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

< PMIX />

Advancing PDMP Data Sharing Through Standardization and Innovation

March 27, 2018

Prescription Drug Monitoring Program Project Manager
Oklahoma PDMP
Oklahoma Bureau of Narcotics
419 NE 38th Terrace
Oklahoma City, OK 73105

Dear Sir/Madam:

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 October 28, 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:** Vogt, Don
> **Sent:** Saturday, October 28, 2017 12:18 PM
> **To:** Hall, Jean S (CHFS OATS HSSMB) <jean.hall@ky.gov>; Donald Gabbin <Donald.Gabbin@ijis.org>
> **Cc:** pknue@pdmpassist.org; Hopkins, Dave (CHFS OATS HSSMB) <Dave.Hopkins@ky.gov>; Jim Giglio (jgiglio@pdmpassist.org) <jgiglio@pdmpassist.org>
> **Subject:** Re: NIST 800-171 r1
>
> Jean,
>
> Comments as I read through the standards:
>
> **Limit Access to Authorized Users**
>
> This is the tricky part and the hardest to control. It also happens to be the one that tends to worry me the most. Some states are moving to a 'trust' model, allowing user and device authentication to occur outside of the PMP system. This occurs with limited auditing capabilities by administrators, primarily relying on logging. Basically an agreement that the 'trust' partner will provide adequate security controls and logging to satisfy a state that unauthorized access is

> not occurring. Thus far, we have never had a serious breach of PMP data. I would want to make sure that any new controls, or lack thereof, don't increase the risk that it could happen. This issue tends to transcend technical restrictions as access holes could be allowed by bad policy with unintended consequences. For instance, we allow delegates in the portals but they are carefully controlled. A technical specification where a 'trust' relationship exists could greatly expand access without the direct knowledge of the PMP. However, I would also say, that a technical specification alone cannot adequately address this issue.
>
> A weakness, though not of the proposed NIST standards, are that PMP administrators realistically don't have the time to audit the security of their current systems effectively or efficiently. I just don't see they would have the ability to audit activity of a third party, especially in a 'trust relationship'. This is a potentially serious problem. For instance, remote connections to PMP data that is being authenticated by a third party trust system should not be allowed. Yet, another policy based decision.
>
> In this regard, I would encourage the PMIX Board to consider also drafting policy recommendations for the states when allowing access to PMP data via third party systems outside direct state authentication systems. This recommendations seems to be supported in sections of 3.2, 3.4, 3.5, 3.11 and 3.12 of the document.
>
> Overall, I am very much in favor of adopting the NIST security structure over the existing PMIX ones. A positive step forward. However, I also don't want to further delay sharing using RxCheck.
>
> Don

The Executive Committee reviewed all comments carefully. We agree that it is impossible to audit all aspects of the exchange of information, including authentication. We suggest that the trust relationships that are established have agreements that place responsibility on trusted partners for their own accountability to security. This is a typical practice in the security of information. This could be done via Memoranda of Understanding.

Trust relationships agreements can address specific subsets of security. Below is an example of trust relationship language from an agreement used by the Kentucky Prescription Drug Monitoring program:

> "Administrative Regulation 902 KAR 55:110 specifies that as a condition precedent to the disclosure of data or a report pursuant to KRS 218A.202 (6) (f), a hospital or long term care facility shall maintain, and provide upon request by the cabinet, a copy of the hospital or long-term care facility's policy for the management of eKASPER data and reports. You do **not** need to provide a copy of the policy at this time. The policy must contain the following information.
>
> - A description of the hospital or long-term care facility's internal procedures for educating the designated employee or employees on the:
> - proper use of the eKASPER system;
> - prohibition on the improper use or intentional disclosure of eKASPER data to unauthorized individuals; and

- Sanctions imposed for the improper use or intentional disclosure of eKASPER data to unauthorized individuals, including criminal misdemeanor offenses.”

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 S Hall Gary M Garrety

Jean Hall
Chairperson

Gary Garrety
Vice Chairperson