Prepared for

Office of the National Coordinator
for Health Information Technology,
in partnership with the Substance Abuse
and Mental Health Services Administration

Enhancing Access to Prescription Drug Monitoring Programs Using Health Information Technology:

Work Group Recommendations

August 17, 2012

Version 1.1

MITRE
7515 Colshire Drive
McLean, VA 22102

Record of Changes

Version Number	Date	Author/Owner	Description of Change
1.0	May 29, 2012	J. Hammer	1.0
1.1	August 17, 2012	J. Hammer	1.1

Table of Contents

List of Figures

List of Tables

1 Introduction: Findings and Recommendations

Prescription drug misuse and overdose is one of the fastest growing health epidemics in the United States. In 2010, U.S. pharmacies dispensed enough opioid pain relievers to medicate every adult in America with a 5 mg hydrocodone every 4 hours for an entire month.[1] As of 2010, nearly 5% of people 12 years or older in the United States stated that they used opioids nonmedically.[2] The amount of controlled substances dispensed and used nonmedically is alarming considering that the Centers for Disease Control and Prevention (CDC) reported that in 2009, opioid drugs, including oxycodone and hydrocodone, caused more than 15,500 overdose deaths—a number that is increasing.[3] The overdose death rates for all drugs including opioids increased in Louisiana, Mississippi, Kentucky and West Virginia from the years 1999 to 2008.[4] In 2008, New Mexico and West Virginia reported the highest drug overdose death rates at 27 and 25.8 deaths per 100,000 population respectively.[5]

To address the prescription drug abuse problem, many states have established Prescription Drug Monitoring Programs (PDMPs). These programs collect prescription data on medications that the federal government classifies as controlled substances and other non-controlled substance drugs. Their purpose is to reduce prescription drug abuse and diversion. PDMPs are not federally operated; they are statewide electronic databases that collect, monitor, and analyze electronically transmitted prescribing and dispensing data submitted by pharmacies and dispensing physicians. PDMP information can be useful to improve decision-making when prescribing and dispensing scheduled prescription drugs, but not all states benefit equally from these programs. Although this data is made available to authorized healthcare professionals in the majority of states, access is generally optional.

States' use of PDMPs also varies because these state programs were created for a variety of reasons, including law enforcement, legal and regulatory compliance, and, more recently, patient care and safety. This led to great variability in the design, process, and functions among PDMP systems. The first PDMPs were created in the 1930s. In 1992, only 10 operational programs existed.[6] As of July 31, 2012, there are 43 operational programs (see Figure 1), yet technology and policy issues and inconsistencies impact their effectiveness. Consequently, there is a movement by organizations such as the National Alliance for Model State Drug Laws (NAMSDL) and the Alliance of States with Prescription Monitoring Programs (Alliance) to make laws and technological processes for PDMPs consistent across the states. Modern

---

[1] CDC, "Vital Signs: Overdoses of Prescription Opioid Pain Relievers – United States, 1999–2008," *Morbidity and Mortality Weekly Report*, vol. 60, no. 43, pp. 1487-1492, Nov. 2011.

[2] Substance Abuse and Mental Health Services Administration. Results from the 2009 National Survey on Drug Use and Health: Volume 1: Summary of national findings. Rockville, MD: US Department of Health and Human Services, Substance Abuse and Mental Health Services Administration, Office of Applied Studies; 2010. http://oas.samhsa.gov/nsduh/2k9nsduh/2k9resultsp.pdf.

[3] CDC. (2012). *CDC National Vital Statistics System*. Department of Health and Human Services (HHS). http://www.cdc .gov /nchs /data _access/Vitalstatsonline .htm#Downloadable.

[4] CDC, "Vital Signs: Overdoses of Prescription Opioid Pain Relievers – United States, 1999–2008," *Morbidity and Mortality Weekly Report*, vol. 60, no. 43, pp. 1487-1492, Nov. 2011.

[5] Ibid.

[6] K. Blumenschein et al., "Review of Prescription Drug Monitoring Programs in the United States," Kentucky All Schedule Prescription Electronic Reporting Program (KASPER), June 2010.

technology can improve access to PDMP data, and this increased access will ultimately improve patient care. Figure 1 shows the states that currently have an operational PDMP as well as those with enacted legislation that do not yet have a functioning program.

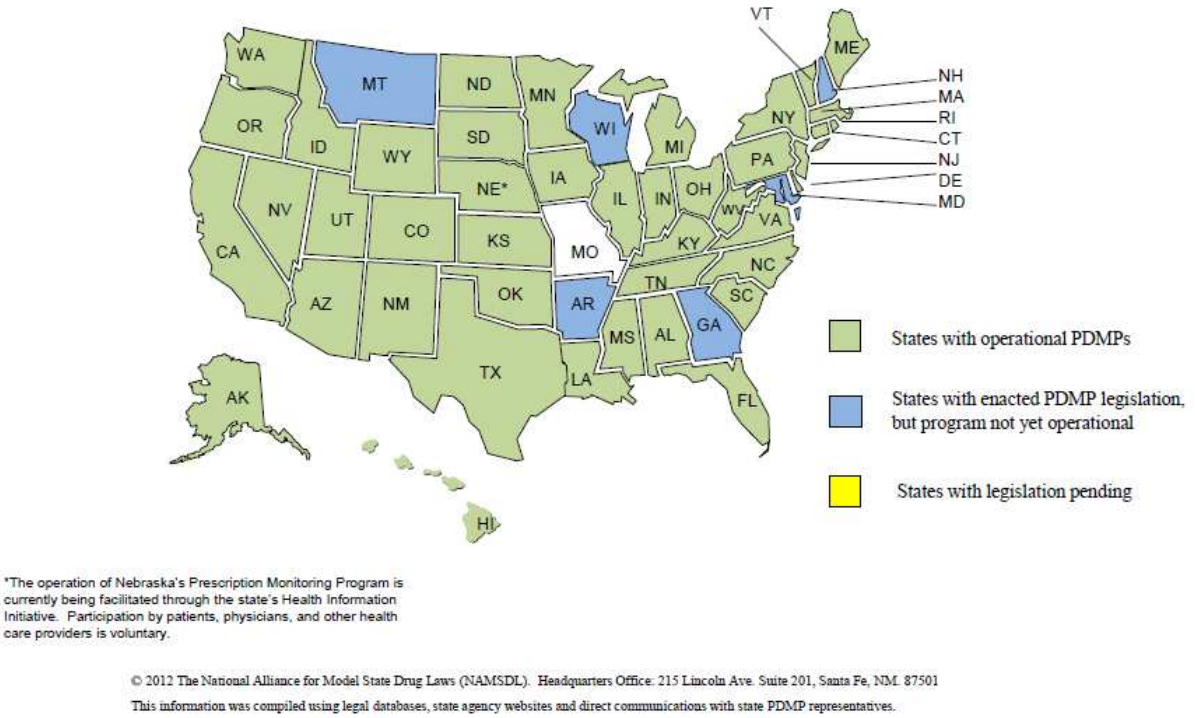


Figure 1. Status of State Prescription Drug Monitoring Programs

In recognition of these important issues, the Obama Administration issued an Action Plan in 2011 to address the prescription drug abuse crisis.[7] A subsequent White House Roundtable on Health Information Technology and Prescription Drug Abuse, held on June 3, 2011, concluded that prescription drug abuse is a preventable problem requiring immediate attention.[8] As a result, the Office of the National Coordinator for Health Information Technology (ONC), in collaboration with the Substance Abuse and Mental Health Services Administration, the CDC, and the Office of National Drug Control Policy, contracted with The MITRE Corporation to identify ways to leverage health information technology (IT) to improve access to PDMPs.

The current healthcare landscape is changing so that there is an increase in the adoption of health IT. As of 2010, it is estimated that over 50% of providers in the United States adopted and currently use electronic health record (EHR) systems. Figure 2 illustrates this increase in the percentage of office-based physicians with electronic medical records or EHRs in the United

[7] Executive Office of the President of the United States. (2011). "Epidemic: Responding to America's Prescription Drug Abuse Crisis." http://www.whitehouse.gov/sites/default/files/ondcp/policy-and-research/rx_abuse_plan.pdf.

[8] Prescription Drug Abuse and Health Information Technology Work Group. (2011). "Action Plan for Improving Access to Prescription Drug Monitoring Programs through Health Information Technology." http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_0_9025_3814_28322_43/http%3B/wci-pubcontent/publish/onc/public_communities/_content/files/063012_final_action_plan_clearance.pdf

States from 2001 to 2010.[9] Health IT systems like these can be used to improve the workflow of accessing PDMP information. For example, states such as New York passed legislation that requires healthcare professionals to check the PDMP before prescribing controlled substances. Health IT systems would be useful for automating queries in states where mandatory PDMP checks are required. The use of health IT to increase access to PDMP information is a core component of the Enhancing Access to PDMPs Project.

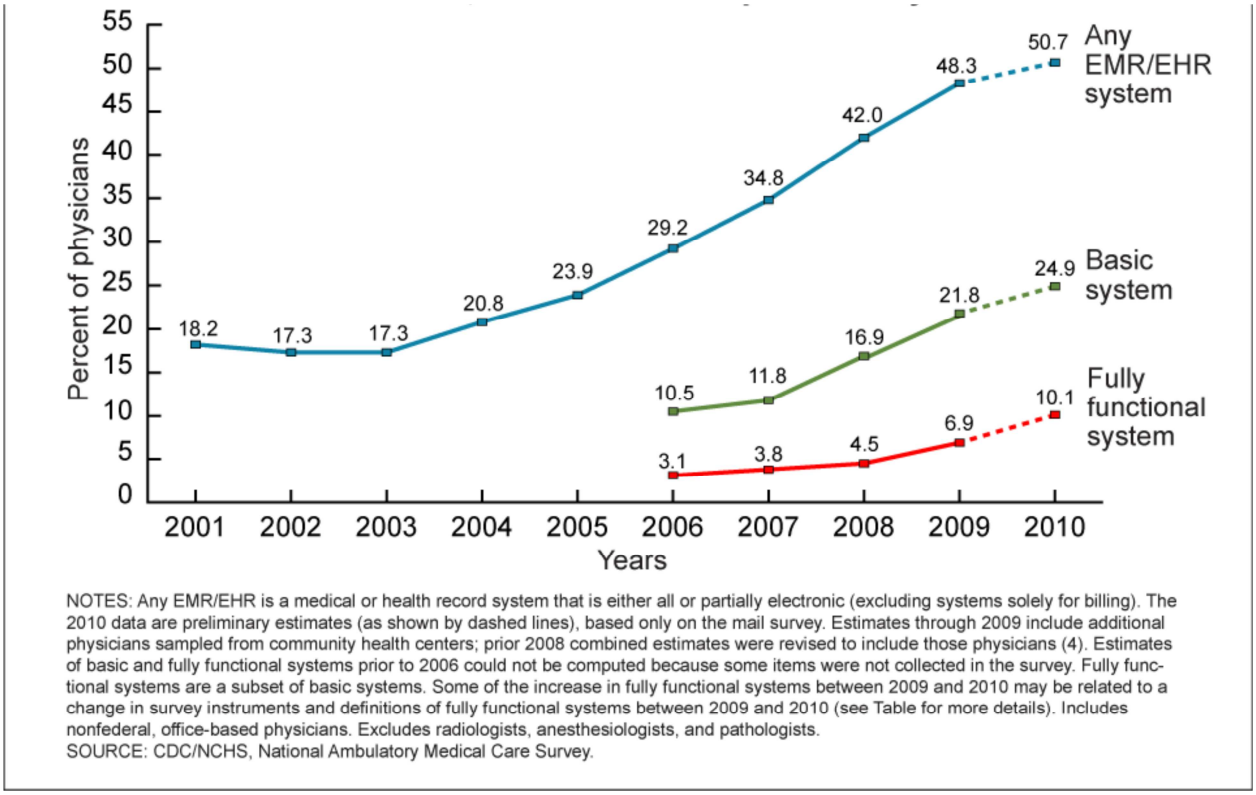


Figure 2. Adoption of Electronic Health Records in the United States from 2001 to 2010

As part of the Enhancing Access to PDMP effort, MITRE convened Work Groups comprising individuals from the healthcare community, industry, trade and advocacy groups, and state and federal government. The project is also conducting pilot studies to demonstrate opportunities to improve access.

The project's purpose is to use health IT to increase timely access to PMDP data and thus to reduce prescription drug misuse and overdose. Specifically, the project focuses on enhancing access for three types of medical professionals within a variety of care settings:

- Ambulatory clinic healthcare providers (e.g., physicians, nurses, nurse practitioners)
- Emergency department (ED) physicians

[9] C. J. Hsiao et al. "Electronic Medical Record/Electronic Health Record Systems of Office-based Physicians: United States, 2009 and Preliminary 2010 State Estimates," *Health E-Stat*, December 2010. http://www.google.com/url?sa=t&rct=j&q=&esrc=s&frm=1&source=web&cd=1&ved=0CIkBEBYwAA&url=http%3A%2F%2Fwww.cdc.gov%2Fnchs%2Fdata%2Fhestat%2Femr_ehr_09%2Femr_ehr_09.pdf&ei=yUUZUKr4AsL30gHIoYGgBg&usg=AFQjCNFkSRd9cWku_jZ0zM9QwwDlHDgpsw&sig2=AeAo9SZB6SPzJkTchvz7rg.

- Dispensing pharmacists.

In this report, physicians and pharmacists are referred to as prescribers and dispensers, respectively. The following chapters enumerate specific goals that the Work Groups addressed.

1.1 How to Use This Document

This report contains multiple levels of information tailored to different audiences, thus there are different ways to approach reading the document, as shown in Figure 3:

1. **Read the Top 7 Findings and Recommendations**
   Section 1.2 presents the most impactful recommendations. This serves as a starting point for people in the PDMP and Health IT community who already have a context for understanding PDMPs and their current state.
2. **Read the Summary of Impediments for Clinical Decision-Makers in Accessing PDMP Data**
   Section 1.3 presents summaries of key recommendations that are organized by impediments that hinder PDMP effectiveness today. This section is geared for all audiences wanting an overview of the PDMP issues and a high-level description of key recommendations to overcome those obstacles.
3. **Read the Details**
   This document provides an in-depth look at five unique topic areas. Sections 2–6 contain a detailed set of recommendations complete with rationales, products, and/or solutions for implementation. The chapters are organized by the Work Groups convened to examine each topic. PDMP administrators, health IT vendors, lawmakers, and others involved in the intricacies of PDMPs or health IT will find this information valuable.

Figure 3. Paper Structure

1.2 Top 7 Findings and Recommendations

This report summarizes the findings, recommendations, and products of the Work Groups. The views, opinions, and/or findings contained in this report are those of The MITRE Corporation and should not be construed as official government position, policy, or decision unless so designated by other documentation.

The Work Groups developed over 45 individual recommendations to enhance PDMPs. However, seven stand out as some of the most important to increase the effectiveness of PDMPs for the user community. Figure 4 sorts these seven recommendations into three primary groups: States, PDMP Community, and Vendors.

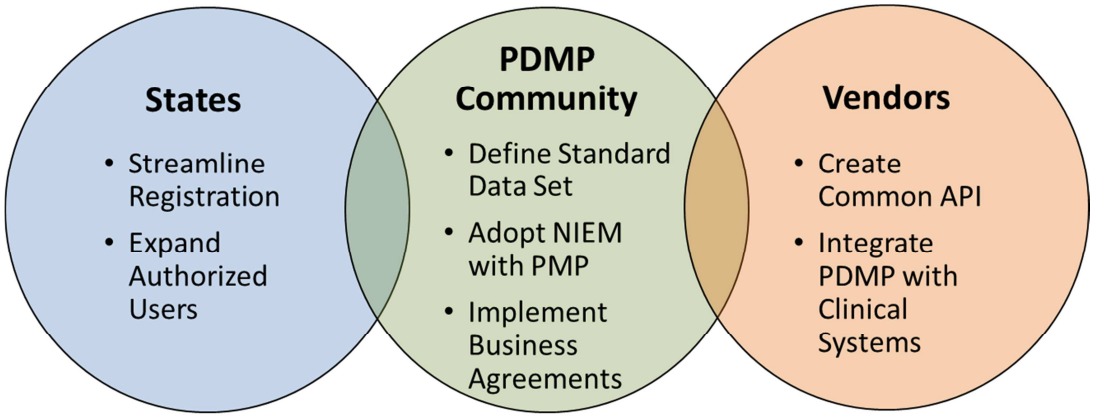


Figure 4. Top 7 Recommendations

These three groups bear some of the greatest responsibility for enhancing access to PDMPs for use by prescribers and dispensers. Some of the recommendations require multi-organization coordination, while others can be undertaken by individual entities. In all cases, these seven recommendations are central to enhancing access to PDMPs:

- **Streamline the registration process** – PDMP registration should improve with automatic or mandatory registration.
- **Expand the pool of authorized healthcare professionals permitted to access PDMP data** – Authorized users should have the ability to delegate their access to other healthcare professionals under their supervision.
- **Create a common application programming interface (API) for PDMP system-level access** – PDMPs need technology to allow other systems to query and retrieve data to supplement the standalone web portals that exist today for user-level access.
- **Integrate access to the PDMP data into the clinical workflow** – PDMP information should be integrated in EHR and pharmacy systems to varying degrees of sophistication depending on resources and expertise available.
- **Define a standard set of data that should be available in PDMP reports** – Every report should contain a standard set of PDMP information.
- **Adopt the National Information Exchange Model (NIEM) Prescription Monitoring Program (PMP) specification** – This specification should be formally established as the standard for PDMP data exchange.
- **Implement an agreement framework and model agreements** – Standard business agreements with third-party intermediaries should be widely used to facilitate PDMP data sharing.

These seven recommendations serve as a starting point for PDMPs and related stakeholders. They can be implemented to different degrees with great success. While some are more immediate and others require a greater degree of community organization, they are all critical to increasing PDMP usage and moving toward greater integration with other health IT.

1.3 Impediments for Clinical Decision-Makers in Accessing PDMP Data

PDMPs collect and store information about prescribing and dispensing controlled substance data. Prescribers and dispensers may use this information to (1) identify patients who are abusing or diverting prescription drugs and (2) make clinical decisions regarding controlled substances at the point of care. While PDMPs contain useful information, several impediments may hinder prescribers and dispensers from accessing or using this information:

1. **Low Usage** – PDMPs are not used as much as desired by the healthcare community and state governments, given their value to clinical decision-making, because of issues with awareness and system registration and because the data is not current or real-time.
2. **Limitations on Authorized Users** – Members of the care team supporting prescribers and dispensers often are not permitted access to PDMP systems.
3. **Current Processes Do Not Support Clinical Workflows** – The use of standalone Web portals and unsolicited reports does not support clinical practices and workflows.
4. **Low Technical Maturity to Support Interoperability** – Prescribers and dispensers have insufficient access to the PDMP data. Existing solutions are inflexible and lack support for automated queries and reporting.
5. **Lack of Business Agreements** – The business and health IT landscape increasingly contains third-party intermediaries that can facilitate the exchange of information; however, strong model business agreements are needed to adequately protect PDMP information.

1.3.1 Low Usage

Considering their value to clinical decision-making, PDMPs are not used frequently. According to the Bureau of Justice Assistance (BJA) performance measures in 2010, many state registration rates are low, ranging from 5 percent to 39 percent of potential authorized users within a state.[10] These low registration rates are concerning because of the pervasive prescription drug abuse problem. A review of outpatient opioid prescription data from 2000 to 2009 shows that opioid prescriptions are on the rise.[11] Results of the study indicated that 257 million prescriptions for opioids were dispensed in 2009. Of these prescriptions, 3.8 million individual patients were prescribed extended release or long-acting opioids. PDMP information is especially relevant for prescribers and dispensers considering that, as of 2009, the majority (60%) of opioid

[10] J. Eadie, BJA. (June 21, 2012). "PDMP Project Question," email message to L. Canzone.

