Prescription **M**onitoring **I**nformation e**X**change

Advancing PDMP Data Sharing Through Standardization and Innovation

March 27, 2018

Joe Fontenot, R.Ph.
Assistant Executive Director
Louisiana Board of Pharmacy
3388 Brentwood Drive
Baton Rouge, LA 70809-1700

Dear Joe:

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 21, 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.

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

> **From:** Joe Fontenot [mailto:jfontenot@pharmacy.la.gov]
> **Sent:** Tuesday, November 21, 2017 4:45 PM
> **To:** Hall, Jean S (CHFS OATS HSSMB) <jean.hall@ky.gov>; denise.robertson@arkansas.gov;
> PDMP Training & Technical Assistance Center <info@pdmpassist.org>
> **Subject:** PMIX - Information Security Standard Proposal
>
> Hello,
>
> I have reviewed the proposal and I have the following questions and comments:
>
> 1. Implementing a real standard like the NIST SP800-171 standard is a good thing. Why is it necessary to also have another set of PMIX standards?
> 2. Where does the **authority** for Sections 4.2 and what follows, come from? I am not aware of any legal agreement that exist between the PMIX Working Group and Louisiana or any other state.
> 3. Can someone define "Third Party Intermediaries"? "Agents"?
> 4. *4.2.3 - …Evaluations shall be approved by a simple majority of the Executive Committee.* What are the qualifications of the Executive Committee members to be able to approve? Once again, where does the **authority** come from?

Sincerely,

Joe Fontenot, R.Ph.
Assistant Executive Director

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

Necessity of a Security Standard

The existing PMIX specifications require the use of SOAP. SOAP is a mechanism not a standard. While SOAP is often used to comply with security standards, there are other acceptable mechanisms which would allow those using REST, SOAP, etc. to comply with the standards. The committee sought to define new security standards that would not specify a mechanism. NIST on its own was written for federal agencies. There is nothing established for Prescription Drug Monitoring Programs. The use of this subset of NIST 800-53. We are addressing the specific parts that apply to PDMPs through the use of NIST 800-171.

Authority of the PMIX Working Group and its Standards

Standards organizations typically do not have legal authority. Their authority lies in the voluntary choice to become compliant with this PMIX standard. Standards organizations are traditionally based on a group of organizations who desire to have a common way of operating certain aspects of their business in order to establish and maintain trust relationships, to conduct business efficiently and effectively, and to create a methodologies that allow them to conduct integrated business practices. No one is obligated to become compliant. However, compliance to this standard will offer an opportunity to measure your security readiness and the security readiness of your partners.

> Example: State 1 submits a certification that indicates that they are compliant with 80%, has a plan of action for 5 % and requests (and is granted) waivers for 15%

> State 2 submits a certification that indicates that they are compliant with 50% and requests waivers for 50%

Scope of Standards Compliance

You asked "How far down the line would this go? PMPs, agents and third party intermediaries-what does that mean? I don't see these defined. The independent pharmacy with an integration solution? Kaiser Permanente Mid-Atlantic?" The scope defined in the Security Standard addresses states, intermediaries and agents who are engaged in the data sharing processes. The Executive will clarify the definitions of these parties in the Security Standard. For clarification, the Executive Committee defined the following:

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

- Third party intermediaries are those agents who facilitate the exchange of information on behalf of two or more states. We plan to clarify the definitions and the use of hub/intermediary in the standards document in this way:

- Third Party Intermediary: An organization or vendor that provides a service that facilitates the exchange between PDMPs and/or between PDMPs and their stakeholders by routing transactions to and from their software systems. This includes, but is not limited to hubs such as PMP interconnect and RxCheck.

This would apply to states, their agents and intermediaries. States would be responsible for their agents who are presenting or exchanging on their behalf. It is important to note that agents of the states are subject to the requirements of states. States should be encouraged to examine their trust relationships with agents in the sharing of other states' data.

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)   Gary Garrety (WA)
Chairperson   Vice Chairperson