Prescription Monitoring Information eXchange

Advancing PDMP Data Sharing Through Standardization and Innovation

"Ashwini Jarral" <ashwini.jarral@ijis.org>,

March 27, 2018

Kim Gaedeke, Acting Deputy Director
Department of Licensing and Regulatory Affairs
611 Ottawa Street, 4th Floor
Lansing, MI 48909

Dear Kim:

On behalf of the Executive Committee of Prescription Monitoring Information eXchange (PMIX), we thank you for your response to the call for comment on the Proposed PMIX Security Standard dated November 27, 2017. We apologize for the delay in responding to your feedback. It has taken more time than expected to review and respond to state comments. In addition to the responses provided herein, we would like to schedule a conference call to bring you up to speed on the PMIX Working Group and its activities. Please let us know when it would be convenient.

You had provided the following comments to the PMIX Executive Committee:

> **From:** Gaedeke, Kimberly (LARA) [mailto:GaedekeK@michigan.gov]
> **Sent:** Monday, November 27, 2017 11:11 AM
> **To:** Hall, Jean S (CHFS OATS HSSMB) <jean.hall@ky.gov>
> **Cc:** Winans, Haley (LARA) <WinansH@michigan.gov>; Hudson, Andrew (LARA) <HudsonA3@michigan.gov>
> **Subject:** PMIX Information Security Standard Proposal - Michigan Feedback
> **Importance:** High
>
> Jean,
>
> I hope you and your family had a nice Thanksgiving holiday. My apologies for the delay in providing Michigan's comments and concerns regarding the PMIX Information Security Standard Proposal which will also be discussed for today's TTAC/PMIX webinar.
>
> Below are questions and comments some of which may be elementary because we are not as familiar with PMIX:
>
> 1. Who is on the Executive Committee?
> 2. How many states are with PMIX?

3. Why is so much effort going toward PMIX when we have the ability to share PDMP data through NABP's InterConnect? This seems a bit duplicative in terms of time, effort and resources.
4. While NIST standards are good Michigan has concerns over the following sections:

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.

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.

a. Audits – Does this mean states who participate in PMIX have to find and pay for an independent auditor who will determine of the state is meeting the PMIX Security Standard? What happens if the PMIX Working Group rejects the audit findings even

if the audit and/or intermediaries determine that the PMIX Security Standard was met by the state?

b. Evaluations – In addition to the independent Audit, states have to conduct separate evaluations and demonstrate compliance to the PMIX Executive Committee, this group different than the PMIX Working Group? What is a simple majority of the Executive Committee and who is on this Committee?
c. POA&M – It references that states and third party intermediaries shall provide progress reports, how frequent are the updates to be provided by the state and third party intermediary to the PMIX Executive Committee? When referring to the third party intermediary are you referring to the auditors or to the state's vendor used to maintain the state's PDMP?
d. Document Maintenance – The PMIX Working Group or Subcommittee of the Executive Committee will review the PMIX Security Standard twice a year and then decided whether it needs to be modified and/or updated at which point it will go through the Process to Change in accordance to the PMIX Working Group bylaws. If changes to the Security Standard are made, how much leeway or notice is given to the states to adjust to such a change? What if the changes don't make sense? Is there an appeal process?

5. Additionally, Michigan questions the governance structure and review process as well as wanting to better understand the measure that is being used and what body or 3rd party vendor is being used for certification.

Again, the state appreciates uniformity in security standards but Michigan at this time is not supportive of what has been drafted, mainly because Michigan has limited resources and our focus is to create an environment that allows for the sharing of data and information that is critical to not only our practitioners but other practitioners in other states at the time of treating patients.

Thank you for seeking state feedback and I look forward to further discussions.

Respectfully,

Kim

The Executive Committee reviewed all comments carefully. We hope that our feedback below will provide clarification on the intent of the PMIX Security Standard**.**

1. **Who is on the Executive Committee?** Provide link to Executive Committee membership on the PMIX Website. You can find a copy of the bylaws here: http://www.pdmpassist.org/pdf/PMIX_By-Laws_20180122.pdf . We are also working on a revision that will clarify terminology, add a subcommittee on compliance and address some inconsistencies/confusion in the original set. These will be posted at the same location when complete.