[11] "Risk Evaluation and Mitigation Strategies (REMS) for Extended-Release and Long-Acting Opioid Analgesics," *Joint Meeting of the Anesthetic and Life Support Drugs Advisory Committee and the Drug Safety and Risk Management Advisory Committee*, Adelphi, MD, 2010. http://www.fda.gov/downloads/AdvisoryCommittees/CommitteesMeetingMaterials/Drugs/AnestheticAndAnalgesicDrugProductsAdvisoryCommittee/UCM217510.pdf

prescriptions were dispensed from retail pharmacies, and most prescriptions were written by primary care physicians (27%). Further, emergency department physicians were one of the top five prescribers for opioids. There is a clear need to increase PDMP usage among dispensers and primary care and emergency department prescribers. Yet, there are several underlying reasons for the low usage rates:

- The registration process requires time-consuming and cumbersome steps that are an impediment to granting access to the system. For example, in some cases, potential authorized users must notarize their medical license and government identification before they receive access.
- Prescribers and dispensers are concerned that by using PDMPs, they may be at risk for increased liability.
- Many prescribers and dispensers are unsure of how PDMP data may support the care they provide. They also lack awareness and education about the value of these data.[12]
- Patient information in statewide PDMP systems may not be current. As a result, prescribers and dispensers often do not trust PDMP data and therefore do not feel that they can rely upon it when a controlled substance is prescribed or dispensed.

The Work Groups identified the following recommendations, which may increase PDMP use:

Recommendation 1a: Streamline the registration process – States should review previously enacted registration policies and requirements to determine if they can be streamlined to facilitate higher registration rates. Some states require notarized copies of medical licenses to receive access to PDMPs; however, policies or procedures may exist that can simplify this process. Once policies that facilitate the registration process are implemented, corresponding technology can be developed, such as Web portals for electronic registration.

Other solutions, such as automatically registering prescribers and dispensers to PDMPs when they are licensed, may require additional time for implementation. Further, states might consider requiring registration to expand the pool of authorized users.

Recommendation 1b: Provide increased protection for authorized users to encourage greater use of PDMP systems – Legal liability is an important issue, and many state PDMP laws provide protections for prescribers and dispensers. But these protections are neither universal nor consistent from state to state. To address the disparate treatment of liability for authorized users, prescribers and dispensers should not be civilly or criminally liable for complying with state PDMP laws that require them to submit or share data as part of their legitimate professional activities.

Recommendation 1c: Increase awareness and education about the value and use of PDMP data at the point of care – This can be achieved by creating awareness campaigns to increase the visibility of PDMP systems and their potential value and by educating prescribers and dispensers about the role of PDMP information in the drug

[12] T. C. Green, "How Does Use of a Prescription Monitoring Program Change Medical Practice?" *Pain Med*, Substance Abuse and Mental Health Services Administration, "National All Schedules Prescription Electronic Reporting Act of 2005 Program Grants," 2005. http://www.pmpalliance.org/pdf/FY-2011-NASPER-RFA.pdf.

abuse crisis. In addition, awareness and education programs also should address how to access and safeguard sensitive PDMP data appropriately. All authorized users of PDMP systems, regardless of whether they submit data to the program or query these databases, should receive appropriate education regarding the proper use of these systems.

Recommendation 1d: Consider more real-time transmission of dispensed data to PDMPs to build trust in the currency of the information – Dispensers report data on filled prescriptions to PDMP systems, but in most states, transmissions can occur weekly or even monthly. The reporting period for PDMP data directly affects the currency of this data; less frequent reporting results in less current data. Within the next year, it is possible to improve data currency with more frequent reporting and, ideally, real-time reporting. Additionally, these reports should be in an electronic format, as opposed to mailing or faxing paper reports. Ultimately, this will improve PDMP data currency, and as a result, prescribers and dispensers will be more likely to rely on this information as their trust in the data increases.

1.3.2 Limitations on Authorized Users

Members of the care team supporting prescribers and dispensers often are not permitted access to PDMP systems. As of July 2012, only 17 of the 43 states with operational PDMPs allow prescribers to access their patients' controlled-substance drug histories, but they may not delegate this authority to their staffs.

Recommendation 2: Expand the pool of authorized healthcare professionals permitted to access PDMP data and grant these professionals the authority to appoint delegates who can access this data on their behalf. Prescribers and dispensers, also known as "authorized healthcare professionals," should be able to delegate PDMP access to others. This delegation should be subject to the supervising professional who is accountable for the delegates' actions. Enabling healthcare professionals to appoint authorized delegates would not only bring state laws and policies in line with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and current real-world clinical practices, but it also would increase the number of authorized users. Since some states prohibit authorized users from delegating access, this recommendation would require new legislation. This may be a lengthy process, depending on current state laws, but from 2011 to 2012, the number of states that permit access delegation grew from 10 to 17. States such as Iowa and Minnesota permit authorized healthcare professionals to delegate access to PDMP data, provided the delegates register for their own accounts in the PDMP system and are held accountable as agents of the healthcare professional.

1.3.3 Current Processes Do Not Support Clinical Workflow

It is crucial that prescribers and dispensers have relevant PDMP information when interacting with patients. Prescribers and dispensers have limited time to retrieve and view this information, and they want to obtain it at the right point in the clinical workflow to help inform complex, controlled-substance prescribing decisions. Therefore, the Work Groups recommended creating mechanisms that provide the PDMP data at the ideal point. This could be as simple as a link within an EHR that healthcare professionals use to access the state's PDMP Web portal, to more robust solutions in which EHR systems query and store the data within the patient's record.

In addition, some PDMPs send unsolicited reports to prescribers and dispensers when patients exceed a predetermined threshold set by state PDMPs. For example, a dispenser may receive an unsolicited report for a patient who exceeds six prescriptions from six prescribers in a one-month period.[13] The Work Groups have noted several concerns regarding unsolicited reports; specifically, unsolicited reports are of less value to clinical decision-making. These reports are unanticipated by the recipients and currently are delivered through a variety of methods, including fax or postal mail; yet, these notifications do not occur frequently enough to support current workflows. Often the information is not available at the right time, such as when the patient is present and decision-making is occurring. Further, attaching a paper report to a patient's record in an EHR can be difficult.

Improving access to and the usability of PDMP data may reduce the need for unsolicited reports in the long term; however, the following solutions may quickly improve the value of current processes for accessing PDMP information:

Recommendation 3a: Integrate access to the PDMP Web portal into the clinical workflow – Reducing the effort required to use PDMP data is critical for increasing use. Since these users already work within EHR and pharmacy systems, if the PDMP data is available in these user interfaces (UIs), there will be minimal disruption to their normal workflow. This single point of access for PDMP and patient health data also would eliminate the time and resources wasted by multiple user accounts, system logons, and multiple UIs.

Recommendation 3b: Consider secure electronic communication of unsolicited reports – Secure messaging options, such as email, eFax, and Direct messaging, will help shift away from postal mail and fax reports. Lightweight, standardized, secure messaging technologies such as Direct messaging will provide more timely access to these reports and will provide a more effective means to attribute the report to a particular patient.[14]

Recommendation 3c: Prescribers and dispensers should receive an alert or notification when they receive an unsolicited report concerning a patient – One of the primary limitations to using unsolicited reports is that they are unanticipated, so they often are overlooked. Prescribers and dispensers would benefit from an electronic alert or notification upon receiving the unsolicited report. Integrating this alert with the patient's records, such as in the EHR, would be ideal.

Recommendation 3d: Provide a variety of mechanisms for PDMP access at the point of care – PDMP system queries should occur around the time that the patient is seen in the clinical setting. This ensures that patient information is current during clinical decision-making. Short-term solutions include user-initiated querying (via a link or button in the EHR or pharmacy system) as well as longer-term ideas, such as systems generating queries at appointment-making, patient check-in, or point of prescribing. Healthcare organizations such as hospital and ambulatory systems should work with their EHR or pharmacy system vendors to identify the optimal workflows for their organizations. The one type of transaction not favored by the Work Groups was

[13] Ibid.

[14] Direct provides a standard and universal method for healthcare professionals to send secure messages over the Internet. See http://wiki.directproject.org/ for more information.

co-transmission, or partnering the PDMP data request with other requests such as third-party payer eligibility checks. Co-transmission was not ideal because it placed PDMP information in a suboptimal position in the user's workflow.

Recommendation 3e: Define a standard set of data that should be available to support clinical decision-making – There currently is no standard for the specific data that must be included in all PDMP reports. The Work Groups identified a recommended standard data set to be included in a PDMP report, including data elements for patient, prescriber, dispenser, and prescription information. This data set was based on the American Society for Automation in Pharmacy (ASAP*)* 2009 standard,[15] which is used to report dispensing data. In addition, the Work Groups identified a subset of the most relevant controlled-substance history for patients to be displayed in EHR and pharmacy systems. Lengthy or cluttered displays of PDMP information decrease effective use. In an ideal scenario, a prescriber would open a patient's record in the EHR to view a shortened list of the patient's most relevant PDMP information. This shortened list would contain the most valuable 10 items from the PDMP report. At the top of the shortened list, there would be a summary including the total number of prescribers, dispensers, and prescriptions for controlled substances for a patient over the last year. This summary and shortened list would allow prescribers and dispensers to quickly view only the most valuable PDMP information and determine the need to retrieve the entire set of data in a PDMP report.

1.3.4 Low Technical Maturity to Support Interoperability

To provide timely and accurate information at the point of care, it would be helpful to automate the query of patient PDMP reports and the availability of the reports in the workflow at the time of clinical decision-making. However, there is a lack of technical, system-level access and standards among PDMPs and the EHR and pharmacy systems that prescribers and dispensers use to support automated queries and reporting. In addition, no formal standards or specifications exist for sharing a PDMP report electronically with a prescriber or dispenser. Several options are available to PDMPs for sharing reports with other states, some of which include the use of data sharing intermediaries, or hubs. Specifically, two interstate PDMP data-sharing exchanges are in operation today: the Prescription Monitoring Program Interconnect (PMPi) and RxCheck. These solutions are converging on existing common standards that will enable nationwide query and reporting capability. However, despite the progress to date, the standards were created primarily to support sharing among PDMP systems; incorporation of additional user groups such as dispensers and prescribers may require modification or enhancement to the process and specifications. Considering the PDMP landscape, several recommendations can be implemented within a year to improve interoperability.

Recommendation 4a – Adopt the National Information Exchange Model (NIEM) Prescription Monitoring Program (PMP) specification as the common specification for exchanging PDMP reports with prescriber and dispenser organizations. This specification is already in use for PDMP data exchange, is reusable and extensible, and has become a *de facto* standard for data exchange. The NIEM PMP information exchange specification

[15] 2009 American Society for Automation in Pharmacy (ASAP) Prescription Drug Monitoring Program Standard, Version 4.1, 2009.

currently is the basis for PDMP interstate data access and exchange. The Prescription Monitoring Information Exchange (PMIX) architecture has already implemented the foundation for the NIEM PMP data and messaging specifications for interstate data exchange. In addition, PMPi also uses the NIEM PMP specification. Formalizing this specification would establish a single standard so that vendors could confidently move forward and build solutions for interoperable PDMP data exchanges. One option would be to formally add the NIEM with PMP extension data exchange specification to the NIEM Health Domain managed by ONC. This would expand the specification from an *ad hoc* solution to a formalized specification with a permanent home under a sponsoring organization with full life-cycle management. Because two different interstate exchanges currently use NIEM PMP, the schemas may need to be consolidated before the NIEM Health Domain adopts them.

Recommendation 4b – Develop system-level access (API, Web services) to support computer-to-computer integration with statewide PDMPs.[16] [17] An authoritative body would specify the API that all vendors would need to support; this should be done once (not state by state), but it would take more than a year to finish. States should demand that PDMP vendors provide a data access API as an intrinsic (i.e., not extra cost) product feature. This would be achieved during the acquisition process. Specifically, an API should be a requirement for a vendor's solution.

While this effort is in progress, states can use interstate exchanges (such as PMPi and RxCheck) to provide access to PDMP data even to intra-state clients. This approach, while not technically optimal, worked well for several of the PDMP pilot tests.

Recommendation 4c – Define the requirements for the three common types of PDMP data requests to shorten the implementation time for organizations and to improve interoperability. Workflow analysis revealed that only three basic kinds of requests for PDMP data exist. As such, the full spectrum of current PDMP data access requires building a general purpose interface able to request patient, prescriber, and dispenser data. The Work Groups used this knowledge to enumerate and define the specific data fields that prescribers and dispensers would need. In addition, the Work Groups developed the following products and recommended their use to ensure technical and semantic interoperability for accessing patient, prescriber, and dispenser data:

- A common set of Data Elements and definitions, including a human-readable view of the data. The Data Elements are needed to:
    - Configure a query that uniquely identifies prescribers, dispensers, and patients
    - Specify the kind of data being requested from these systems.
- A generic and reusable Data Element Exchange Standard that explains how to electronically define and exchange the Data Elements

[16] An application programming interface (API) is a specification that allows two or more different software components to communicate.

[17] A Web service is communication among different systems over the Internet.

- A Cross-Reference Guide that maps the Data Elements onto other data specifications to eliminate any ambiguity in the correlation of different data definitions used by different systems

The NIEM Information Exchange Package Documentation (IEPD) can encapsulate the human-readable data element view and the electronic data exchange standard. These items have been described separately to emphasize their importance.

Recommendation 4d: Share and distribute PDMP technical information and products – Using a collaborative infrastructure for advertising, sharing, updating, and testing conformance would help PDMP system and EHR and pharmacy system vendors effectively adopt and use the API, Data Elements Table, Data Element Exchange Standard, and Cross-Reference Guide products.

1.3.5 Lack of Effective Business Agreements

The business and health IT landscapes increasingly contain third-party intermediaries that facilitate the exchange of PDMP information. Intermediaries such as Health Information Exchanges (HIEs) and benefit-management switches already facilitate a variety of data transactions among healthcare organizations, including both payers and prescribers. Leveraging these components of the health IT ecosystem provides both opportunities and risks, and these interactions should be managed carefully. There is an increasing need for HIEs and other intermediaries to implement appropriate agreements corresponding to their projected increased participation in PDMP data dissemination activities. Thus, strong and enforceable agreements are needed to govern the collection, use, disclosure, storage, and other aspects of PDMP data exchange. Yet establishing the appropriate set of agreements is a time-consuming process requiring extensive expertise.

Recommendation 5: Implement an agreement framework and model agreements to facilitate data-sharing through intermediaries – Standardization of legal agreements advances the goal of facilitating better PDMP data-sharing among authorized users in every jurisdiction. The third-party intermediaries that provide services on behalf of the PDMPs should use well-drafted contracts and agreements based on a comprehensive legal framework. The Work Groups developed examples of these agreements, available in the appendices, which can be implemented. These can supplement the existing agreements in place between interstate data hubs and individual state PDMPs. Over time, the Work Groups hoped that the existing agreement infrastructure will continue to build. This should reduce the need for new agreements, and in addition, the individual agreements may converge to create best practices.

1.3.6 Summary

The previous section contained a discussion of the various impediments for accessing PDMP data at the point of care. The recommendations are a compilation of the Work Group findings. The following section describes the Work Groups, the goals they addressed, and how they were composed.

1.4 Introduction to Work Groups

1.4.1 Overview of Work Groups

Work Groups convened to address issues impacting the use of and access to PDMP data. The diverse set of members relied on their extensive knowledge and expertise to develop recommendations and products that should be used to increase the usefulness and availability of PDMP information. Ultimately, prescribers and dispensers may use this information to make more knowledgeable decisions regarding the prescribing and dispensing of controlled substances.

The Work Groups considered the following goals when making their recommendations:

- Connect PDMPs with existing health information technologies to rapidly introduce change
- Provide timely access to PDMP data in the hopes of identifying issues prior to prescribing
- Establish standards for facilitating information exchange to improve interoperability
- Increase overall practitioner use of PDMP data to facilitate the appropriate prescribing of controlled substances
- Ultimately reduce drug overdose and deaths

The Work Groups explored the legal, technological, and operational aspects of the PDMP data and user landscapes, and they developed specific recommendations aimed at improving timely access to PDMP information. The Work Groups also addressed a wide variety of complex issues involving laws and policies, access to and use of PDMP information, and enabling technologies, as listed in Table 1. For brevity, Work Groups will be referred to by their abbreviated title in the report.

Table 1. Work Group Titles

Name	Abbreviated Name
Information Usability and Presentation	Usability Work Group
Data Content and Vocabulary	Vocabulary Work Group
Transport and Architecture	Transport Work Group
Law and Policy	Law Work Group
Business Agreements for Intermediaries	Business Agreements Work Group

Each Work Group developed specific recommendations designed to benefit a variety of entities in the PDMP landscape, including PDMP administrators, state law and policy makers, practitioners, technology vendors supporting these communities, and members of federal agencies, including congressional leaders. The Work Groups developed recommendations and

products that were guided by questions and issues enumerated in the task list of the action plan.[18] These recommendations and products are mapped to the original tasks and pilot activities in the action plan (see Appendix A).

Figure 5. Work Group Composition and Efforts

Work Group members represented diverse perspectives and a variety of relevant healthcare-related business and technology interests (see Appendix B). Federal agencies also were represented. These members were recruited through a voluntary and open process and selected for their expertise in a field related to the project's goals. Great consideration was given to selecting members from relevant backgrounds who would add significant knowledge to the Work Groups. Figure 5 illustrates the breadth and the depth of the Work Group composition.

[18] Prescription Drug Abuse and Health Information Technology Work Group. (2011). "Action Plan for Improving Access to Prescription Drug Monitoring Programs through Health Information Technology." http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_0_9025_3814_28322_43/http%3B/wci-pubcontent/publish/onc/public_communities/_content/files/063012_final_action_plan_clearance.pdf

2 Information Usability and Presentation

2.1 Introduction

The Information Usability and Presentation Work Group, also known as the Usability Work Group, focused on how PDMP information should be presented in the user interfaces (UIs) of pharmacy management systems and provider and ED EHRs, also known as User Systems. The Work Group's objective was to maximize the value of PDMP data for treatment and drug-dispensing decision purposes. The members addressed the content and structure of data display for the prescribing or dispensing decision maker, focusing on what information is needed to enable appropriate decisions.

The Work Group developed specific recommendations about how data sent from PDMPs should be presented to individuals responsible for making treatment decisions. The following individuals are authorized users (the Users) of PDMP data:

- Physicians, including both ambulatory practices and ED practitioners (referred to as "prescribers" throughout this document)
- Pharmacists or dispensing physicians (referred to as "dispensers")
- Healthcare professionals who are authorized delegates appointed by either dispensers or prescribers (referred to as "delegates")

The Work Group set out to achieve the following three goals:

1. Identify the minimum set of PDMP information required for decision-making.
2. Evaluate the usefulness of patient-at-risk filters for prescribers or dispensers.
3. Determine how accessing PDMP reports would alter a User's typical workflow. Provide recommendations for mitigating any changes.

2.1.1 Relevant Background

To accomplish its goals, the Work Group considered how prescribers and dispensers would use PDMP information and would interact with the PDMP and User Systems. The usability of systems and the presentation of information are important factors in realizing the full advantage of these systems. Since a key usability consideration is understanding the Users' perspective and how they typically work, the members took time to examine the typical workflow for each type of User. For example, dispensers often are required to fill a prescription no later than an hour after receiving the prescription order. This process includes several tasks such as inputting the prescription information in the system, verifying the prescription with the prescriber, receiving authorization from the patient's insurance, and filling the prescription. In addition, dispensers often log in to multiple terminals, speak with patients, answer phone calls from prescribers, and handle additional interruptions. Therefore, the process of accessing PDMP information for dispensers should be:

- Easy
- Efficient
- Within the User's current workflow

The members considered these guiding principles when creating their recommendations.

2.1.2 Summary of Recommendations

This section provides several recommendations that enhance how Users access PDMP information. These recommendations are grouped according to the following topic areas:

Data elements for PDMP data

Workflow integration

Patient-at-risk filters

Electronic data correction

- Training for using PDMP data

The Work Group identified the following principles to guide these recommendations:

- PDMP information should be current and timely, meaning that the data should be as up-to-date as possible and available when needed.
- Information should be presented to Users within their normal workflow. The ideal scenario is for the PDMP data to be integrated in the Users' System.

2.2 Recommendations

2.2.1 Data Elements for PDMP Data

2.2.1.1 Complete List of Data Elements for PDMP Reports

In an ideal scenario, there would be a standard set of information that must be included in all reports across different state PDMPs. However, numerous state law, policy, and technical challenges are barriers to achieving this ideal scenario. Prescribers and dispensers would like to have access to the most relevant PDMP information when caring for a patient. The Work Group reviewed a variety of PDMP reports and agreed upon a standard data set that should be available in all reports, shown in Table 2. Specifically, this recommendation is based on the data elements provided in the following documents:

- American Society for Automation in Pharmacy (ASAP) 2009 Prescription Drug Monitoring Program Standard, Version 4.1
- "Prescription Monitoring Program Model Act 2010 Revision," Alliance of States with Prescription Monitoring Programs[19]
- Prescription Monitoring Information Exchange (PMIX) Service Specification Package (SSP), Version 1.0.1 (December 2011)[20]
- PMIX Information Exchange Package Documentation (IEPD) as provided in the PMIX SSP, Version 1.0.1 (December 2011)[21]

[19] Alliance of States with Prescription Monitoring Programs, "Prescription Monitoring Program Model Act 2010 Revision," Voorheesville, NY, June 28, 2010.

