ACLU of Oregon Position on PDMP 2016 Session Bill: HB 4124)

ACLU of Oregon will be neutral on HB 4124, so long as an amendment is adopted which requires OHA to periodically ensure Health IT Systems' ongoing compliance with privacy and security standards set in rule.

Our concerns have been addressed as follows:

Concerns	How concerns have been addressed
Ensuring that this bill will not open up PDMP data to more permissive access by law enforcement.	• Under current law, PDMP may only be accessed by law enforcement with a warrant. This is a crucial access restriction that was deliberately included in the original bill creating the PDMP. Despite the fact that the legislature clearly stated its intent that law enforcement get a warrant before accessing PDMP data, law enforcement has attempted to access such data without a warrant. This lead to litigation in the US District Court of Oregon. Judge Haggerty ruled that law enforcement must have a warrant to access PDMP data. The case is now on appeal to the 9th Circuit. • The bill language does not change anything regarding law enforcement access. As such, it should not change the warrant requirement for law enforcement access to PDMP data. We understand that this point will be discussed with legislators during committee hearings, in order to clarify and reemphasize legislative intent not to change the current standard which requires law enforcement to obtain a warrant in order to access PDMP data.
Privacy and security of Health Information Technology (HIT) systems including Health Information Exchanges (HIEs) and electronic health record systems that will have access to PDMP data; note that EDIE is one of these systems	• Language of bill requires OHA to ensure that HIT systems meet privacy and security requirements of HIPAA and OHA rules. Note that Courtni Dresser is checking with LC to see if it would be better to say the system must meet "all" privacy and security requirements. It currently says "any." • Bill amendment will be introduced that requires OHA to periodically ensure HIT systems' ongoing compliance of privacy and security standards set in rule, including HIPAA. • OHA will promulgate rules to ensure privacy and security of systems beyond what is required under HIPPA. • OHA has committed to working with the PDMP Advisory Commission and its members in crafting privacy and security rules. • ACLU of Oregon has requested its inclusion in privacy and security discussions as rules are contemplated and adopted.

Concerns	How concerns have been addressed
Authentication of HIT system users to ensure that they are authorized to access PDMP; ensuring that a single log-in doesn't leave the system open to unauthorized users having access	• Bill language requires that anyone accessing PDMP data through an HIT system must be an authorized PDMP user. We understand that this will happen one of two ways: ○ For EDIE, only authorized PDMP users will receive PDMP results through EDIE notifications (e.g., everyone in the ER will be an authorized PDMP user before PDMP data become available through EDIE). ○ For HIEs or electronic health record systems, authentication will occur at login, results will only be displayed in a view-only window, and system will time out with no information retained
Ensuring that data from the PDMP database is not migrated to the HIT system, but is instead merely viewable through the HIT system and not retained (to ensure that HIT users who are not authorized PDMP users will not obtain access to PDMP data)	• Bill language prohibits permanent retention of PDMP data in HIT system except for purpose of audits and maintaining patient records. • We understand that this means data will only be retained in short-term memory while it is in the process of being accessed through the HIT system, except for data retained for the following two reasons. • "For purpose of audits": We understand that this means audit data will not be accessible to HIT users, but will merely be accessible to individuals conducting audits • "For purpose of maintaining patient records": We understand that practitioners are required to maintain some patient records under current applicable laws. We understand that this language will allow practitioners to save the PDMP data that they have viewed in order to comply with this legal requirement. Practitioners are able to retain PDMP data in the patient record under current law and practice.
Prevention of unsolicited reports to HIT users which include PDMP data	• We understand that this will not be allowed under the bill's language.
Disallowance of wildcard searches and searches which could allow accidental access to a person's account who is not a patient	• We understand that that wildcard searches will not be allowed, just as they are not allowed when using the PDMP system. • We also understand that data points will be required which will ensure that only the patient's records are accessed, just as occurs under PDMP.