

Prescription Monitoring Information eXchange



Advancing PDMP Data Sharing Through Standardization and Innovation

March 27, 2018

Ralph Orr
Program Director
Virginia's Prescription Monitoring Program
9960 Mayland Drive, Suite 300
Henrico, VA 23233

Dear Ralph:

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 20, 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: Orr, Ralph (DHP) [mailto:Ralph.Orr@DHP.VIRGINIA.GOV]
Sent: Monday, November 20, 2017 5:05 PM
To: Denise Robertson <Denise.Robertson@arkansas.gov>; Hall, Jean S (CHFS OATS HSSMB) <jean.hall@ky.gov>
Cc: Brown, David (DHP) <David.Brown@dhp.virginia.gov>; Hahn, Lisa R. (DHP) <Lisa.Hahn@DHP.VIRGINIA.GOV>; Rutkowski, James E. <JRutkowski@oag.state.va.us>; Jenkins, Robert (DHP) <Robert.Jenkins@dhp.virginia.gov>
Subject: PMIX security standard Comments
Importance: High

Denise and Jean,

I am very pleased to see the change to the NIST standard.

However, I have very serious concerns about the rest of Section 4. (I view 4.1 as a statement of fact that is already in place today as a result of existing policies and requirements in states)

1. I am not aware of any MOU, contract, compact, etc. that any state has with the PMIX Working Group. Where does the authority for Sections 4.2 et seq come from?

2. 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?
3. I am concerned with the idea that the Executive Committee is apparently giving itself authority to approve (or disapprove) evaluations without legislative or other authority. This seems like overreach, what expertise do the members possess to determine such results? If this were to somehow be put in place, what would actually happen, who would enforce, and what if a state does not agree with evaluation results or does not wish to participate or cannot participate due to state law?
4. Virginia already has extensive and rigid security requirements in place with all vendors and for applications in use in the Commonwealth. The Agency IT Director has reviewed the draft proposal and stated the PMP cannot agree with the contents of this draft.
5. Review of language by Program Counsel at the Office of the Attorney General resulted in statement that program security information is confidential, therefore the PMP has no authority to provide it.

Lastly, who is actually paying for all of this? Seems like this is a lot of redundancy for processes already in place that will end up getting paid at taxpayers' expense.

Ralph

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

Authority of the PMIX Working Group and its Standards

The 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)
Chairperson

Gary Garrety (WA)
Vice Chairperson