[20] Alliance of States with Prescription Monitoring Programs, "PMIX," http://www.pmpalliance.org/content/prescription-monitoring-information-exchange-pmix.

Table 2. Data Elements for PDMP Reports

Patient Information	
First name Last name Street address City State ZIP code	Date of birth Identification (ID) qualifier and/or patient identifier (situational) Gender code (situational) Species code (situational) Phone number (situational)
Prescriber Information	
First name Last name Street address City	State ZIP code Phone number (situational) Drug Enforcement Agency (DEA) number (situational)
Dispenser Information	
Pharmacy or dispensing prescriber name Street address City State ZIP code	Phone number (situational) DEA number (situational) National Council for Prescription Drug Programs (NCPDP)/ National Association of Boards of Pharmacy (NABP) Provider ID (situational) National Provider Identifier (NPI) (situational)
Prescription Information	
Name of drug Strength Form Quantity dispensed Days' supply dispensed Date prescription filled	Date written Refills authorized Refill number Refill status to indicate a full or partial refill Prescription number
Note: The term "situational" describes data elements that are available only in some state PDMPs.	

[21] http://www.pmpalliance.org/pdf/20111227%20PMIX_SSP_v_1.0.1.zip.

2.2.1.2 Future PDMP Data Elements and Functionality

Users search the information in a PDMP report to look for patterns of drug abuse or diversion. Some prescription data is not currently collected by these programs, but in the future, this information would be useful at the point of prescribing or dispensing. The following three data elements suggestions currently are not collected, but they can be useful to determine which patients are at risk for abusing prescription drugs. For example, payment type may be useful because drug-seeking patients often will pay out of pocket for their prescriptions. Further, the inclusion of patient instructions will remove the ambiguity of dispensers deciphering the providers' instructions, which they typically do by calculating the days' supply and quantity dispensed. However, patient instructions will only be useful when there is greater standardization for how these instructions are written.

Recommendations:

PDMPS should collect the following data elements in the future:

- Drug administration instructions: This should be included, but only after there is more standardization of the format and how this information is written.
- Payment type
- First and last name of the person picking up the prescription (if different from the patient)

2.2.1.3 Timeliness and Currency of PDMP Data Reports

Prescribers and dispensers have a short period of time to interact with a patient and make a decision about whether to prescribe or dispense a controlled substance. The PDMP information is useless after the patient interaction, so the response time of the PDMP system is vital. Further, some PDMP data is not current, meaning that the data may not reflect controlled substance history in real time. This lack of currency occurs because several PDMPs only require dispensers to report prescription information to the PDMP once a week, or even once a month. The reporting requirements directly impact the currency of data so that more frequent reporting leads to more current data. Unfortunately, patients who frequently abuse or divert prescription drugs may collect multiple prescriptions within the course of a few hours or days, so it would be helpful for dispensers and prescribers to see a patient's most recent activity. In the future, it would be ideal for PDMP information to be as timely and current as possible to provide the most useful data to Users.

Recommendations:

Dispensers and prescribers should have timely access to PDMP data, which means that they should receive the data within 30 seconds after a request. The data should be available while the prescriber or dispenser is still interacting with the patient.

The PDMP data should be as current as possible. Users should receive a disclaimer stating that the data is current the day it is received, but data currency can change over time because of additions and corrections.

In the future, it would be ideal if the PDMP data was updated at the point that the User requests a PDMP report so that the data reflected all prescription activity in real time.

2.2.1.4 Default Length of Patient Drug History in PDMP Data

Chronic pain and drug addiction are persistent conditions, and the PDMP data should indicate patients who are suffering from these illnesses. Therefore, dispensers and prescribers benefit from seeing a patient's history of controlled substances over several months. This allows them to determine if there is a pattern of potential prescription drug abuse. At a minimum, dispensers and prescribers should see at least six months of a patient's controlled substance history in a report for an initial evaluation with a patient or if they are new Users of a PDMP system. Providing 12 months of data is ideal because it allows the User to view the patient's pattern of controlled substance use.

Recommendations:

Dispensers and prescribers should receive a minimum of six months of a patient's controlled substance history in the patient's PDMP data. Ideally, they would be able to request one year of information.

2.2.2 Workflow Integration

2.2.2.1 Integrating PDMP Data in User Systems

Currently, prescribers and dispensers must access a separate system to view PDMP data. Accessing a separate system outside a User's System is time-consuming and frustrating because prescribers and dispensers have limited time. Many prescribers and dispensers work under time pressure and often are inundated with interruptions. Most importantly, dispensers and prescribers must deviate from their normal workflow to access this data. Depending on the circumstances, a prescriber or dispenser may spend three minutes or more retrieving a patient's data from a Web-based portal.

Users will be less likely to access PDMP information if the process requires several actions and takes longer than a few minutes per patient to retrieve the data. Therefore, Users should be able to access data without deviating from their normal workflow. Ideally, they should be able to retrieve this data through their User Systems.

The Work Group considered three different options to integrate PDMP data in User Systems. All of these options have value to the Users because they (1) enhance access to PDMP information and (2) reduce the amount of time and number of steps required to view the information.

The following recommendations range from low-level integration to full integration. Each recommendation is discussed as a possible option for integrating PDMP data in User Systems:

A single sign-on (SSO) to the PDMP and User System

A link to the PDMP system that automatically passes query information

Full integration of PDMP data in the patient record within a User System

2.2.2.2 Single Sign-On to the PDMP and User System

Currently, dispensers and prescribers must leave their normal system and log on to a separate system to view PDMP data. This discourages Users from accessing this data. Most prescribers and dispensers log on to their User System as a normal part of their workflow. Signing on to a separate system, such as the PDMP system, adds tasks to a User's normal workflow and requires more time. At a minimum, Users should be able to automatically sign on to the PDMP system based on their User System credentials. This would be more efficient and less frustrating to dispensers and prescribers. It may be possible that the SSO can occur concurrently with requests to the state HIE or e-prescribing system.

Recommendations:

Dispensers and prescribers should be granted access to the PDMP system by signing in to their User System. The SSO to the system will depend on the level of trust in the credentialing and authentication processes for the User System.

There may be different levels of access depending on the level of trust in the User System. For example, for systems with lower levels of trust, the User could be granted access to the system only when retrieving PDMP data or when electronically prescribing.

Authentication should not interfere with the User's workflow.

The User should be logged out of the PDMP system after a period of inactivity not to exceed 20 minutes. Users could be logged out of the system as soon as the report is closed for systems that have less rigorous credentialing and authentication.

Users should receive a short message concerning their responsibility to protect the patient's protected health information (PHI).

2.2.2.3 A Link to the PDMP System that Automatically Passes Query Information

Currently, dispensers and prescribers do not have a direct link to PDMP information from their User Systems. At a minimum, Users should have an SSO for the PDMP and their User System. However, dispensers and prescribers would benefit from an additional level of integration: providing a link in the User System would automatically (1) pass the query credentials and (2) populate the query information in the PDMP system. This option would be more efficient than pulling up the PDMP system, even if the User is already signed in due to the SSO capability.

A common Applications Programming Interface (API) for accessing PDMP data is recommended in subsection 4.2.2. This API should support passing queries along with the required query credentials as part of the PDMP interface.

Recommendations:

Dispensers and prescribers should have the ability to click a link in their User System that would allow them to more efficiently access a patient's PDMP data. The link should automatically populate the following search fields from information in the patient file within the User System:

- First name
- Last name
- Date of birth
- Address (situational)
- Gender (situational)

The PDMP system would be populated with the correct patient information because the link would be located within a patient's file.

If multiple patients match the query, then the report should not be sent until the correct patient is selected from a list of possible patients. If multiple patients match the query and the User cannot determine the correct patient, then the User should receive an error message that reads "Deferred for manual review," and the PDMP system administrators will review the request.

Users also should be able to specify the search parameters before searching for a patient's data in the PDMP system. However, the search parameters may not be accessible depending on the system.

2.2.2.4 Full Integration of PDMP Data in the Patient Record within a User System

Dispensers and prescribers have limited time to retrieve and read PDMP reports in a PDF format from a separate system. Users could provide better patient care if they were able to view this data in the context of the patient's history in the User System. Prescribers and dispensers are more likely to view the PDMP information and use it to make clinical decisions when the information is clearly visible in their normal workflow. Therefore, PDMP data should be integrated in EHR and pharmacy systems.

Prescribers and dispensers should not be overwhelmed with a cluttered display of PDMP data. Instead, they want to view only the most relevant information. A large amount of information should be transferred electronically for PDMP reports. Users will want the option to view the full list of information; however, dispensers and prescribers will become overwhelmed if they must visually search all available PDMP information displayed in the UI. They will be less likely to use the PDMP information if the display is not well formatted or is cluttered with too much information.

Users can benefit from a small subset of PDMP information because this would greatly reduce the full list to only the most relevant information. When time is of the essence, dispensers and prescribers will be able to scan this subset of information and make a quick judgment without reading the full list. Therefore, a minimum, useful set of information should be readily visible for these Users, and further information should be viewable if more detail is needed.

Recommendations:

The ideal recommendation is to provide the PDMP data in the User System. There should be a shortened list of prescription information from the PDMP system that includes the following information (see Figure 6):

- Date prescription filled
- Prescriber first and last name
- Name of drug
- Strength
- Quantity dispensed
- Days' supply dispensed
- Indicator of new or refill prescription
- Refills authorized
- Data prescription written
- Dispenser

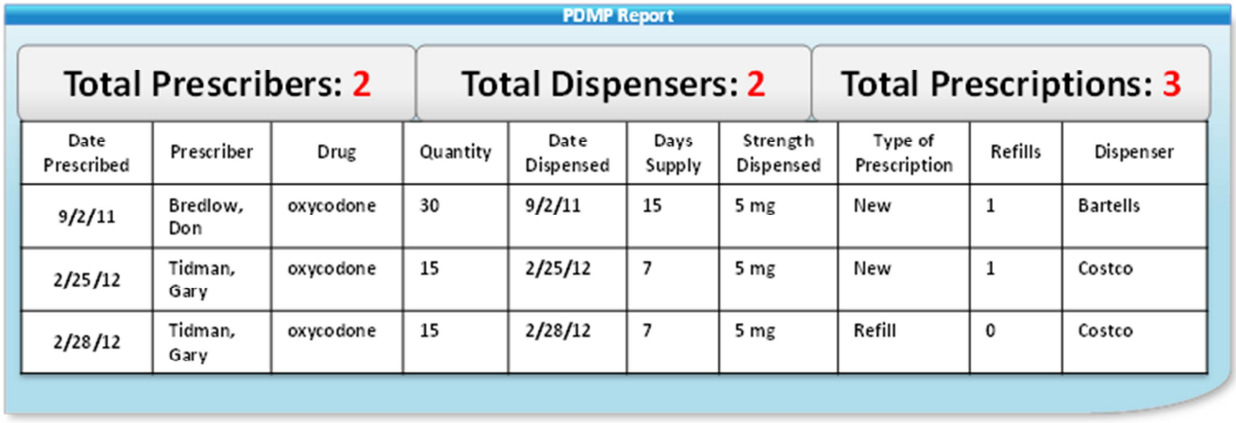
This information should be listed in chronological order according to the date a prescription was filled, beginning with the most recent prescription at the top of the list. Users should be able to sort the list.

At the top of the list there should be a summary of the total number of prescribers, pharmacies, and number of prescriptions in a 6-month to 1-year period. This summary also could be achieved using a score or statistic of the patient's history of controlled substances.

Users should have the ability to retrieve the full list of information sent in a PDMP report. One example of this recommendation is the ability to view more information through an additional action such as scrolling over the following data elements to view additional information:

- Scroll over "Prescriber" to view the prescriber's full address and phone number (if available)
- Scroll over "Dispenser" to view the dispenser's full address and phone number (if available)

Figure 6 shows one way of structuring a PDMP report with a minumum set of data.



PDMP Report

Total Prescribers: 2 | Total Dispensers: 2 | Total Prescriptions: 3

Date Prescribed	Prescriber	Drug	Quantity	Date Dispensed	Days Supply	Strength Dispensed	Type of Prescription	Refills	Dispenser
9/2/11	Bredlow, Don	oxycodone	30	9/2/11	15	5 mg	New	1	Bartells
2/25/12	Tidman, Gary	oxycodone	15	2/25/12	7	5 mg	New	1	Costco
2/28/12	Tidman, Gary	oxycodone	15	2/28/12	7	5 mg	Refill	0	Costco

Figure 6. PDMP Data Elements to Be Displayed in User Systems

2.2.2.5 Integration of Unsolicited Reports in User Systems

There are two types of PDMP reports: solicited and unsolicited. The difference between these reports depends on the circumstances of the report's generation. A solicited report is any report that is generated because it is requested by the recipient of the report. For example, a prescriber may suspect that a patient is abusing prescription drugs and requests that person's PDMP report. An unsolicited report, or "push report," is generated because program personnel query the PDMP database, identify patterns of suspicious behavior, and send a report to authorized Users without their request. In this case, the recipients do not expect the report.

Dispensers and prescribers may be unaware of unsolicited reports because there is no consistent mechanism to notify them. Currently, Users are notified of unsolicited reports by eFax, email, and sometimes fax or postal mail. However, prescribers and dispensers will need to receive a notification, preferably via email or another electronic message that can directly take them to the PDMP data. Ideally, this notification would be viewed in the EHR or pharmacy system or as an email that provides a link to the PDMP data.

Recommendations:

Dispensers and prescribers should be able to receive a message or alert (see Figure 7) in the EHR or pharmacy system or as an email that contains a link to the unsolicited PDMP report.

Figure 7 provides an example of how different data elements could be organized into an EHR or pharmacy system UI.

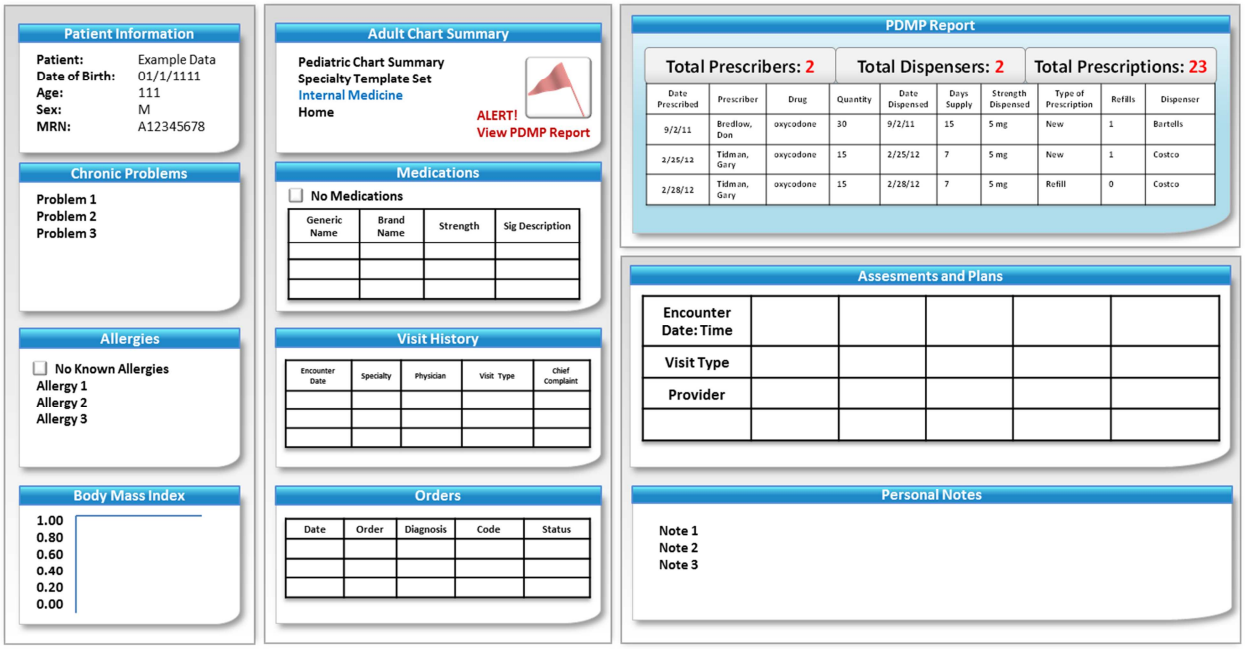


Figure 7. PDMP Data Elements Incorporated in the User System Display

2.2.3 Patient-at-Risk Filters

A patient-at-risk filter is any system or threshold that can be used to identify patients who may be misusing or diverting prescription drugs. The purpose of these filters is to highlight the most likely prescription drug abusers. These filters are considered a useful tool for surveilling the patient population.[22] Because the majority of patients are not considered at risk, these filters enable dispensers and prescribers to prioritize their list of patients and view the PDMP reports for only high-risk patients. Various criteria are used to identify at-risk patients. Some states consider patients high risk if they fill six or more prescriptions for controlled substances from six or more prescribers or six or more dispensers in a single month; this is called the 6-6-1 threshold. The Work Groups also discussed the possibility that prescribers and dispensers have the ability to create customizable thresholds and criteria. This customization would provide the freedom to set more stringent thresholds depending on the prescribers' and dispensers' personal preferences. Other criteria could be used to determine patients-at-risk including attempts for early refills and the number concurrent prescriptions of a controlled substance. Overall, the purpose of these filters is to reduce the time users spend sifting through several PDMP reports so that they may focus on the most valuable information. Dispensers and prescribers do not have time to review every patient's report; therefore, these filters may benefit Users by sending information on only high-priority patients.

The Work Group discussed the usefulness of applying a patient-at-risk filter to PDMP data to sort the most at-risk patients. Without data that supports one filter or threshold over another, it is difficult to make a decision about which filter to use. However, there is value in filters that act as

[22] N. Katz et al., "Usefulness of Prescription Monitoring Programs for Surveillance-Analysis of Schedule II opioid prescription data in Massachusetts: 1996-2006." *Pharmacoepidemiology and Drug Safety*, vol. 19, pp. 115-123, December 2010.

clinical decision support tools. These tools can be used to support decision-making by supplementing the prescriber or dispenser's clinical judgment. The Work Group believed that more research is needed to better understand how patient-at-risk filters can be implemented in PDMPs and which filters result in fewer detection errors. Further, providing education about these tools to dispensers, prescribers, and other authorized healthcare professionals is useful. The members provided recommendations that should improve patient-at-risk filters.

2.2.3.1 Methods to Improve Using Patient-at-Risk Filters

The Work Group identified issues with patient-at-risk filters and noted that such filters need further development to improve how they are used. In particular, every threshold and filter is imperfect. For patient-at-risk filters, there is always the potential to incorrectly identify a patient who is not abusing prescription drugs and also to miss or not identify a patient who truly is at risk. Therefore, Users of any filter should be educated about how the filter works as well as the error rate for that filter. Filters also may be made more accurate by including additional criteria for filtering patients. This is consistent with prior research that suggests using additional criteria may improve the detection of patients who are inappropriately receiving prescription opioids.[23] Researchers suggest additional criteria may include the incidence of early refills, the use of brand name prescriptions compared to generic drugs, and an escalation in the dosage. However, the Work Group highly suggests that further research is needed to determine the optimal level for each criteria.

[23] Ibid.

Recommendations:

The following are recommended methods to optimize a patient-at-risk filter:

- Provide online continuing education.
- Provide access to policies concerning how the filter selects patients.

The following are recommended methods to reduce the potential bias that prescribers or dispensers may experience when using a patient-at-risk filter:

- Provide a disclaimer that the filter may incorrectly identify or not identify some patients. If possible, this should include education about the filter's error rate.
- Educate dispensers and prescribers about how to use the information to make clinical decisions.
- Explicitly state that these tools must be used with caution.

The following data elements should be used in the future to determine which patients are at risk for abusing or diverting prescription drugs:

- Number of prescribers
- Number of dispensers
- Number of prescriptions
- Number of concurrent prescriptions
- Time period

Note: It is currently not possible to view a patient's number of concurrent prescriptions, but this would be valuable information.

