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

Advancing PDMP Data Sharing Through Standardization and Innovation

March 27, 2018

Dave Hopkins
David Vick
KASPER
275 E Main Street 5ED
Frankfort, KY 40621

Dear Dave and David:

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 29, 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 from the Cabinet for Health and Family Services, Office of Administrative and Technology Services' Security Team to the PMIX Executive Committee:

> "Though NIST 800-171, which PMIX will have to adhere to, is a subset of 800-53 and FIPS 200, based on the risk exposure that comes with other states' shared data, I'd suggest that PMIX reiterate the following mandatory requirements:
>
> 1. Two-Factor authentication must be used for ALL user access without exception.
>
> 2. ALL sensitive data must be encrypted at all times at rest (Database, Filesystems, Backups, Archives, User Devices, Mobile Devices, Portable Storage Devices etc.) and in-transit (TLS 1.2 or higher, VPN, SFTP etc.).
>
> 3. ALL remote users must use security hardened and enterprise managed devices with two-factor authentication for both user and devices with end-to-end secure channels.
>
> 4. All software, firmware, hardware accessing or housing PMIX data must use only manufacturer supported versions and kept up-to-date."

The Executive Committee reviewed all comments carefully. We agree that all areas addressed in your comments are important components of the standard. We would like to be clear that the PMIX Security Standard will only apply to ***shared data*** in transit and at rest. This standard will not address security standards for a state's Prescription Drug Monitoring Programs in state data except when that data is shared with other states. Current state data sharing agreements via the PMPi and RxCheck hubs do not

allow other state data retention. Finally, while we agree that Multifactor authentication is ideal, its use of having two of these three requirements for authentication, knowledge (something the user knows), possession (something the user has) and inherence (something the user is) are not feasible for many states at this time. As this would significantly limit states' ability to share, we will not require multi-factor authentication as a part of this standard. Since the standard does not supersede any state security requirements, your state may choose to require this of your partner states when sharing data.

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
Chairperson

Gary Garrety
Vice Chairperson