shall be approved by a simple majority of the Executive Committee. States and third party intermediaries with a POA&M shall

report progress on their plan as required by the Executive Committee or its designee, but no less than quarterly.

4.4. Exemption

Balancing security considerations with mission and operational needs is paramount to achieving an acceptable authorization decision. Risk acceptance decisions are made based on the degree to which the desired security capabilities have been effectively achieved and are meeting the security requirements defined by an organization. These risk-based decisions are directly related to organizational risk tolerance that is defined as part of an organization's risk management strategy. Risk factors such as cost, schedule, and performance are considered in the overall determination of which security controls to employ in organizational information systems and environments of operation. The risk associated with any security control that has not been implemented, and for which the entity has no intentions of implementing, is considered an Accepted Risk and should be documented to include information regarding mitigating controls, and operation requirements. Exemptions/waivers shall be approved and monitored. The weakness and corresponding risk must be monitored periodically, **but no less than annually**, to ensure the associated risk remains at an acceptable level and reported to the Executive Committee or its designee.

States and Intermediaries may submit a request for an Exemption for any areas of non-compliance with the PMIX Security Standard to the PMIX Executive Committee, and/or its designee. The application for an Exemption must identify each area with the reason for the exemption and any compensating controls that will be in place, if applicable. Exemptions shall be approved by a simple majority of the Executive Committee for a designated period of time not to exceed two years. States or Intermediaries shall be responsible for requesting a new Exemption prior to the expiration of the previous Exemption period. Requests shall be submitted no less than three months in advance of the Exemption expiration.

4.5. Breach of Information Security

States, their agents and intermediaries shall notify the PMIX Executive Committee and the state(s) who owns the compromised data of any security incident or breach from a failure to comply with the PMIX Information Security Standards within three business days of discovery. Notifications to states must include the data needed per state statute, regulation, policy and procedure. Notifications to the PMIX Executive Committee shall include the nature of the breach, the applicable security standard associated with the breach, mitigating procedures taken to respond to the security incident and action plans for evaluating and implementing policies, procedures and practices in response to said incident. The PMIX Executive Committee may declare the state or intermediary non-compliant with PMIX Security Standards, approve an action plan or require additional actions.

5. Document Maintenance

This document must be reviewed at least biennially, and updates made to keep it in accord with the organization's overall goals and risks. The initial review shall be conducted by a subcommittee designated by the PMIX Executive Committee. Any corrections, updates, improvement suggestions or other comments should be sent to the Executive Committee for review and delegation to a subcommittee, if appropriate. All modifications to this standard shall be approved through the Process to Change the PMIX National Architecture as defined in the bylaws of the PMIX Working Group.

End note

[1] *These definitions are reproduced from the bylaws of the PMIX Working Group. The definitions found in the bylaws will supersede these definitions in the case of discrepancy.*