2.2.4 Electronic Data Correction

To date, no electronic method exists for requesting corrections to PDMP inaccuracies. Users should be able to easily detect and request corrections of errors in this data. For example, the most common error occurs when two prescribers have similar names. Prescribers and dispensers should be able to electronically complete an online form that states the nature of the error and then submit this form electronically to the PDMP system administrator. This request would then be routed to the dispenser. Ideally, the system should automatically send a confirmation email to the person submitting the form that provides a confirmation of receipt. The requester involved should be notified when the correction is made. This ability to electronically request corrections to PDMP data would improve the overall accuracy of information in PDMP systems.

Recommendations:

EHR and pharmacy management systems should have the capability to identify and report errors in PDMP data to the appropriate party, and Users should have the ability to correct this error at the source.

2.2.5 Training for Using PDMP Data

Many prescribers and dispensers have little or no training in how to appropriately prescribe controlled substances, let alone in how to detect patients who may be abusing or diverting these drugs. Prescribers and dispensers have minimal knowledge of what behaviors or patterns indicate a problem with prescription drugs or where to seek help if they discover such a problem with a patient.

However, by requiring training before granting access to the PDMP system, states may discourage dispensers and prescribers from using PDMP systems. Nevertheless, thorough PDMP training would be well suited during medical or pharmacy school, and brief tutorials would be helpful when dispensers and prescribers register to use their state's PDMP system.

Recommendation:

PDMP Users should receive training to teach them how to access, synthesize, and understand the data.

Medical and pharmacy students should receive this training during their instruction on prescribing/dispensing medications to assist them with making treatment decisions.

2.3 Topics for Further Exploration

The Usability Work Group discussed several topics related to the presentation of PDMP data and the usability of the systems that display this data. However, these topics were not addressed in more detail because they were beyond the scope of the Work Group's goals. The topics are important enough to be explored in the future by a different project or Work Group that can address them in greater detail.

2.3.1 User Interface Design

The members decided not to provide specific recommendations for the presentation of PDMP data in User Systems. Specifying the UI design recommendations and criteria could negatively impact system usability and stifle design innovation. To date, usability and user interface design experts do not provide specific recommendations for the design of EHR systems because they recognize that each system must meet unique requirements. Some EHRs are designed for a

specific medical specialty. Further, these systems are used in a variety of settings such as pharmacies, EDs, and family medical practices.

Therefore, the Work Group decided there was no benefit to suggesting UI design recommendations or requirements. Instead, the individual vendors for EHRs and pharmacy management systems should have the flexibility to incorporate PDMP data to satisfy systems' and Users' needs. The Work Group does encourage the vendor community to employ the principles of user-centered design (UCD) to ensure the usability of these systems. UCD is a design philosophy in which the user's requirements and limitations are considered throughout the design process or product development cycle.

2.3.2 Usability Testing

The Work Group believes that usability testing is an important part of the UCD process. However, the members did not provide specific recommendations regarding usability testing methods. Because there are a variety of methods, vendors should have the freedom to select the usability methods that are most appropriate for their product.

3 Data Content and Vocabulary

3.1 Introduction

The Data Content and Vocabulary Work Group, also known as the Vocabulary Work Group, focused on the data standards and data elements needed to facilitate the exchange and use of PDMP data. The members developed a core set of PDMP Data Elements and the supporting Data Element Exchange Standard. These two products are the foundation for future data exchanges. The members also identified the data elements needed for report request interfaces and the resulting report contents for the data exchanges associated with the most common use cases that the Transport Work Group identified.

The Vocabulary Work Group achieved the following goals:

- Reviewed existing standards and vocabularies for requesting and receiving prescription drug information
- Identified a core set of standards and data elements to be used by recipient communities
- Reviewed existing standards for attributes needed to uniquely identify patients
- Identified core identity attributes needed to resolve patient identity in the PDMP

The recipient communities referenced in the second goal are:

- Pharmacists or dispensing physicians ("dispensers")
- Physicians, including both ambulatory practice and ED practitioners ("prescribers")
- Healthcare professionals who are authorized delegates appointed by either dispensers or prescribers (referred to as "other authorized healthcare professionals" throughout this section)

3.1.1 Relevant Background

The driving force behind the work of both the Vocabulary and Transport Work Groups is interoperability. The Vocabulary Work Group developed recommendations for the purpose of improving data access and interoperability by providing a common data framework for exchanging PDMP data between systems.

The healthcare industry has devoted considerable resources to understanding interoperability. In the context of health IT, interoperability is typically defined as the ability of two or more entities or components to exchange information and to effectively use that information for business purposes. Interoperability types are used to further classify and scope the level of information exchange. The book *Coming To Terms: Scoping Interoperability for Health Care*[24] specifies three main types of interoperability:

[24] P. Gibbons et al. *Coming to Terms: Scoping Interoperability for Health Care* (Final), Health Level Seven, EHR Interoperability Work Group. Feb. 7, 2007.

1. Technical (physical conveyance of a “payload”)
2. Semantic (communication of meaning)
3. Process (integration into a work setting)

3.1.2 Summary of Recommendations

The Vocabulary Work Group developed several products that provide the foundation for improving timely access to a common, well-understood set of PDMP data. The recommendations are organized using the following categories:

- Interoperability – Data content and vocabulary information needed for interoperability:
    - Common PDMP Data Elements
    - Data Element Exchange Standard
    - Cross-Reference Guide
- Identity – Data needed to uniquely identify persons associated with PDMP data:
    - Patient identity
    - Dispenser identity
    - Prescriber identity
    - Authorized user identity
- Data Element Usage for Requests and Reports:
    - Requests for patient data
    - Requests for dispenser data
    - Requests for prescriber data
    - PDMP reports

Implementing the recommendations in the Work Group’s products will have many benefits, including:

- Improving data access while limiting the amount of new interface development time and costs by using the common data defined in the PDMP Data Elements and Data Element Exchange Standard. These products re-use the existing data elements defined in a standalone NIEM-based information exchange specification.
- Improving data accuracy by the specification of a minimum set of data elements needed to uniquely identify the most common report objects (patient, prescriber, or dispenser).
- Standardizing and simplifying the development of a small, well-defined set of PDMP interfaces.
- Promoting data accuracy by eliminating ambiguity in the correlation of different data elements used by different systems with the cross-reference between specifications.

3.2 Recommendations

3.2.1 Interoperability Recommendations

Interoperability is essential for effective PDMP data flow and use. The interoperability recommendations identify ways of improving the exchange of PDMP information using:

- PDMP Data Elements
- Cross-Reference Guide
- Data Element Exchange Standard

The healthcare arena has a wide variety of stakeholders with different business roles and needs (e.g., payers versus physicians). Over time, these organizations have organically developed IT systems and vocabularies to best address their health IT needs, resulting in a set of divergent and poorly interoperating data specifications and semantics. In the absence of a common set of data meanings and interpretations, and owing to a lack of uniform technical guidance for exchanging the data, interoperability is hindered, and interfaces must be developed in an ad hoc manner.

By converging to one common baseline set of PDMP Data Elements, the Work Group has provided the semantic standard needed to accurately describe PDMP information. Likewise, legacy data collections exist in native data representation that must be correctly mapped to the common data elements to enable incorporation of legacy data. To enable the best use of prescription drug monitoring data, software developers need clear technical guidance on how to present data to the diverse stakeholders as well as on how to implement systems that can effectively access the desired data. The proposed Data Element Exchange Standard is intended to provide this guidance.

3.2.1.1 PDMP Data Elements

Recommendation:

The Work Group proposed a common set of PDMP Data Elements largely based on the ASAP Implementation Guides that PDMPs use for receiving reports of controlled substances dispensed by pharmacies. Each PDMP Data Element has the following information:

- Human-readable data element name
- Human-readable definition
- Synonyms for other names by which the data element is known (e.g., birth date can be represented as DOB, Date of Birth, Patient Birth Date, etc.)

The PDMP Data Elements include the minimum data needed to uniquely identify the common components of the PDMP systems used in report requests. The PDMP Data Elements also cover other prescription information and persons who pick up prescriptions.

The Work Group recommends adopting the PDMP Data Elements for interactions with PDMP systems.

3.2.1.2 Data Element Exchange Standard

Recommendation:

Adopt the proposed Data Element Exchange Standard to define the technical implementation guidance required for health IT systems that exchange information with PDMP systems. This standard enables recipient systems to request and receive data from PDMP systems using a common set of data elements and data element types. The Data Element Exchange Standard has the following information:

- Human-readable data element name
- Computer definition of data element with Extensible Markup Language (XML) schema type
- Defined values/rules of use for the data element

The Work Group recommends reusing the standalone NIEM-based information exchange specification called NIEM Prescription Monitoring Program.

See Appendix C.2 for the PDMP Data Element Exchange Standard.

3.2.1.3 Cross-Reference Guide

Recommendation:

Adopt the Cross-Reference Guide to facilitate data exchange between systems that use different healthcare data representations. This will ensure a consistent, accurate, and unambiguous exchange of PDMP information. This Cross-Reference covers ASAP,[25] *Health Information Technology Standards Panel (HITSP) Summary Documents Using HL7 Continuity of Care Document (CCD) Component/C32*,[26] and the NIEM PMP implementations used by the PMIX and PMPi interstate exchanges. The Cross Reference could be further extended to cover other specifications to ensure ongoing technical interoperability among the PDMP and recipient systems.

See Appendix C.3 for the Cross-Reference Guide that maps the PDMP Data Elements to related specifications.

3.2.2 Identity Recommendations

The identity recommendations improve the exchange of PDMP information by providing unambiguous identity of:

1. Patient
2. Dispenser
3. Prescriber
4. (Other) authorized user

The first three define the unambiguous identity needed for well-configured PDMP data queries, while the final recommendation, required to protect privacy by controlling data access, identifies the entity initiating the PDMP data exchange.

Establishing unambiguous identity is a key aspect of any well-configured data query. Methods to resolve identity ambiguity for patients, dispensers, and prescribers serve to satisfy the core PDMP data exchange use cases identified in this chapter. This is expected to be more acute as the size of the PDMP data store grows (i.e., worse for larger states than smaller ones), and especially when interstate exchange through interstate data hubs becomes more prevalent. Identity ambiguity may shelter those engaged in diversion as well as implicate those innocent of such misuse. Thus, PDMP data use will significantly improve when queries return unambiguous results.

[25] American Society for Automation in Pharmacy (ASAP) Standard for Prescription Monitoring Programs, *Implementation Guide*, Version 4, Release 2, 2011.

[26] Healthcare Information Technology Standards Panel. "HITSP Summary Documents Using HL7 Continuity of Care Document (CCD) Component," Version 2.5, June 8, 2009.

In a related issue, the identity of those accessing the data likewise must be uniquely determined to ensure that permissions and data access issues are appropriately handled. Protecting the privacy of PHI is a priority for PDMP systems, and health IT must implement data safeguards, including use of individual user identity (and role), to appropriately limit data access.

If PDMP systems and interstate data hubs shared a common set of data to uniquely identify a patient, prescriber, and dispenser, the development of interfaces would be enabled, and data queries would be more effective. The set of data elements that the Work Group produced uniquely identifies patients, prescribers, and dispensers, and it should be used to maintain consistency with current systems. The HIPAA Security Rule requires that each employee be assigned a unique username to identify and track the identity of users that are authorized to access PHI information[27]. Therefore, the concept of an "authorized user" is a common data content requirement for all IT systems handling such information, and this concept should be included in required identity data specifications.

3.2.2.1 Patient Identity

Recommendation:

This is the set of minimum information required to uniquely identify a patient:

- Name (first and last)
- Address (including ZIP code)
- Date of birth
- Identifier (if available)

The PDMP Data Elements and Data Element Exchange Standard have other data elements that are considered situational and may be available, but they are not required to uniquely identify a patient.

This information is consistent with a 2008 RAND Corporation study[28] that identified the characteristics needed to uniquely identify a patient. The RAND study analyzed a demographic database containing 80 million records to determine that name, date of birth, ZIP code, address, and some unique identifier (driver's license, partial Social Security number, etc.) was sufficient to uniquely identify a patient.

[27] Health Insurance Portability and Accountability Act of 1996, Public Law (P.L.) 104-191 ("HIPAA"), 45 C.F.R. Parts 160 and 164 ("the Privacy Rule").

[28] R. Hillestad et al., *Identity Crisis: An Examination of the Costs and Benefits of a Unique Patient Identifier for the U.S. Health Care System*. Santa Monica, CA: RAND Corp., 2008. http://www.rand.org/pubs/monographs/2008/RAND_MG753.pdf.

3.2.2.2 Dispenser Identity

Recommendation:

This is the minimum set of information required to uniquely identify a dispenser:

- Name (first and last)
- Address (including ZIP code)
- Identification

The PDMP Data Elements and Data Element Exchange Standard have other data elements that are considered situational and may be available, but they are not required to uniquely identify a dispenser.

3.2.2.3 Prescriber Identity

Recommendation:

This is the minimum set of information required to uniquely identify a prescriber:

- Name (first and last)
- Address (including ZIP code)
- Prescriber DEA number

The PDMP Data Elements and Data Element Exchange Standard have other data elements that are considered situational and may be available, but they are not required to uniquely identify a prescriber.

3.2.2.4 Authorized User Identity

Recommendation:

The data associated with an authorized user must be included in the Data Content and Vocabulary products. This is the minimum set of information needed to uniquely identify an authorized user:

- Name (first and last)
- Role
- Case number (if applicable)
- Authentication credentials (e.g., DEA number, account number)

This includes information needed for both system access control and the generation of audit trails. This is a precondition of affiliating user credentials for query activities.

3.2.3 Data Element Usage for PDMP Data Requests

The requestor may need to specify additional information to further refine the PDMP data being requested in addition to providing an unambiguous identity for the patient, dispenser, or prescriber for PDMP requests. This information is part of the technical interface for requesting information from a PDMP system. An "interface" is typically defined as a set of specifications for use by two or more software components for the purposes of communicating with each other. The request/response part of the interface was covered by the activities of the Transport Work Group.

The recommendations in this section identify the PDMP Data Element information needed to define the most common query interfaces with PDMP systems: those seeking data for patients, prescribers, and dispensers. The Work Group also specifies Data Element usage for reports.

Access to patient prescription information is impaired by the lack of common interface definitions for requesting PDMP data. Of particular note is that a common set of data elements is not currently available for use across all systems engaged in the health IT ecosystem that prescribe and dispense prescription drugs. Additionally, usability of PDMP reports is impaired by the lack of common report contents.

A reusable data element specification would assist the data requestors and system implementers involved in this business environment because it would allow the development of generic, reusable interface definitions for queries involving patient, prescriber, and dispenser information in PDMPs. A common interface to PDMP systems improves semantic interoperability by enabling those seeking PDMP data to finely tune their request for the specific data they need. This common interface would greatly improve technical interoperability because it could be reused by many other systems. The specification of a single interface fosters reuse and provides cost savings for IT systems that reuse this interface.

Likewise, a specification for the content provided by PDMP systems (report Data Elements) will improve technical and semantic interoperability between PDMPs and recipient systems. It will also greatly improve access to PDMP information because all PDMP systems would provide the same minimum set of well-defined information in the reports.

3.2.3.1 Data Element Usage for Patient Data Requests

Recommendation:

The Work Group recommends the interface parameters shown in Table 3 for requesting information about a specific patient. These interface parameters are applicable for a solicited report and for setting up the parameters of an unsolicited report.

Table 3. Patient Data Request

Data Elements for the Data Request	Notes
Patient	
Name (first and last)	
Address (including ZIP code)	
DOB	
Identifier	Optional
Gender	
Species	Optional
Phone number	Optional
Authorized User (Person Requesting the Report)	
Authentication information	
Name (first and last)	
Role	
Case Number	Required for law enforcement requests

3.2.3.2 Data Element Usage for Dispenser Data Requests

Recommendation:

The Work Group recommends the interface parameters shown in Table 4 for requesting information about a specific dispenser. These parameters work for use cases where the dispenser is checking his/her own history as well as when another party (e.g., licensing board) is checking the dispenser's data. These interface parameters are applicable for a solicited report and for setting up the parameters of an unsolicited report.

Table 4. Dispenser Data Request

Data Elements for the Data Request	Notes
Dispenser	
Name of Dispenser	
Address	
Identification	
Prescription	
National Drug Code (NDC) Number	May be used to review dispensing of specific drugs
Name of drug	May be used to review dispensing of specific drugs
Authorized User (Person Requesting the Report)	
Authentication information	
Name (first and last)	
Role	
Case Number	Required for law enforcement requests

3.2.3.3 Data Element Usage for Prescriber Data Requests

Recommendation:

The Work Group recommends the interface parameters shown in Table 5 for requesting information about a specific prescriber. These parameters work for use cases where the prescriber is checking his/her own history, or for when another party (e.g., licensing board) is checking their prescribing history. These interface parameters are applicable for a solicited report and setting up the parameters of an unsolicited report.

Table 5. Prescriber Interface

Data Elements for the Data Request	Notes
Prescriber	
Name (first and last)	
Address (including ZIP code)	
Prescriber DEA number	A prescriber may have multiple DEA numbers.
Prescription	
NDC Number	May be used to review prescribing of specific drugs
Name of drug	May be used to review prescribing of specific drugs
Authorized User (Person Requesting the Report)	
Authentication information	
Name (first and last)	
Role	
Case Number	Required for law enforcement requests

3.2.3.4 Data Element Usage in PDMP-Provided Data

Recommendation:

A minimum, common set of information should be specified for PDMP reports. Appendix C.4 identifies the data elements associated with the information that should be available in the most common types of reports:

1. Patient PDMP information
2. Prescriber wants to check his/her own history (prescriber report)
3. Dispenser wants to check his/her own history
4. Request for information about a specific prescriber or dispenser

See Appendix C.4 for the Data Element Usage Table.

3.3 Topics for Further Exploration

The Work Group identified several topics for future exploration during the Data Content and Vocabulary analysis and product development process. These topics are important work needed to augment the Vocabulary Work Group outcomes and products. The Work Group identified the following unexplored topics for future consideration.

3.3.1 Data and Interface Specifications

A complete framework of data and interface service specifications is needed to provide a comprehensive technical solution for accessing PDMP data. The PDMP Data Elements, Data Element Exchange Standard, and Data Element Usage in PDMP requests define the basic data elements needed for the PDMP interfaces. The Transport Work Group used this information to develop the request and response patterns for the actual exchange of messages. This information needs to be developed into formal interface specifications for system implementers.

3.3.2 Unsolicited Reports

Unsolicited reports are triggered by a predefined set of parameters in the PDMP systems to indicate that a patient has exceeded some threshold for obtaining too many prescriptions within a specific time-frame. To maximize the reuse of specifications, it may be helpful to converge on the specific requirements for alerts and other forms of unsolicited reports. This requires further study to define the most appropriate triggers needed by clinical decision-makers. The technical specifications for the triggering parameters then would be added to the interface specifications for accessing PDMP data.

3.3.3 Authorized Users

The concept of an authorized user is a common data content requirement for all IT systems handling prescription information. Authorized users will be part of any messaging infrastructure implemented, and the concept is mentioned here for thoroughness. The Work Group created a preliminary definition of an authorized user during the use case analysis and associated data elements with report requests. More work is needed to completely understand and define the data required for an authorized user in the PDMP interfaces.

3.3.4 Cross-Reference Guide Expansion

The Cross-Reference Guide (Appendix C.3) between the PDMP Data Elements and other specifications with prescription information will improve data accuracy by eliminating any ambiguity in the correlation of different data elements used by different systems. This Cross-Reference Guide covers ASAP, HITSP C32, and the NIEM-based information exchange specification used by the PMIX and the PMPi. Additional healthcare specifications should be added to the Cross-Reference Guide to eliminate potential data ambiguity errors with other systems that interact with PDMP systems to ensure a consistent, accurate, and unambiguous exchange of PDMP information.

4 Transport and Architecture

4.1 Introduction

The Transport and Architecture Work Group, also known as the Transport Work Group, explored and developed architectural guidelines and technical specifications for data transmission between PDMPs and a variety of recipient systems. Members reviewed and addressed the following topics in detail:

- Domain standards
- Security
- Data transport protocols
- Web service implementations

The Work Group crafted transport and architecture specifications with an eye for general applicability, which would enable the recommendations to be relevant to any system exchanging information with a PDMP system. The Work Group also developed technical recommendations to accomplish effective data sharing and interoperability between PDMPs and data recipients. The Transport Work Group's activities and outcomes align with the typical enterprise architecture framework (EAF) shown in Figure 8.