2. **How many states are with PMIX?** All states are represented by the governance structure of the PMIX Working Group and can be involved with the PMIX Executive or subcommittees. All states have a vote on Executive Committee membership. In addition, other stakeholder groups may serve as Advisory Members and serve on Subcommittees (http://www.pdmpassist.org/content/membership-0) . You can find information on the

Governance Structure of the PMIX organization here: http://www.pdmpassist.org/content/governance-structure-committees . The standards was reviewed at all levels of the PMIX organization. Please take a moment to look at the membership of the:

a) **Executive Committee:** http://www.pdmpassist.org/content/executive-committee

b) **Operations Subcommittee**: http://www.pdmpassist.org/content/operations-subcommittee

c) **Technical Architecture Subcommittee:** http://www.pdmpassist.org/content/technical-architecture-subcommittee

3. **Why is so much effort going toward PMIX when we have the ability to share PDMP data through NABP's InterConnect**? PMIX is not a hub. PMIX is a set of standards for states to assure that sharing partners and hubs have similar levels of security and methods for sharing data. Hubs/Intermediaries are a service that facilitates the sharing of data. PMIX provides technical standards by which the sharing occurs.

4. **While NIST standards are good Michigan has concerns over the following sections:**

a) **Audits – Does this mean states who participate in PMIX have to find and pay for an independent auditor who will determine of the state is meeting the PMIX Security Standard? What happens if the PMIX Working Group rejects the audit findings even if the audit and/or intermediaries determine that the PMIX Security Standard was met by the state**? The audit is only required of third party intermediaries. States may certify their compliance with standards through their internal mechanisms for insuring security compliance. If a state is not doing all of the aspects, we are simply asking them to disclose which controls they are not applying, submit a plan of action for items they intend to implement or request a waiver for those that they do not intend to implement.

b) **Evaluations – In addition to the independent Audit, states have to conduct separate evaluations and demonstrate compliance to the PMIX Executive Committee, this group different than the PMIX Working Group?** As stated in part a, states are only required to certify compliance and are not required to perform independent audits. The Executive Committee is the governing board of the PMIX Working group. **What is a simple majority of the Executive Committee and who is on this Committee?** A simple majority is 51%.

c) **POA&M – It references that states and third party intermediaries shall provide progress reports, how frequent are the updates to be provided by the state and third party intermediary to the PMIX Executive Committee?** Progress reports are only required for those items for which a state has an approved Plan of Action. Progress reports are required quarterly. **When referring to the third party intermediary are you referring to the auditors or to the state's vendor used to maintain the state's PDMP?** Third party intermediaries are those who provide a service that enables sharing of data between two or more organizations or states by routing transactions to and

from PDMPs. We are going to clarify the definitions and use of these terms in the document. Vendors who provide state PDMP systems are agents of the state and subject to the evaluations required of states.

d) **Document Maintenance – The PMIX Working Group or Subcommittee of the Executive Committee will review the PMIX Security Standard twice a year and then decided whether it needs to be modified and/or updated at which point it will go through the Process to Change in accordance to the PMIX Working Group bylaws. If changes to the Security Standard are made, how much leeway or notice is given to the states to adjust to such a change?** All standards changes are posted for state review with a suggested implementation date. To date, all standards adopted have had at least a year for implementation. **What if the changes don't make sense?** The design of the process to change the architecture intentionally includes various levels of review and a wide array of PDMP partners in order to develop and adopt sensible standards. It is also intended to be fluid to address changes that may occur over time. The process to change the architecture incorporates state, vendor, and other third party stakeholders. Input is sought both in development and then, through posting for comments prior to potential adoption. Both hub vendors as well as PDMP software vendors, states and other stakeholders were involved in the review of this proposal within the PMIX Executive and subcommittees. This process is designed to insure that feedback from all interested stakeholders is considered in the adoption of new standards. **Is there an appeal process?** Once adopted, a state or third party intermediary can apply for either a Plan of Action or a Waiver to any part of the standard.

5. **Additionally, Michigan questions the governance structure and review process as well as wanting to better understand the measure that is being used and what body or 3rd party vendor is being used for certification.**

Demonstrating Compliance

As is the case with other standards organizations, participation is totally voluntary. Compliance is like a professional certification, it illustrates the level of capability in a specific area. Compliance certification will allow states to attest to their level of security capability. The Operations Subcommittee is drafting a revision to the bylaws that will include a recommendation for a Standards Compliance Subcommittee. This committee will be intentionally staffed with members with expertise in the technical and other standards. We welcome members from any state interested.

If a state is already doing all of aspects of the security standard, they will simply need to certify it. If a state is not doing all of the aspects, we are simply asking them to disclose which controls they are not applying, submit a plan of action for items they intend to implement or request a waiver for those that they do not intend to implement. This will allow partner states to understand a states' security position. Often, states and their agents are conducting audits or certifications of their security. This process does not have to be exclusive to these standards.

Please do not hesitate to reach out to us if you have any questions. We sincerely appreciate your interest in and support of the PMIX Working Group.

Sincerely,

Jean Hall (KY)
Chairperson

Gary Garrety (WA)
Vice Chairperson