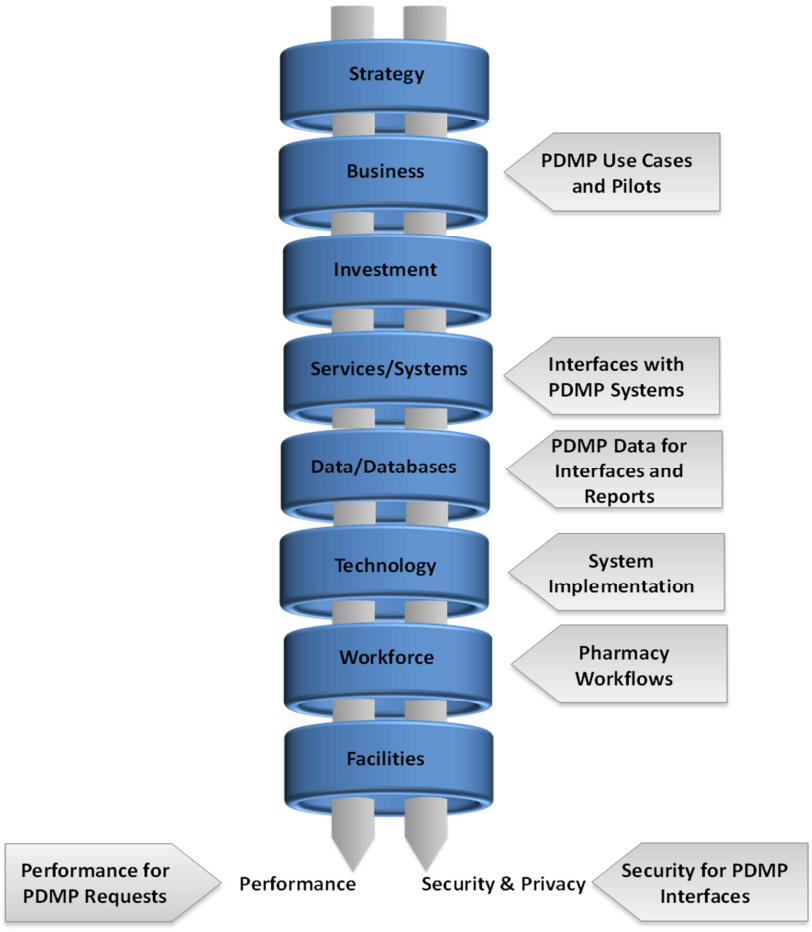


Figure 8. Alignment of the Transport Work Group Activities with a Typical EAF

The Transport Work Group explored the system-to-system workflows and architectures required to support the following scenarios:

- Notifying PDMPs of events (such as prescription fulfillment)
- Requesting data from PDMPs
- Performing the operations needed to support direct interfaces with PDMP systems and interfaces involving third parties

4.1.1 Relevant Background

Transporting PDMP data is a complicated process that involves several entities. These entities include both end users and consumers like the PDMP databases and EHR pharmacy systems and third-party "intermediaries" that route transmissions between PDMPs and end users. Examples of intermediaries include benefits management switches and HIEs. Additionally, the Transport Work Group believed that adhering to common standards and specifications will improve interoperability and timely access to information. The members agreed that adhering to service-oriented architecture (SOA) engineering best practices, reducing technical barriers to entry, and decreasing ongoing maintenance costs were important to the Work Group's success.

For each recommendation, the Transport Work Group provided a rationale explaining why the members arrived at the recommendation, a more detailed explanation of the recommendation, and useful background information.

4.1.2 Summary of Recommendations

The Work Group's recommendations, which aimed at improving the transmission of PDMP data, address the following issues:

- Development of PDMP use cases and the implementation of a patient-at-risk score
- Development of a common set of PDMP interfaces for three report types: patient, prescriber, and dispenser
- Use of the NIEM-based PMP information exchange specification
- Use of XML-based interfaces for messages
- Improving workflows through a common operational approach for unsolicited reports and the rejection of co-transmission queries to PDMPs
- Security of PDMP messages
- Performance or speed of PDMP system response when users request individual patient PDMP reports

4.2 Recommendations

4.2.1 Leverage the Existing NIEM-Based Information Exchange Specification

Access to patient prescription data is impaired by the lack of the common data exchange specification needed for PDMP interfaces. A common data specification is needed to obtain patient, prescriber, and dispenser information from PDMP systems.

The PMIX National Architecture is a formal set of technical requirements that existing and planned interstate data hubs use to enable hub-to-hub communication. A critical component of the architecture is the use of open standards (design elements that are in the public domain and available free of charge). Adopting open standards reduces costs and ensures a state's ability to remain flexible. Two interstate data-sharing hubs are currently in operation: the National Association of Boards of Pharmacy's (NABP) PMPi and the Bureau of Justice Assistance's RxCheck. Additional hubs may be developed in the future.

Both interstate data hub players use a standalone NIEM-based information exchange specification (called NIEM PMP). The Transport Work Group proposed that NIEM PMP be formally promoted in the new NIEM Health Domain. This requires an update to the existing NIEM PMP to the latest versions of the NIEM core and the ASAP specification data. Appendix D.3 also identifies some recommended updates for the NIEM PMP patient prescription reports. Members also noted that while not all PDMPs (nor the pharmacies that report the data) use the latest ASAP version, using the latest version is recommended to encourage states to adopt and populate PDMPs with the extra data needed for the Data Element Exchange Standard. Finally, aligning stakeholder solutions with the NIEM-based information exchange specification would help ensure interoperability and information exchange in a timely manner.

Promoting a common informational model will accelerate interoperability, which in turn improves the effectiveness of data exchange. Members of the PDMP community noted that NIEM already is using data and data definitions (from ASAP) that have become a *de facto* standard for storing and exchanging healthcare information. The members believed that the adoption of a modified, updated form of the NIEM-based information exchange specification would benefit the community. The benefits of this recommendation will accrue to both PDMP data managers and those involved in numerous transport activities for this data.

Recommendation:

Leverage existing capabilities and use the NIEM-based information exchange specification to serve as the domain standard for PDMP data exchange. Facilitate the specification's widespread adoption by the community.

4.2.2 Common Set of PDMP Request Interfaces

Access to patient prescription data is impaired by the lack of both a common interface and the data definitions needed for that interface. A common interface specification is needed to obtain patient, prescriber, and dispenser information from PDMP systems. In this case, an "interface" is defined as a set of specifications for use by two or more software components for the purposes of communicating with each other.

The members determined that a more extensive set of interfaces is needed to satisfy the following complete set of use cases:

- Unsolicited ("push") patient reports

- Solicited ("pull") patient reports
- Solicited self-report
- Solicited reports, as typical of a medical oversight agency (e.g., licensing board)
- Solicited reports from an emergency department, triggered by an admission, discharge, or transfer (ADT) event
- Solicited reports from an emergency department, triggered by an ADT event

It is critical that the new interfaces maintain backward compatibility with existing interface designs. The Work Group concluded that the NIEM-based information exchange specification would meet this criterion. The members also identified the need to modify the report request interface schema to reflect the updated data and parameter needs.

Several issues must be addressed in detail, including:

- The expected delivery formats (e.g., XML, PDF, text blob)
- Delivery methods (e.g., email, eFax) and addressing parameters (e.g., email)
- Authorization

These options should be defined based on the use cases. The members also preferred a common method for handling system-level access and authorization (likely through an SSO), although the details regarding SSO are beyond the Work Group's scope.

The issue of "triggers" also is important to the PDMP query process design and report request interfaces. The members stipulated that both automatically triggered and manually initiated queries have the same technical requirements and should be treated similarly. Appendix D.1 contains the interface worksheet for use by individual PDMPs in overall system design.

Finally, the members assessed the appropriate parameters for interfaces. Both preconfigured and flexible parameters must be supported for a fully optimized interface regimen. This includes specific parameter values from the PDMP Data Elements (patient, prescriber, and dispenser). The members differentiated between "Setup Parameters," which are defined in advance and apply to all reports, and "Request Parameters," which are defined in each report request and apply only to that request. Parameter details for the examined use cases are provided in Appendix D.2.

A common API for accessing PDMP data should be developed to support PDMP interfaces. The members developed a set of recommended interface parameters for each report type to be used as a starting point for the development of an API specification. The existing NIEM-based information exchange specification could be updated to include a comprehensive list of use cases and the additional interface parameters and exchange data identified by the Vocabulary Work Group. These interfaces should be coordinated and submitted as interface standards as part of a technical collaborative sharing environment such as the NIEM Health Domain.

Recommendation:

Develop a common PDMP API that includes interfaces for solicited and unsolicited reports for three report types: patient, prescriber, and dispenser. Interstate exchanges of PDMP data currently use a standalone NIEM-based information exchange specification that should be leveraged to develop the three common report interfaces and updated to include the additional parameters and exchange data identified by the Vocabulary and Transport Work Groups.

4.2.3 Support for Web Service Architectures

Implementing electronic access to PDMP data is impaired by the lack of common technical specifications for interfaces and data exchange. A common standard for data exchange with PDMP systems is needed.

The members decided on a simplified set of requirements based on two technology pillars: (1) the use of XML and (2) the use of Web services. For each transaction, the inputs and outputs should be defined, but the protocol should be agnostic as long as the protocol supports XML transport. This conceptual framework is expected to work well with a variety of existing implementations and technologies. This decision also provides considerable flexibility, allowing for wider participation by organizations with a variety of skills and expertise.

The flexibility of XML as a transport media for a variety of transactions is a well-known phenomenon, and XML schemas are an appropriate choice for the data packet in PDMP-related transactions (see Section 6.2.1). Conversely, PDF data exchanges were not considered desirable, even though they are currently used in many states. The use of HTML (HyperText Markup Language) rendering of XML may alleviate the difficulty of reading XML by providing easy access to human-readable text for XML-encoded documents. Within the proposed guidance, Simple Object Access Protocol (SOAP) and representational state transfer (REST) were both deemed acceptable Web service implementation options in this framework, thereby avoiding a detailed analysis of which is superior for PDMP data exchange applications. Either Web service implementation option can be used to define a standard; future standards definition efforts can choose to prefer one over the other.

This technical recommendation cannot and should not be implied as superseding applicable regulations in jurisdictions where less flexible formats (e.g., PDF) are required by law or convention.

Interstate data hub players use XML schemas, but they use different transports. For example, RxCheck uses SOAP, while the PMPi Web services are RESTful. Both are successful at exchanging data; therefore, there are multiple acceptable and usable methods to make these transactions. The Transport Work Group favored an approach that offers a variety of “approved” solutions and declined to specify transport protocols or other parts of the technology stack beyond requiring that it satisfy the functional requirements listed in the Work Group recommendations (e.g., will support an XML data exchange, can support security

recommendations). This inclusive decision should broaden the ranks of participants by reducing the barriers to entry.

Recommendation:

Data transport should be accomplished through the use of XML and the solution(s) adopted should support a variety of Web service technology stacks and implementations. The use of XML embraces a neutral approach to Web service architectures that does not preclude any best-of-breed technologies in the current market or future technologies.

4.2.4 Common Approach for Unsolicited Reports

Currently, there are a variety of methods to define and deliver unsolicited reports. This causes data access and interoperability issues for interstate information exchanges. The use of unsolicited ("push") reporting is an important part of the PDMP landscape. Unsolicited reporting is an alert message provided to an appropriate party when a predefined threshold is crossed within a PDMP database. Thresholds for unsolicited reporting typically are set by pharmacy boards or other agencies and may vary widely. In some cases, these trigger thresholds correspond to the previously published National All Schedules Prescription Electronic Reporting National Drug Control Policy and Prevention of Prescription Drug Abuse Reauthorization Act of 2010 guidelines,[29] but frequently they represent the judgment of specific state authorities.

The many variations in how unsolicited reports are sent reduce interoperability and slow the development of effective interstate data sharing. By moving toward a common operational approach among participants ("operational convergence"), both the effectiveness and ease of implementation of this data-sharing process should be improved.

Recommendation:

The underlying nature of unsolicited ("push") requests within the PDMP community should move toward a common operational approach and design to improve interoperability and data access.

4.2.5 Security

PDMP reports contain PHI that must be secured from potential data breaches. Federal agencies that handle PHI are subject to the Federal Information Security Management Act of 2002

[29] American Society of Interventional Pain Specialists. (2010). Facts on NASPER: National Drug Control Policy and Prevention of Prescription Drug Abuse Reauthorization Act of 2010 guidelines. http://nasper.org/database.htm.

(FISMA)[30] in addition to being subject to HIPAA Security Rule requirements, [HIPAA (P.L.104-191[31] and 45 C.F.R Parts 160, 164[32]). FISMA establishes minimum information security requirements, including technical and operational controls, and defines three security objectives for information systems:

1. Availability
2. Integrity
3. Confidentiality[33]

The "crosswalk" analysis of FISMA to HIPAA offers helpful advice to integrate these policies when needed.[34] The Work Group's recommendation in Table 6 is sufficient for complying with HIPAA and the most applicable portions of the FISMA framework.

PDMP data is exceptionally sensitive because it contains PHI—specifically, scheduled prescription drug history information. As such, data breaches are considered harmful, and system security is recommended. In all cases, HIPAA data security requirements must be met by all PDMPs, data requesters, and intermediaries. Within these guidelines, the members chose to focus on the relevant portions of the FISMA security parameters suggested by the General Services Administration, which are well established and widely regarded as a good basis. If PHI data is not included in a particular response, the security requirements are reduced.

As an example, The Direct Project was created to specify a simple, secure, scalable, standards-based way for participants to send authenticated, encrypted health information directly to known, trusted recipients over the Internet.[35]

[30] National Institute of Standards and Technology (NIST). (May 17, 2012). "Federal Information Security Management Act of 2002," Computer Security Division: Computer Security Resource Center. http://csrc.nist.gov/drivers/documents/FISMA-final.pdf.

[31] HHS. (August 21, 1996). "PUBLIC LAW 104-191, AUG. 21, 1996. HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996," Office of the Assistant Secretary for Planning. http://aspe.hhs.gov/admnsimp/pl104191.htm.

[32] HHS. (February 20, 2003). "Part II: Department of Health and Human Services, Office of the Secretary, 45 CFR Parts 160, 162, and 162, Health Insurance Reform: Security Standards; Final Rule," Office for Civil Rights. http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/securityrulepdf.pdf.

[33] NIST. (February 2004). "Federal Information Processing Standards Publication (FIPS PUB 199): Standards for Security Categorization of Federal Information and Information Security," Computer Security Division: Computer Security Resource Center. http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

[34] HHS. "An Introductory Resource Guide for Implementing the HIPAA Security Rule," Indian Health Service, SP 800-66. http://www.ihs.gov/AdminMngrResources/HIPAA/documents/fisma_to_hipaa.pdf.

[35] HHS. "Direct Project," The Office of the National Coordinator for Health Information Technology. http://healthit.hhs.gov/portal/server.pt/community/healthit_hhs_gov__direct_project/3338

Recommendation:

An appropriate framework based on federal guidelines for message security should be applied to ensure compliance with HIPAA and all relevant state privacy laws. Table 6 outlines the specific recommendations for transport security, message security, message integrity, consumer authentication, and nonrepudiation for PHI and non-PHI PDMP data.

Table 6. Security Recommendations by Data Type (PHI vs. Non-PHI)

	PHI Included		No PHI Included	
Feature	**Point-to-Point**	**Intermediary**	**Point-to-Point**	**Intermediary**
Transport Security	SSL, TLS, VPN (IPSEC), other (FIPS 140-2)	SSL, TLS, VPN (IPSEC), other (FIPS 140-2)	SSL, TLS, VPN (IPSEC), other	SSL, TLS, VPN (IPSEC)
Message Security	Not Required	FIPS 140-2 validated encryption	Not Required	Not Required
Message Integrity	Not Required	Not Required (due to intrinsic message security)	Not Required	XML Signature
Service Consumer Authentication	Certificate, Username	Certificate, Username	IP Address, Certificated, Username	IP Address, Certificated, Username
Non-Repudiation	Not Required	Not Required	Not Required	Not Required

4.2.6 Performance

Prescribers and dispensers should receive individual PDMP reports in a timely manner for clinical decision-making. Currently, there is no standard response interval across all the PDMP systems. In many current situations, PDMP report retrieval requires extra steps to access data on other systems, and this is incompatible with the clinical decision-making workflow.

NABP indicates that at present, the PMPi data hub and individual PDMPs have typical response times of 7.5 seconds and 5.74 seconds, respectively.[36] This preliminary data shows that the system response interval requirement proposed by the Work Group should be achievable for now, though increased traffic in the future may require rebalancing system resources to maintain this goal. The Transport Work Group also indicated that large batch downloads (e.g., all dispensations from a pharmacy chain) may be legitimately slower than this baseline, and such activities represent a use case not covered by this recommendation.

The members resolved that to best promote system-to-system interoperability, it will be necessary to establish a floor for the system response interval that can be used as a baseline for

[36] National Association of Boards of Pharmacy (NABP). "NABP PMP InterConnect," 2012. http://www.nabp.net/programs/pmp-interconnect/nabp-pmp-interconnect/.

all participants' synchronous responses. The members decided that the interval should be (generously) set at 30 seconds. Some participants (e.g., Surescripts) have much lower latency within their own systems. This response requirement is expected to have considerable implications for queries that currently use fuzzy matches in their search, which are expected to have greater time requirements than exact matches. It also sets expectations for the level of hardware support (i.e., numbers, types, and configurations of servers) that underlies the various PDMP and data hub systems.

Recommendation:

The system response interval should be faster than 30 seconds for individual reports to avoid issues of timeouts and asynchronous response.

4.2.7 Co-Transmission of Queries

"Co-transmission," the concept of consolidating new queries and data returns with existing message transmissions along the existing transport pathways, was proposed as part of the White House Action Plan[37] as a method to implement improvements in PDMP data access. This required the Work Group to carefully consider the technical and workflow implications to better understand the full costs and benefits of the proposed approach.

Co-transmission offers one possibility for increasing functionality while reducing development costs. However, upon detailed analysis, the Pharmacy Subgroup determined that rather than resulting in operational or technical benefits, co-transmitting a PDMP query on a pharmacy benefits insurance check would be disadvantageous to PDMP data flows. Benefits management switches and other co-transmission candidates may have gaps that can be exploited by patients engaged in drug-seeking behavior. In particular, such patients may choose to forgo prescription drugs (other health benefits) and instead rely on self-pay options. A variety of known techniques and policies can be used to address this deficiency, though with some degree of legal and technical difficulty.

Co-transmission offers participants considerable potential benefits. However, adoption will be slow if the specifics of a proposed co-transmission process produce a disruption to the workflow or if the technology cannot be easily and cheaply extended. The rationale for this rejection was based on these two categories of concerns as well as on a third item: potential relationship dynamics between the switch and other participants in the data flow.

The benefits check occurs at the wrong place in the workflow. Specifically, these actions happen in the hands of the pharmacy technician or sales clerk, rather than the pharmacist. In all cases, the primary responsibility for the medical decision resides with the pharmacist, and the data should flow to the pharmacist (for both privacy and usability reasons). Appendix D.4 provides a

[37] Prescription Drug Abuse and Health Information Technology Work Group. (2011). "Action Plan for Improving Access to Prescription Drug Monitoring Programs through Health Information Technology." http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_0_9025_3814_28322_43/http%3B/wci-pubcontent/publish/onc/public_communities/_content/files/063012_final_action_plan_clearance.pdf

detailed depiction of an "ideal" PDMP query-enabled pharmacy workflow, as assessed through a careful analysis by the members.

From the technical perspective, the members considered best practices in SOA. Specifically, there should be a loose coupling of severable services and objects. However, tight coupling is intrinsic in co-transmission and thus is not aligned with modern architectural best practices. Further, the members viewed "bad service definitions" as inappropriate engineering decisions.

The Work Group had concerns regarding the role of the switch entity and the potential for secondary uses of the highly sensitive PDMP data. This also aligns with the views of the Law and Business Agreements Work Groups.

Recommendation:

The proposed co-transmission of queries to PDMPs as part of pharmacy benefits check was rejected as unworkable on both technical and workflow grounds.

4.2.8 Patient Risk Score

Dispensers and prescribers may not have time to review every patient's PDMP report, and standard patient drug history reports do not contain any analysis for patterns of behavior or potential abuse. Therefore, to focus their attention, these users would benefit from a method to prioritize those patients who are at the highest risk of abusing prescription drugs.

It would be acceptable to have more than one patient risk score if individual practitioners would find this helpful for their triage. A patient risk score for the purposes of this report is a value derived from PDMP data via an algorithm that classifies a patient's likelihood for prescription drug abuse or overdose.

Providing the underlying numeric score produced by the automated analysis algorithm(s) may or may not need to be provided to the users; they may derive some additional value from this granular information with appropriate training. The exact treatment of intermediate category patients was not explicitly resolved, but most patients should be placed in the lowest risk category if the boundaries are set appropriately.

From a technical implementation standpoint, the use of a triage flag may introduce a small degree of additional technical complexity to system interfaces. Specifically, the transaction for such a flag is likely to differ from a query requesting a full patient prescription history. However, this is balanced by the fact that a transaction that retrieves a triage flag (alone) would be considerably faster than that for a complete PDMP prescription history.

From a workflow perspective, a patient risk score should allow quicker service to be rendered at the point of care to individuals in the lowest category of concern. Thus, the practitioner would have more time to devote to patients in the higher risk category, who by definition will require a greater degree of oversight and case review. Even high-risk patients may not be engaged in inappropriate behavior (e.g., doctor shopping) but instead may simply have an extensive but

legitimate need for heavy pharmaceutical intervention. This recommendation will allow them the extra attention by the practitioner that they deserve.

Recommendation:

Some form of patient risk score should be implemented for use by both prescribers and pharmacies in each state (or nationally if possible) and should be made available in PDMPs. A generic and highly desirable configuration would consist of a two- (high/low) or three-tier (high/medium/low) scoring system to assist in the triage of patients.

4.3 Unexplored Topics

The Transport Work Group discussed the technical implications of the following topics but did not address them sufficiently to create official recommendations.

4.3.1 Authorized Users

Some members lauded the value of using a directory to identify users. The members felt that a directory would provide considerable value for the overall PDMP data-exchange ecosystem, especially if it included specific information about how to interact with users (e.g., delivery of reports via email, fax, etc.) and their authorization status. In a survey of the existing landscape, one PDMP software vendor already possessed a directory for users of PDMP systems. Likewise, PMIX has a directory for how to access specific systems, designed for system-to-system interactions. However, the members did not provide a method for achieving this. A common method is still needed for handling system-level access and authorization.

4.3.2 Access and Authorization

While the directory described in Section 4.3.1 might be of considerable value for the PDMP ecosystem, a list of authorized users and their credentials is insufficient for future needs. Instead, this could be seen as a precondition of the next logical step: implementing a framework to enable transparent system-to-system communications where the passing of credentials is the key element (not username, but system authorization credentials). This framework would need to be able to support both synchronous and asynchronous requests and the delivery of information to the requesting user or application. There needs to be a way to reduce the overhead some users face for PDMP data access (e.g., multiple passwords for practitioners who work at multiple venues).

4.3.3 Risk Evaluation and Mitigation Strategy

The risk evaluation and mitigation strategy (REMS) concept was defined in the U.S. Food and Drug Administration (FDA) Amendments of 2007 for use with biologics or drugs that pose a special degree of risk to public safety. It was designed to allow patients continued access to

medications while striving to lower the potentials for abuse, misuse, addiction, and overdose.[38] The existing REMS infrastructure, including support for strong audit trails and inventory control, operates as a *de facto* parallel (and more stringent) PDMP infrastructure. This bifurcation may not be desirable from the standpoint of reducing total costs. The Work Group chose not to address this issue because it was out of scope, yet it should be addressed.

4.3.4 SCRIPT Integration

Pharmacies submit data to PDMPs via the ASAP standard, yet parallel data streams are in place for electronic prescription exchanges that are typically well integrated into the standard business processes and workflows in health IT. Some of these systems use standards from the National Council for Prescription Drug Programs (NCPDP). For example, the SCRIPT standard facilitates transferring prescription data among prescribers, pharmacies, payers, and other entities.[39] It supports prescriptions, refill requests, fill status notification, and other related events. This standard has been extended to support alerts for Drug Utilization Review (DUR) and medication allergies as well as standardized medication nomenclature. More effective integration of the multiple standards in use could improve healthcare workflows and provide improved capabilities such as full routing to payers and PDMPs without additional manipulation within the pharmacy system.

[38] W. Bell, Jr. (May 31, 2011). "Can REM Programs Solve the Healthcare Prescription Drug Abuse Dilemma," *The Medicare Compliance Blog*. http://themedicarecomplianceblog.com/2011/rems-solve-healthcare-prescription-drug-abuse/.

[39] National Council for Prescription Drug Programs. (November 2011). "Eprescribing Fact Sheet." http://www.ncpdp.org/pdf/Eprescribing_fact_sheet.pdf.

5 Law and Policy

5.1 Introduction

The Law and Policy Work Group, also known as the Law Work Group, was charged with developing policy recommendations that (1) encourage broader and more standardized access to PDMP systems and data by healthcare professionals and (2) provide clear guidance for programs that use third-party intermediaries to exchange data.

The Work Group had two primary goals:

- Examine legal and policy issues that affect access to PDMP data within different settings:
    - Access by prescribers, dispensers, and their delegates
    - Access by other authorized nonprescribing or nondispensing healthcare professionals and their delegates
    - Access by patients to their own data
    - Access by EHR systems, and which PDMP data elements patients can view in their EHR
    - Voluntary or mandatory access to PDMP data by prescribers and dispensers, and the associated liability issues that are implicated
- Examine legal and policy issues regarding the use of third-party intermediaries that enable PDMP data exchange between authorized users:
    - Sharing PDMP data with third-party intermediaries, generally
    - Sharing PDMP data with intermediaries that use federated, centralized, or other architectures whereby healthcare providers no longer directly control patient data
    - Patient consent to sharing data electronically via intermediaries
    - Patient notice

5.1.1 Relevant Background

Several state PDMPs have existed for decades, but the recent surge in prescription drug abuse and diversion has prompted nearly every U.S. state (along with Guam and Puerto Rico) to enact legislation to record patients' controlled substance prescription histories. PDMPs serve two general purposes:

1. To support patient health and safety by enabling prescribers and dispensers to avoid dangerous drug combinations and to identify patients with possible drug dependencies.
2. To create a platform for authorized regulators and law enforcement to identify potential drug diversion or other illicit activity.

The Law Work Group approached the legal and policy issues regarding access and intermediaries mainly from the perspective of patient care and safety. The members leveraged their experience in state and federal privacy and confidentiality laws—including Health Insurance Portability and Accountability Act (HIPAA), 42 C.F.R. Part 2, and the Health Information Technology for Economic and Clinical Health Act (HITECH)—to develop their

recommendations. Additionally, the Law Work Group's recommendations were informed by the Fair Information Practice Principles (FIPPs)[40] and the Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.[41] Appendix A provides more detailed explanations of these principles.

The Law Work Group's policy recommendations are an important contribution to current prescription drug policy discussions throughout the United States. The National Conference of State Legislatures asserts that "Interstate Sharing of Information" and "Prescription Drug Monitoring Programs" are key solutions that must be addressed to halt and reverse the trend of prescription drug overdose and abuse.[42] In New York, legislation passed for two actions: expanding access to dispensers (who currently do not have access to reports) and making PDMP checks mandatory for healthcare professionals when they initially prescribe or dispense controlled substances.[43] Concurrently, the New York Civil Liberties Union is raising privacy concerns.[44] State representatives in Oklahoma also are considering mandatory checks, but opponents urge that doctors should not be doing the job of law enforcement and that mandatory checks would harm workflow and drive up costs.[45] Finally, federal lawmakers have introduced bipartisan legislation to regulate nationwide PDMP standards.[46] The Interstate Drug Monitoring Efficiency and Data Sharing Act would "direct the US Attorney General to establish uniform standards for the exchange of controlled substance and prescription information for purposes of preventing diversion, fraud, and abuse…"[47]

Mindful of these current events, the Law Work Group's policy recommendations are designed to inform the current discourse at the local, regional, and national levels.

5.1.2 Summary of Recommendations

The Law Work Group members considered the following issues when drafting their recommendations:

- Whether broadening access to PDMP data will increase the value and demand for use of PDMP systems

[40] Fair Information Practice Principles were first provided by the U.S. Department of Health, Education, and Welfare in 1973; they are currently the core of the Federal Trade Commission's policy regarding privacy. Retrieved from http://www.ftc.gov/reports/privacy3/fairinfo.shtm.

[41] "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," *OECD.* Organisation for Economic Co-operation and Development. http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

[42] "Prevention of Prescription Drug Overdose and Abuse," *National Conference of State Legislatures*, August 2012. http://www.ncsl.org/issues-research/health/prevention-of-prescription-drug-overdose-and-abuse.aspx.

[43] G. Koleva. "Plan to Stem Prescription Drug Crisis in New York Fuels Disagreement," *Forbes*, March 2, 2012. http://www.forbes.com/sites/gerganakoleva/2012/03/02/plan-to-stem-prescription-drug-crisis-in-new-york-fuels-disagreement/.

[44] H. Anderson. "HIEs: Protecting Civil Liberties: ACLU Chapter Spells Out Privacy Recommendations," *HealthcareInfoSecurity*, March 21, 2012. http://www.healthcareinfosecurity.com/interviews.php?interviewID=1499.

[45] KJRH, "Bill Designed to Curb Drug Abuse Hits House Floor," February 23, 2012. http://www.kjrh.com/dpp/news/bill-hopes-to-strengthen-rx-oversight-by-doctors.

[46] U.S. Congressman Hal Rogers Press Release. "Congressman Rogers, Wolf and Senators Portman, Whitehouse Introduce Legislation to Combat Prescription Drug Abuse," March 29, 2012. http://halrogers.house.gov/News/DocumentSingle.aspx?DocumentID=287835.

[47] "S. 2254, H.R.4292: Interstate Drug Monitoring Efficiency and Data Sharing Act of 2012," U.S. Government Printing Office, March 29, 2012. http://www.gpo.gov/fdsys/pkg/BILLS-112s2254is/pdf/BILLS-112s2254is.pdf.

- Whether the data elements in a PDMP report should be accessible in an EHR
- Whether prescriber and dispenser queries of program databases should be voluntary or mandated by state law
- Whether PDMP programs can overcome the significant challenges (including state conflicts of law) that arise when transmitting patient data between states, especially if patients do not consent to sharing their personal information electronically
- Whether states should provide notice of required data collection, use, and disclosure to patients, where most states do not currently provide such notice

The following points summarize the Law Work Group's policy recommendations:

- Prescribers, dispensers, and other authorized healthcare professionals should not only be able to request and receive PDMP data themselves, but they also should be able to appoint authorized delegates to do the same.
- PDMP data should be easily shared with patient EHR systems.
- States should not impose a statutory duty on healthcare providers to check PDMP systems; instead, states should explore reasonable methods to encourage greater use of systems, such as through user registration and education.
- Authorized users should enjoy limited civil and criminal liability for sharing PDMP data in certain circumstances, including mandatory compliance with state laws, good faith exchanges with law enforcement, and sharing data with fellow treating physicians.
- Patients should receive notice to ensure that they are aware of their practitioners' legal obligation to submit patient personal information to PDMP systems.

Each recommendation is followed by an explanation of the rationale for how the Work Group arrived at that conclusion. Additionally, where applicable, examples of existing statutory language are provided to show how some states currently address these issues. These examples of statutory language are not intended to be definitive or to represent the entire universe of possible options; they are merely for reference.

5.2 Recommendations

5.2.1 Access to PDMP Systems and Data

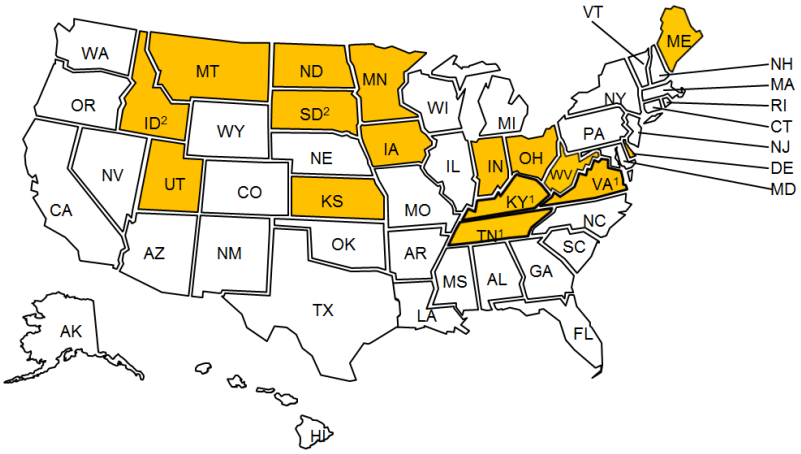
5.2.1.1 Data Recipients and Delegation

5.2.1.1.1 Prescribers and Dispensers May Delegate Access

In some states, important consumers of PDMP data do not have statutory or regulatory authority to access data; for example, New York State prevents dispensers from accessing the PDMP system. Additionally, some pharmacies prevent their employees from accessing this data. In most states, authorized users cannot lawfully delegate access to their assistants.

By January 1, 2013, only 16 states will permit practitioners to designate an authorized agent to access the PDMP database.[48] This indicates a positive trend, as only 10 states permitted delegation to authorized agents in 2011. The Law Work Group felt that in the future, all prescribers and dispensers should have the ability to appoint delegates who can access data under state laws. Delegates do not need to be licensed professionals, but delegates must be able to be identified in a PDMP system. Delegates should obtain individual sub-accounts that are linked to their supervisor (the primary account holder). The creation of individual sub-accounts ensures that (1) delegates do not use the primary account of a supervisor; (2) delegates do not establish an account wholly independent from a supervisor; and (3) delegates' account activity can be tracked for audit purposes.

In these recommendations, access means the ability to request and receive data from the PDMP system. The Work Group's definition of access does not include the ability to submit data. Data submission describes the flow of information to the PDMP system; dispensers are usually the only people who submit data. Figure 9 shows the states that allow practitioners to designate an authorized agent to access a PDMP database.



[1] The Kentucky provision goes into effect in July 2012. The Tennessee provisions go into effect on January 1, 2013. On July 1, 2012, Virginia will go from allowing only two delegates per practitioner to an unlimited number.
[2] Idaho and South Dakota only allow prescribers to designate an agent at this time.

This information was compiled using legal databases, state agency websites and direct communications with state PDMP representatives

Figure 9. States Allowing an Authorized Agent to Access a PDMP Database

[48] S. Kelsey. "States that Allow Practitioners to Designate an Authorized Agent to Access the PDMP Database," *National Alliance for Model State Drug Laws (NAMDL)*, February 2012. http://www.namsdl.org/documents/StatesthatAllowPractitionerstoDesignateanAuthorizedAgenttoAccessthePMPDatabaseMapFebruar_000.pdf.

Recommendation:

Both prescribers and dispensers should be able to request and receive PDMP data. Prescribers and dispensers also should be able to appoint delegates as authorized users under state law to request and receive PDMP data, provided that prescribers and dispensers retain supervision and accountability of those delegates.

Statutory Examples:

The following examples of statutory language are provided to demonstrate that several state PDMP laws currently support the recommendations in this report. These statutory examples are not intended to be definitive or to represent the entire universe of possible options. Policy makers and legislators may reference the language below as a point of reference when considering the best approach for implementation in their own jurisdiction.

1. Indiana (35-48-7-11.1(d) (4): "Except as provided in subsections (e) and (f), the board may release confidential information described in subsection (a) to the following persons: . . . (4) A practitioner or practitioner's agent certified to receive information from the INSPECT program."[49]
2. Iowa (Title IV, Subtitle 1, Chapter 123, Division VI) 124.553: "The board may provide information from the program to the following: . . . A pharmacist or a prescribing practitioner may delegate program information access to another authorized individual or agent only if that individual or agent registers for program information access, pursuant to board rules, as an agent of the pharmacist or prescribing practitioner."[50]
3. Minnesota (Chapter 152) 152.126, Subd. 6 Access to reporting system data: "(b) . . . the following persons shall be considered permissible users and may access the data . . . in the same or similar manner, and for the same or similar purposes, as those persons who are authorized to access similar private data on individuals under federal and state law: (1) a prescriber or an agent or employee of the prescriber to whom the prescriber has delegated the task of accessing the data, to the extent the information relates specifically to a current patient . . . and with the provision that the prescriber remains responsible for the use or misuse of data accessed by a delegated agent or employee; (2) a dispenser or agent or employee of the dispenser to whom the dispenser has delegated the task of accessing the data, to the extent the information relates specifically to a current patient . . . and with the provision that the dispenser remains responsible for the use or misuse of data accessed by a delegated agent or employee."[51]
4. Virginia (Chapter 25.2, Title 54.1) § 54.1-2523.2: "Any prescriber authorized to access the information in the possession of the Prescription Monitoring Program pursuant to this chapter may, pursuant to regulations promulgated by the Director to implement the

[49] Ind. Code § 35-48-7-11.1(d) (2011).

[50] Iowa Code § 124.553 (2011).

[51] Minn. Stat. § 152.126 (2011).

provisions of this section, delegate such authority to up to two health care professionals who are (i) licensed, registered, or certified by a health regulatory board under the Department of Health Professions, and (ii) employed at the same facility and under the direct supervision of the prescriber."[52]

5.2.1.1.2 Access and Delegation by Other Authorized Healthcare Professionals

Other healthcare professionals involved in patient treatment who may not have prescribing or dispensing authority currently do not have the ability to request and receive PDMP data or to appoint delegates. Many of these healthcare professionals work in pain management or mental health and need to know a patient's controlled substance prescription history.

The licensed healthcare professionals referenced here may include persons who do not have authority to prescribe or dispense controlled substances, but they should have access to PDMP data because such access directly impacts the quality of patient treatment and care. These licensed healthcare professionals could include practitioners who work in fields such as disease management, behavioral health that involves utilization management review and case management, and practitioners such as substance abuse clinicians and psychologists.

The Work Group agreed that extending access to these other licensed healthcare professionals makes sense. The members caution that even in the five states where access is partially expanded, some state statutes remain more restrictive than the Work Group would prefer. The statutes below merely represent the approach that states have currently taken. Although the Work Group agrees that other licensed healthcare professionals should be able to view PDMP data, the members were unable to form a consensus for extending access beyond these licensed healthcare professionals, thus future discussion is required.

Recommendation:

Licensed healthcare professionals other than prescribers and dispensers should be authorized to request and receive PDMP data when the data are necessary to evaluate or treat a patient. Licensed healthcare professionals include healthcare practitioners certified or registered by a state.

The same licensed healthcare professionals should be able to appoint delegates authorized under state law, provided that the licensed or certified healthcare professionals retain supervision and accountability of those delegates.

Statutory Examples:

1. Colorado (Title 12, Article 22, Part 7) § 12-22-705: "(3) The program is available for query only to the following persons or groups of persons: . . . (c) Practitioners engaged in a legitimate program to monitor a patient's controlled substance abuse."[53]

[52] VA. Code Ann. § 54.1-2523.2 (2009).

[53] Colo. Rev. Stat. § 12-22-705 (2011).

2. Indiana (Title 35, Article 48, Chapter 7) § 35-48-7-11.1: "(d) Except as provided in subsections (e) and (f), the board may release confidential information described in subsection (a) to the following persons: . . . (8) A substance abuse assistance program for a licensed health care provider who: (A) has prescriptive authority under IC 25; and (B) is participating in the assistance program."54
3. Maryland (Title 21, Subtitle 2A) § 21-2A-06: "(b) The Program shall disclose prescription monitoring data, in accordance with regulations adopted by the Secretary, to: . . . (5) A rehabilitation program under a health occupations board, on issuance of an administrative subpoena. . . ."55
4. North Dakota (Title 19, Chapter 19-03.5) § 19-03.5.03: "3. Unless disclosure is prohibited by law, the board may provide data in the central repository to: . . . j. A licensed addiction counselor for the purpose of providing services for a licensed treatment program in this state."56
5. Utah (Title 58, Chapter 37F, Part 4) § 58-37f-301: "(2) The division shall make information in the database available only to the following individuals, in accordance with the requirements of this chapter and division rules: . . . (i) a mental health therapist, if: (i) the information relates to a patient who is: (A) enrolled in a licensed substance abuse treatment program; and (B) receiving treatment from, or under the direction of, the mental health therapist as part of the patient's participation in the licensed substance abuse treatment program described in Subsection (2)(i)(i)(A); (ii) the information is sought for the purpose of determining whether the patient is using a controlled substance while the patient is enrolled in the licensed substance abuse treatment program described in Subsection (2)(i)(i)(A); and (iii) the licensed substance abuse treatment program described in Subsection (2)(i)(i)(A) is associated with a practitioner who: (A) is a physician, a physician assistant, an advance practice registered nurse, or a pharmacist; and (B) is available to consult with the mental health therapist regarding the information obtained by the mental health therapist, under Subsection (2)(i), from the database;"[57]

5.2.1.1.3 Patients Should Be Able to Access Their Own PDMP Data

Patients do not have access to their own PDMP data in every state. In fact, as of July 2012, only 33 states permit patients and/or parents or guardians of minor children to request and receive their own PDMP data.[58] When states deny patients access to the personal information being collected on them, states are in conflict with longstanding privacy principles like the FIPPs, which have been the foundation of open-government best practices since the 1970s.

The Law Work Group believes that in the future, all states should permit patients to access their own data.

[54] Ind. Code § 35-48-7-11.1(d) (2011).

[55] Md. Code Ann. Health Occ. § 21-2A-06 (2011).

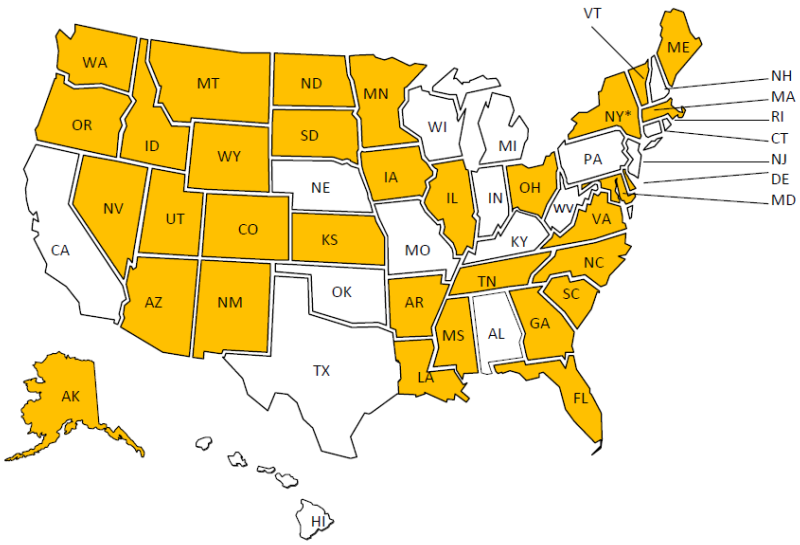
[56] N.D. CENT. CODE § 19-03.5.03 (2011).

[57] UTAH CODE ANN. § 58-37f-301(2)(i) (2011).

[58] H. Gray. "States that Provide PMP Database Information to Patient and/or Parent or Guardian of Minor Child," *NAMSDL*, March 2012. http://www.namsdl.org/documents/StatesthatProvidePMPDatabaseInfotoPatientandParentofMinorChild_001.pdf.

Some states provide patients with limited access to their data; certain data elements, such as prescriber or dispenser DEA registration numbers, are restricted in order to mitigate potential fraud. States should retain the ability to restrict sharing certain PDMP data elements with patients. The members agreed that the methods to request and receive personal data from the PDMP should be "reasonable." A reasonable method may include submitting a notarized hard copy request to the PDMP. An unreasonable method may be to appear in person with three forms of identification on the first Tuesday of the month.

Currently, no PDMP systems offer patients electronic access to their data. Some members raised a concern that such ease of access may lead to potential abuse or compromise of sensitive PDMP data if patients lose their authentication credentials. The Work Group recognized that in the future, many patients will have the ability to access health records securely via a Web portal or other electronic medium. Figure 10 highlights states that provide PDMP database information to patients and/or the parent or guardian of a minor child.



* Pending confirmation

Please see the companion compilation of statutes and regulations on the NAMSDL website for more specific information.

Figure 10. States Providing PDMP Access to Patients and/or Parents/Guardians

Recommendation:

To encourage patients to take responsibility for their own health records and to ensure that PDMP data are correct, state laws and regulations should provide patients with reasonable methods to request and receive their own data.

Finally, patient access referred to here should include access by legal representatives authorized to receive patient data on behalf of a patient under applicable state laws.

Statutory Examples:

1. Arkansas (Title 20, Subtitle 2, Chapter 7, Subchapter 6) §20-7-607. Providing prescription monitoring information: (b) The department shall provide information in the Prescription Drug Monitoring Program upon request and at no cost only to the following persons: . . . (2) A patient who requests his or her own prescription monitoring information; (3) a parent or legal guardian of a minor child who requests the minor child's Prescription Drug Monitoring Program information. . . ."[59]
2. Alaska (Title 17, Chapter 30, Article 5) §17.30.200(d): "The database and the information contained within the database are confidential, are not public records, and are not subject to public disclosure. . . The board may allow access to the database only to the following persons, and in accordance with the limitations provided and regulations of the board: . . . (6) an individual who is the recipient of a controlled substance prescription entered into the database may receive information contained in the database concerning the individual on providing evidence satisfactory to the board that the individual requesting the information is in fact the person about whom the data entry was made and on payment of a fee set by the board under AS 37.10.050 that does not exceed $10."[60]
3. New Mexico (Title 16, Chapter 19, Part 29) § 16.19.29.9 ACCESS TO PRESCRIPTION INFORMATION: "E. The Board shall be authorized to provide data in the prescription monitoring program to the following persons: . . . (2) an individual who requests their own prescription monitoring information in accordance with the procedures established under 61-11-2.D. NMSA . . . (10) a parent to have access to the prescription records about his or her minor child, as his or her minor child's personal representative when such access is not inconsistent with state or other laws."[61]
4. Maryland (Title 21, Subtitle 2A) § 21-2A-06: "(b) The Program shall disclose prescription monitoring data, in accordance with regulations adopted by the Secretary, to: . . . (6) A patient with respect to prescription monitoring data about the patient. . . ."[62]
5. Oregon (Title 36, Chapter 431) §431.966 (c): "The authority shall disclose information relating to a patient maintained in the electronic system operated pursuant to the

[59] ARK. CODE ANN. §20-7-607 (2012).

[60] ALASKA STAT. §17.30.200(d) (2011).

[61] N.M. STAT. § 16.19.29.9 (2011).

[62] MD. CODE ANN. HEALTH OCC. § 21-2A-06 (2011).

prescription monitoring program . . . to that patient at no cost to the patient within 10 business days after the authority receives a request from the patient for the information."[63]

6. Virginia (Chapter 25.1, Title 54.1) § 54.1-2523.C: "In accordance with the Department's regulations and applicable federal law and regulations, the Director may, in his discretion, disclose: 1. Information in the possession of the program concerning a recipient who is over the age of 18 to that recipient."[64]

5.2.1.2 Data Elements

5.2.1.2.1 Authorized PDMP Users and Patients Should Be Able to View Information from PDMP Databases in Their EHR

Currently, there is no law or policy that provides which specific PDMP data elements should be captured in an EHR. There is a need to determine (1) which PDMP data elements would add value to healthcare professionals during their treatment of patients and (2) which PDMP data elements should be viewable by patients who are looking at their own EHR data. Due to privacy concerns for healthcare professionals (such as protecting their home addresses and DEA registration numbers), patients may not need to view all PDMP data in their EHR, but they likely would benefit from seeing appropriate data regarding their controlled substance prescribing and dispensing history.

In the future, the most current patient prescription drug data will be updated automatically in a patient's EHR. The automatic method will not be an aggregation of actual PDMP reports (many of which exist in PDF format today), but rather an automated query that requests specific data elements that are then updated within the system.

The Law Work Group recommends that the updated prescription drug data in an EHR be presented in a format that is easy to read. Prescribers and dispensers want information that is integrated into the workflow and displayed in a manner that is quickly accessed and easily absorbed; otherwise, they will be less inclined to check the data. Prescription data in an EHR should not be presented in a manner that discourages use (e.g., avoid information overload or a cluttered and confusing display of data). An EHR user interface populated with PDMP data should provide essential data, and users should be able to quickly drill down and receive more granular data if necessary.

The Law Work Group agreed that platform designers should follow the principle of "data minimization," meaning that only necessary data should be exchanged and revealed. For workflow, privacy, and security reasons, nonrelevant and unnecessary data should be avoided.

For example, certain data elements may be restricted from patient view in the interest of prescriber and dispenser privacy. These data elements may be personal information about other individuals or may increase the risk of fraud, such as prescriber or dispenser home addresses or prescriber or dispenser DEA registration numbers.

For safety, prescriber and dispenser addresses and phone numbers should be business addresses and phone numbers, not home addresses or personal phone numbers. Practitioners who have home practices should consider using a different, business-related address when registering with

[63] OR. REV. STAT. § 431.966 (c) (2012).

[64] VA. CODE ANN. § 54.1-2523.C (2009).

the DEA. The Work Group members also chose to include pharmacy and prescriber phone numbers in the following recommendation list. This information is not captured by many PDMP systems, but these data elements would facilitate communication among practitioners.

Recommendation:

As systems develop in the future, and to improve patient safety and care, the EHR should reflect the most current prescription data, including all data elements from available PDMP reports, when healthcare providers update their patients' EHRs.

When updating patient EHRs, prescribers and dispensers should be able to (1) request and receive the most current PDMP data and (2) store any PDMP data elements for historical purposes, regardless of the types of intermediaries that facilitate the query.

If patients access their own EHR data, some data elements may be hidden to ensure the safety of healthcare providers and to reduce the risk of fraud. The following data elements from a PDMP report should be visible to patients in an EHR:

Patient name (first and last)	Drug name
Patient address (street, city, state, ZIP)	Drug strength
Patient date of birth	Drug form (e.g., tablet, capsule)
Patient gender	Drug quantity dispensed
Prescriber first name	Drug date filled
Prescriber last name	Drug date prescription written
Prescriber phone number	Drug refills authorized
Dispenser, pharmacy, or dispensing prescriber name (first and last)	Drug refill number
Dispenser phone number	Drug refill status (to indicate a full or partial refill)
	Drug prescription number

5.2.1.3 Voluntary Access to PDMP Data, Education, and Liability

5.2.1.3.1 No Statutory Duty to Access Data

Considerable public debate exists about whether prescribers and dispensers should be required by law to query PDMP databases or whether access should remain voluntary. Voluntary use of PDMP systems is the legal posture in nearly all jurisdictions. In fact, 17 state PDMP statutes explicitly note that prescribers and dispensers are not legally obligated to query the database. Deliberations within the Law Work Group indicated that mandating PDMP use by statute represents a state's failure to establish adequate incentives that motivate healthcare professionals to embrace a system with real value.

PDMPs are currently underused, but dispensers and prescribers generally oppose laws or regulations that require them to check these systems.

The Work Group preferred voluntary checks of PDMP data over statutorily mandated queries. States should avoid statutory mandates to check data prior to every instance of prescribing or dispensing controlled substances. If a state feels that mandatory checks are absolutely necessary in a certain circumstance, then the number of those circumstances should be limited, such as the first time a prescriber prescribes a controlled substance to a patient. As a better solution, states should consider alternatives to legal mandates that encourage PDMP use and visibility. Such alternatives include (1) mandatory registration to use PDMP systems, (2) PDMP education, or (3) unsolicited PDMP reports. Figure 11 shows states with PDMP laws that explicitly do not require prescribers or dispensers to access PDMP information.

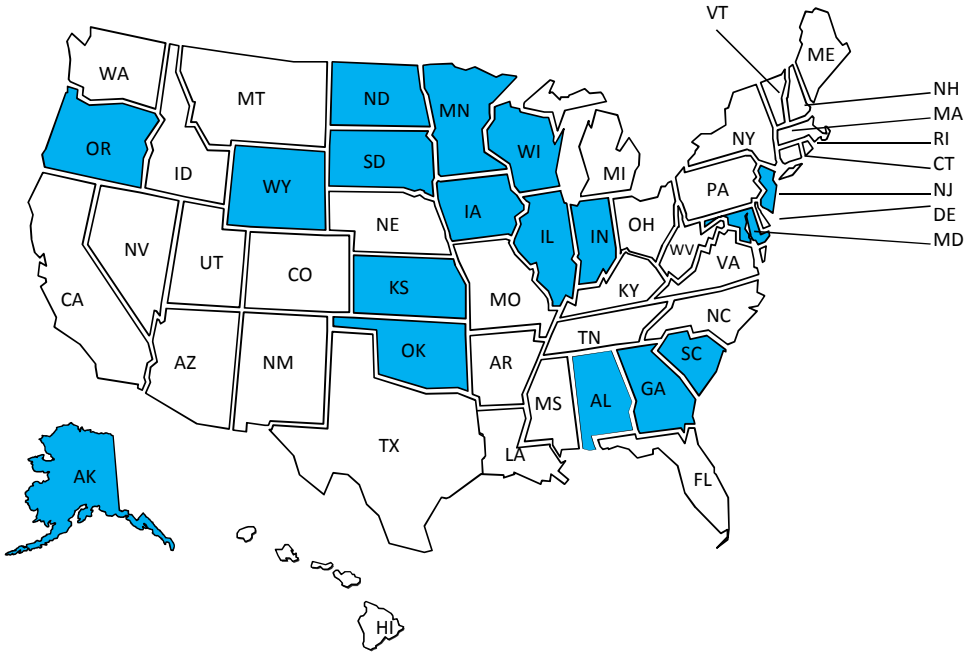


Figure 11. State PMP Laws That Do Not Require Prescribers/Dispensers to Access PMP Information

Recommendation:

States should consider laws and policies that support the use of PDMP databases and services by prescribers, dispensers, and other authorized healthcare professionals. States should not create a statutory duty requiring prescribers, dispensers, or other authorized healthcare professionals to access the database every time a covered controlled substance is prescribed or dispensed.

Statutory Examples:

1. Alabama (Title 20, Chapter 2, Article 10) § 20-2-214 (2): . . . "Practitioners shall have no requirement or obligation to access or check the information in the controlled substances database prior to prescribing, dispensing, or administering medications or as part of their professional practice." . . . (4) . . . Pharmacists shall have no requirement or obligation to access or check the information in the controlled substances database prior to dispensing or administering medications or as part of their professional practice."[65]
2. Alaska (Title 17, Chapter 30, Article 5) § 17.30.200 (h): . . . "Nothing in this section requires or obligates a dispenser or practitioner to access or check the database before dispensing, prescribing, or administering a medication, or providing medical care to a person."[66]
3. Indiana (Title 35, Article 48, Chapter 7) §35-48-7-11.1 (k) "This section may not be construed to require a practitioner to obtain information about a patient from the data base."[67]
4. Kansas (Chapter 65, Article 16) § 65-1688: . . . "Nothing in this act shall be construed to create a duty or otherwise require a person authorized to prescribe or dispense scheduled substances and drug of concern to obtain information about a patient from the prescription monitoring program prior to prescribing or dispensing scheduled substances and drug of concern to such patient."[68]

5.2.1.3.2 Optimal Circumstances for Querying PDMP Databases

Policy makers require guidance regarding the optimal circumstances when a PDMP query is most valuable. By January 1, 2013, 11 states will require access to PDMP information in certain circumstances. This indicates a trend towards mandating PDMP access in specific circumstances, as only six states required such access to PDMP data in 2011. These circumstances vary from state to state and may be limited to (1) when patients receive methadone treatment (as in Colorado) or (2) when medical directors or specialists prescribe controlled substances in pain clinics (as in Louisiana). The following recommendation lists specific events in which the Work

[65] ALA. CODE § 20-2-214 (2008).

[66] ALASKA STAT. §17.30.200 (h) (2011).

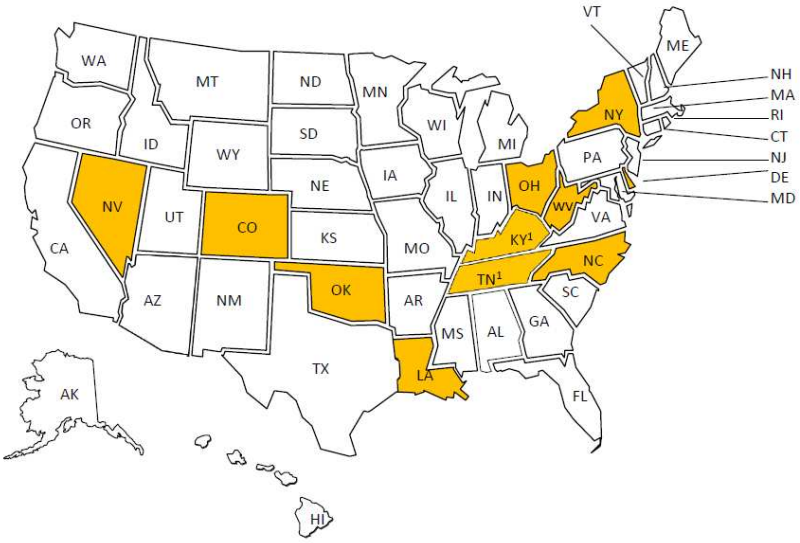
[67] IND. CODE § 35-48-7-11.1 (k) (2011).

[68] KAN, STAT. ANN § 65-1688 (2008).

Group believes practitioners should be encouraged (not legally bound) to query PDMP databases.

An increasing number of prescribers and dispensers are accessing their patients' PDMP information, but these systems remain underused. Prescribers and dispensers prefer the freedom to check data based on their experience and relationship with a patient. The circumstances for initiating a PDMP query listed above represent the Work Group's best judgment, but they should not be interpreted as suggesting a new standard of care.

The members rejected the concept of creating a "national standard of care." As PDMP systems become more common, visible, and accessible, it may become "good medical practice" to query PDMP databases, and one day such checks may become part of a local standard of care. However, this is not the current standard of care in most communities, and such a decision should be left up to local medical boards. Figure 12 highlights states that require prescribers and/or dispensers to access PDMP information in certain circumstances.



* Please see the accompanying memorandum for specifics as to the circumstances under which a prescriber and/or dispenser is obligated to access the PMP database in each state.

[1] The Kentucky law goes into effect in July 2012. Parts of the new Tennessee law go into effect on January 1, 2013, while other aspects go into effect on April 1, 2013. The New York law goes into effect one year after enactment. Please see the companion memorandum for more information.

This information was compiled using legal databases, state agency websites, and direct communications with state PDMP representatives.

Figure 12. States Requiring Prescribers/Dispensers to Access PMP Information

Recommendation:

Prescribers, dispensers, and other authorized healthcare professionals should be encouraged to access the PDMP database regularly. At a minimum, access is particularly useful and strongly encouraged in the following circumstances, where applicable:

- Upon receipt of an unsolicited PDMP report or alert
- Upon initiating a prescribing or dispensing relationship with a patient that potentially involves a controlled substance
- Upon initiating a relationship with patients with significant risk factors, such as a history of substance abuse
- Periodically for continuous prescriptions (e.g., every six months) or as often as clinically indicated
- When a practitioner has either a reasonable suspicion or evidence of abuse, diversion, non-compliance, or misuse or in the presence of an abnormal drug test or drug screening

Prescribers and dispensers should periodically review their prescribing or dispensing history to ensure its accuracy or to detect fraud or forgery.

5.2.1.3.3 Encourage PDMP Use through Mandatory Registration

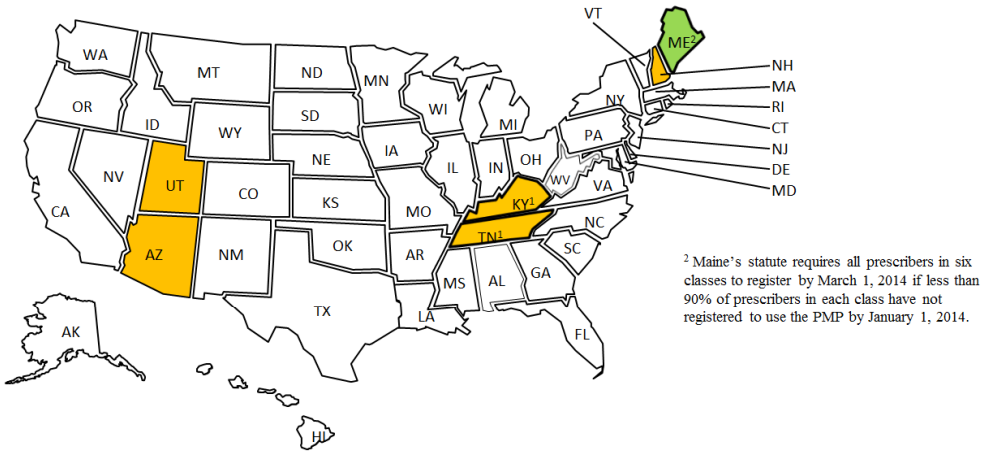
As some states consider making PDMP queries mandatory to increase database use, legislators and PDMP administrators are considering other, less onerous mechanisms to increase participation. Healthcare professionals feel that mandatory queries would be overly burdensome and would interfere with the workflow and flexibility of their practices. However, the same healthcare professionals are less opposed to mandatory registration for a PDMP account, provided the registration process is quick and easy. Finally, many practitioners agree that a minimum level of training on using the PDMP system properly at the time the account is established would encourage greater use and participation.

Many prescribers or dispensers currently do not have user accounts in their state PDMP systems. For example, even though Nevada's PDMP has operated since 1997, only 14 percent of dispensers and 21 percent of prescribers participate.[69] By January 1, 2013, only six states will require practitioners to register for PDMP access.

Obtaining or registering for an account is clearly distinguished from accessing PDMP data. It is less onerous to require practitioners to obtain an account than it is to mandate that practitioners use the account. With a PDMP account, practitioners can receive (1) patient prescription history reports (both solicited and unsolicited), (2) PDMP-specific training, and (3) updates regarding regulatory and policy changes affecting the PDMP. Thus, having this exposure to PDMP systems

[69] The Fix, "Pharmacists Fail to Track 'Scripts," 2011. Available: http://www.thefix.com/content/pharmacists-fail-prescription-monitoring9959.

may encourage use. Figure 13 shows states that require practitioners to register for a PDMP database.



* Many states require that persons requesting access to the state PMP database first register as an authorized user. This map and the accompanying memorandum is concerned with only those states that require all practitioners licensed in the state to also register to use the PMP database.

[1] The Kentucky provision goes into effect in July 2012. The Tennessee provision goes into effect on January 1, 2013.

This information was compiled using legal databases, state agency websites and direct communications with state PDMP representatives

Figure 13. States Requiring Practitioners to Register for PDMP Database

Recommendation:

In the interest of quality patient care and safety, and to increase the use of PDMP systems, states should consider requiring all prescribers and dispensers of controlled substances to obtain an account that enables them to access PDMP data. States should provide a basic PDMP tutorial as a prerequisite to registration for all persons authorized to access PDMP data, both primary account holders and their delegates.

The PDMP tutorial curriculum should include the following topics:

- Proper access and use of the PDMP system, including an understanding of data privacy and security requirements
- Understanding the roles and responsibilities of primary account holders and their sub-account delegates
- How to interpret PDMP reports and understand their limitations
- State laws governing the prescribing of controlled substances
- How to identify common drug-seeking behavior

Statutory Examples:

1. Arizona (Title 36, Chapter 28, Article 1) § 36-2606: "A. Beginning November 1, 2007 and pursuant to rules adopted by the board, each medical practitioner who is issued a license pursuant to title 32 and who possesses a registration under the federal controlled substances act must have a current controlled substances prescription monitoring program registration issued by the board."[70]
2. Utah (Title 58, Chapter 37F, Part 4) § 58-37f-401 (1): "Each individual, other than a veterinarian, who, on June 30, 2010, has a license to prescribe a controlled substance under Chapter 37, Utah Controlled Substances Act, but is not registered with the division to use the database shall, on or before September 30, 2012, register with the division to use the database."[71]

5.2.1.3.4 Increase PDMP Use through Education

Currently, prescribers and dispensers receive little or no training on either the use of PDMP systems or their value to a medical or pharmacy practice when prescribers and dispensers make clinical decisions regarding controlled substance prescriptions. In addition to a basic tutorial regarding proper PDMP system use, prescribers and dispensers could benefit from educational programs about systems and laws. Federal and state agencies, as well as professional organizations and nonprofit entities, could provide such programs.

All personnel who access PDMP databases should be appropriately trained prior to being granted access. The Work Group suggested that states should require personnel to complete a PDMP education course or tutorial as a prerequisite for obtaining a state-issued practitioner license or a state-issued license to prescribe or dispense controlled substances. However, there was no consensus on this point to merit a formal recommendation.

The DEA may consider PDMP controlled-substance training as part of its processes or standards for granting DEA registration numbers. The DEA already requires eight hours of education as a prerequisite for obtaining a registration to prescribe buprenorphine, so a precedent for training exists. By requiring training, the DEA may support the increased use of PDMPs in the future.

Finally, the Work Group expressed concern that a PDMP course should not be a significant burden to practitioners. A brief tutorial may be sufficient at the state level.

[70] ARIZ. REV. STAT. ANN. § 36-2606 (2011).

[71] UTAH CODE ANN. § 58-37f-401 (2011).

Recommendation:

States should develop and make available educational resources to increase PDMP use and awareness. These resources should focus on the role of PDMPs in helping practitioners properly manage patients who are being prescribed controlled substances. If possible, states should work with organizations to integrate PDMP training into appropriate professional continuing education programs. Examples of existing programs include:

- Properly prescribing controlled substances
- Recognizing potential drug dependence or abuse
- Techniques for screening for a substance use disorder or a pain disorder
- How to use EHRs

Statutory Examples:

1. Utah (Title 58, Chapter 37F, Part 4) § 58-37f-401: "(2) Each individual who, on November 1, 2012, is registered with the division to use the database shall, on or before January 1, 2013, participate in the online tutorial and pass the online test described in Section 58-37f-402. . . . (4) Beginning on November 2, 2012, in order to register to use the database, the individual registering must participate in the online tutorial and pass the online test described in Section 58-37f-402. . . . (5) Failure by an individual to comply with the requirements of this section is grounds for the division to take the following actions in accordance with Section 58-1-401: (a) refuse to issue a license to the individual; (b) refuse to renew the individual's license; or (c) revoke, suspend, restrict, or place on probation the license."[72]

5.2.1.3.5 Civil Immunity

State laws are not consistent with regard to civil and criminal immunity for prescribers, dispensers, and other healthcare professionals when they either access or do not access the PDMP database. This inconsistency makes it more challenging for states to share data with each other. Additionally, if a state law does not provide immunity for dispensers who submit patient data to these programs to comply with their statutory duty, then dispensers may be exposed to frivolous lawsuits brought by patients. Though meritless, these suits still would incur a financial burden on dispensers. If immunity for submitting PDMP data exists, then frivolous suits may be avoided. Even if they are brought, such suits could be more easily dismissed at a lower cost to healthcare professionals.

The Work Group declined to offer a policy recommendation that provides immunity to prescribers, dispensers, and other authorized users for either accessing or not accessing the PDMP system. For now, the members felt that immunity for accessing or not accessing the data should remain a state determination that comports with local standards of care.

[72] UTAH CODE ANN. § 58-37f-401 (2011).

However, the members agreed that if dispensers are required by law to submit patient data to these systems, then such dispensers should be immune from civil liability for complying with their legal obligations. No healthcare provider should be sued for complying with the law if they are obligated to submit patient data to the state.

Recommendation:

Dispensers who are required by law to submit patient data to PDMP systems should be immune from civil liability for submitting patient data to the system.

5.2.1.3.6 Civil and Criminal Immunity for Good-Faith Disclosure to Law Enforcement; Disclosure for Treatment

Interstate data sharing becomes more complicated because state laws vary regarding civil or criminal immunity for prescribers, dispensers, and other healthcare professionals. Many state PDMP statutes and regulations require law enforcement to obtain a warrant or court order before they access the database. Law enforcement first must demonstrate adequate cause that a crime either has either occurred or is about to occur.

The medical and law enforcement communities would better complement each other if healthcare professionals could disclose certain PDMP data to law enforcement if healthcare professionals have a reasonable, good-faith belief that such data suggests a crime or unlawful act has occurred or is likely to occur (*prima facie:* good-faith immunity). Additionally, both patient care and public safety are enhanced when healthcare professionals can appropriately share patient data with each other as part of the treatment process. Healthcare providers may be discouraged from using PDMP systems if they believe that they could be sued (either civilly by patients or criminally by the state) for sharing PDMP data with other authorized healthcare professionals for legitimate treatment purposes.

By giving information to law enforcement in good faith or to other healthcare practitioners for treatment purposes when a patient has consented to such treatment, healthcare professionals would not be violating patient confidentiality; there are existing exceptions for such disclosures in the federal context under HIPAA.

Under current federal health privacy laws, patient consent is not required to share sensitive patient data with other healthcare professionals as part of the treatment, payment, or operations (TPO) process. Members feel that state laws should similarly protect healthcare professionals when they need to share such data with other healthcare professionals.

Recommendation:

Prescribers, dispensers, and other healthcare professionals should be immune from civil and criminal liability if they disclose PDMP data to law enforcement officials in good faith. A good-faith disclosure occurs when a professional reasonably believes that a crime or unlawful act may have occurred, based on the professional's knowledge, expertise, and his or her review of the PDMP data. Additionally, prescribers, dispensers, and other healthcare professionals authorized to access PDMP data should be immune from civil and criminal liability if they share PDMP data with each other for legitimate patient treatment purposes.

Statutory Examples:

1. Indiana (Title 35, Article 48, Chapter 7) § 35-48-7-11.1 (n) "A practitioner who in good faith discloses information based on a report from the INSPECT program to a law enforcement agency is immune from criminal or civil liability. A practitioner that discloses information to a law enforcement agency under this subsection is presumed to have acted in good faith."[73]

5.2.1.3.7 Privileged and Confidential Information Not Admissible in Civil Actions; Access for *Bona Fide* Investigations

Some parties have attempted to introduce patient PDMP data in civil actions for divorce or business dissolution. Some groups also are concerned that PDMP data may be considered a public record. When enacting PDMP statutes, states carefully considered patient confidentiality. The Work Group respected this caution, believing states should adopt a uniform approach that ensures PDMP reports do not become public records or tools for leverage in private civil actions.

PDMP data is privileged and confidential; PDMP data should not be admissible in civil actions, and it should not be a public record subject to state or federal freedom of information laws. For example, PDMP data should not be used by former business partners in company dissolution disputes or by spouses in marital disputes, divorce proceedings, or custody battles.

Access to this data by authorized law enforcement or regulatory bodies should only be granted if such entities are directly and actively engaged in legitimate, *bona fide* investigations. Additionally, state and federal laws may require a subpoena, court order, or warrant.

[73] IND. CODE § 35-48-7-11.1(n) (2011).

Recommendation:

All information in state PDMP databases is privileged and confidential and must not be subject to subpoena or discovery in civil proceedings. PDMP data must not be a public record and must not be subject to state or federal open records laws. However, PDMP data may be used for *bona fide* investigations related to violations of state or federal laws. Such investigations must be conducted by (1) authorized law enforcement or (2) authorized regulatory entities charged with oversight of professionals with access to PDMP data.

Statutory Examples:

1. Kansas 65-1685: "(a) The prescription monitoring program database, all information contained therein and any records maintained by the board, or by any entity contracting with the board, submitted to, maintained or stored as a part of the database, shall be privileged and confidential, shall not be subject to subpoena or discovery in civil proceedings and may only be used for investigatory or evidentiary purposes related to violations of state of federal law and regulatory entities charged with administrative oversight of those persons engaged in the prescribing or dispensing of scheduled substances and drugs of concern, shall not be a public record and shall not be subject to the Kansas open records act, K.S.A. 45-215 et seq., and amendments thereto, except as provided in subsections (c) and (d)."[74]
2. Delaware (Title 16, Part IV, Chapter 47, Subchapter VII) § 4798 (h): "Prescription information submitted to the PMP is protected health information, not subject to public or open records law, and not subject to disclosure, except as otherwise provided in this section."[75]
3. Virginia (Chapter 25.1, Title 54.1) § 54.1-2523: "A. All data, records, and reports relating to the prescribing and dispensing of covered substances to recipients and any abstracts from such data, records, and reports that are in the possession of the Prescription Monitoring program pursuant to this chapter and any material relating to the operation or security of the program shall be confidential and shall be exempt from the Virginia Freedom of Information Act. . . ."[76]

[74] KAN. STAT. ANN. § 65-1685 (2008).

[75] DEL. CODE ANN. tit. 16, § 4798 (h) (2010).

[76] VA. CODE ANN. § 54.1-2523 (2009).

5.2.2 Use of Third-Party Intermediaries to Exchange PDMP Data

5.2.2.1 General Guidelines for Sharing PDMP Data with All Intermediaries

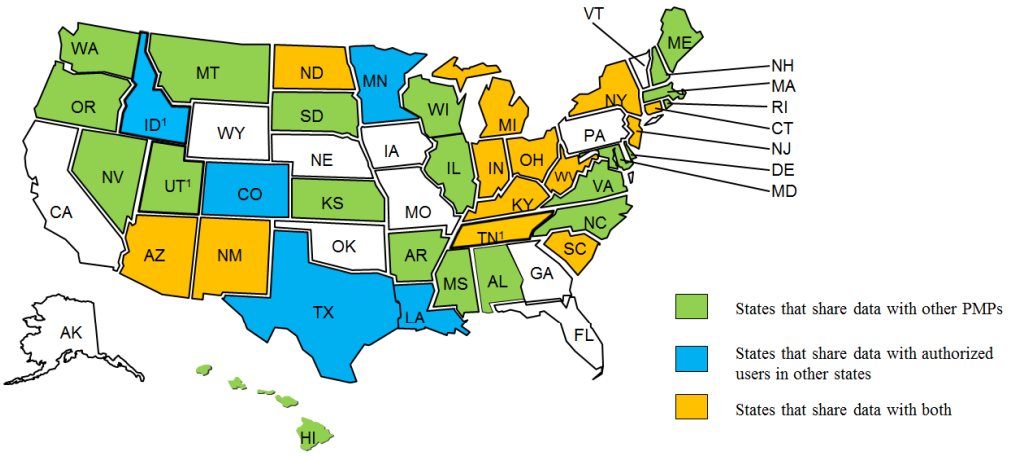
5.2.2.1.1 Legal and Regulatory Compliance

Data sharing among multiple state PDMPs via third-party intermediaries is still a nascent and growing practice that requires significant coordination, cooperation, and standardization. The Law Work Group felt that it would be helpful to identify the general scope of legal instruments that will facilitate the exchange of PDMP data via third-party intermediaries. The form of legal instruments may vary—from business agreements to memoranda of understanding (MOU)—but any agreement for sharing PDMP data should include the basic elements set forth in the following recommendation.

Any intermediary that transmits PDMP data must be able to authenticate the requestor. The authentication process must be able to (1) verify the identity of the requestor and (2) verify the requestor's authority to access PDMP data. When selecting which intermediaries to use to transmit PDMP data, regardless of whether the intermediary is a "Pure Intermediary" or a "Hybrid Intermediary," states should be mindful of fundamental privacy guidelines like the FIPPs and the ONC Privacy Principles. In short, these principles include:

1. Providing individuals with access to their own data and the ability to correct it
2. Transparency with regard to the intermediary's policies and procedures
3. Individual choice as to whether to share personal information with an intermediary
4. Technical and administrative limitations on the collection, use, and disclosure of personal information
5. Processes that ensure an individual's data is accurate
6. Administrative, technical, and physical safeguards to ensure data confidentiality, integrity, and security
7. Accountability of intermediaries through appropriate monitoring and audits to mitigate non-adherence to policies and data breaches

Figure 14 illustrates interstate sharing of PDMP data pursuant to statute, regulation, and/or statutory interpretation.



[1] The Idaho provision will become effective on July 1, 2012. The Tennessee provisions become effective on January 1, 2013. The Utah law became effective on May 8, 2012.

This information was compiled using legal databases, state agency websites and direct communications with state PDMP representatives

Figure 14. Interstate Sharing of PDMP Data

Recommendation:

Any sharing of PDMP data through third-party intermediaries must comply with state and federal laws and regulations. At a minimum, state PDMP laws, regulations, or policies should provide for (1) proper authentication (to ensure that only authorized individuals access PDMP data), (2) data accountability through audits, and (3) rules that govern data collection, use, and disclosure.

5.2.2.1.2 Data Sensitivity

Members of the Law Work Group believe that PDMP data are particularly sensitive, even when they are de-identified. There is also an ongoing dispute over the effectiveness of de-identification and a question of whether data can be re-identified. Some intermediaries may use the data in an unintended way.

Some data are more sensitive than other data (e.g., HIV, mental health, abortion, etc.). Patient consent is not required when sensitive data are transmitted in a traditional directed exchange (e.g., doctor to doctor). However, the increased use of third-party intermediaries to exchange electronic data means that doctors are no longer directly controlling the transfer of patient data.

Technological advancements are fueling a movement toward more granular control over patient information. Some policy advocates favor limited patient control over data (e.g., a patient decides not to share abortion data with a nurse in a podiatrist's office). Technologies that provide a filtering capability are important in advancing trust and should be further explored.

The Work Group acknowledged that in very sensitive cases, it is appropriate that completely separate records are maintained and not released (e.g., substance abuse, abortion). In the case of PDMP data, the members agreed that reasonable safeguards include data encryption during transmission and/or at rest, as appropriate. Intermediaries should never be able to view or process unencrypted PDMP data.

Additionally, regardless of the process of de-identification, intermediaries should not be able to monetize PDMP data. The members acknowledged that there is an ongoing academic and professional debate regarding the effectiveness of de-identification. The Department of Health and Human Services (HHS) is currently revising its de-identification rules and policies. Until HHS provides a solution, the members feel that de-identified data should not be provided to any party seeking to sell or otherwise monetize that data. The restriction on selling or otherwise marketing PDMP data should not interfere with a state's ability to share de-identified PDMP data for bona fide research or public health purposes.

Recommendation:

PDMP systems collect, use, and disclose patients' personal data, which include information about their personal history of controlled substance prescriptions. Due to the inherently sensitive nature of this information, patients should reasonably expect that data collected under PDMP regimes are provided commensurate protections under state and federal laws and regulations.

Due to the inherent sensitivity of PDMP data, intermediaries should not retain legal rights to mine, sell, or otherwise market PDMP data, even if these data are de-identified. These restrictions should be enforceable through data-sharing agreements and MOUs as well as under applicable state laws and regulations.

5.2.2.1.3 Data-Sharing Agreements

The PDMP community requires more standardization regarding data sharing among PDMPs, intermediaries, and other authorized users (prescribers, dispensers, and other authorized healthcare professionals).

Contracts and MOUs are important for establishing the duties and responsibilities of parties to an agreement. If a standard legal agreement is not feasible, such as when one state forms an agreement with another state, then an MOU is preferred. Regardless of the form of agreement, it will be helpful to standardize agreements based on best practices as data sharing between multiple jurisdictions becomes more common.

Additionally, these policy recommendations support the privacy principles of purpose specification, data limitation, and use limitation. Any agreement should specify (1) why patient data are being collected, used, or disclosed; (2) with whom the data will be shared; and (3) the limits on such collection, use, or disclosure.

Recommendation:

State entities that share PDMP data should enter into binding legal agreements, including MOUs, with intermediaries prior to sharing PDMP data. These agreements and MOUs should be informed by applicable state and federal laws and regulations.

Intermediaries should not collect, use, or disclose PDMP data for any purpose other than to provide the services specified (1) in an agreement or MOU, (2) as necessary pursuant to an administrative function, or (3) as required by law or regulations.

5.2.2.2 General Guidelines for Sharing PDMP Data under Any Model That Processes Patient Data Outside the Direct Control of a Provider or Organized Healthcare Arrangement

5.2.2.2.1 Electronic Exchanges and Storage of PDMP Data with Intermediaries

Third-party intermediaries operate different architectural models; some maintain centralized databases that store and process patient PMDP data (centralized model), while others merely reference a patient record locator service (RLS) to route data from multiple end-user databases (federated model). In any scenario, healthcare providers no longer directly control patient data, and privacy and security risks are greater. PDMP laws, regulations, policies, and business agreements must be drafted to mitigate these risks.

Patients reasonably expect that prescribers, dispensers, and other authorized healthcare professionals will share their personal information with other healthcare professionals actively involved in providing treatment to them. In the past, sharing consisted of mailing or faxing patient data and records. In this point-to-point, "directed exchange" model, patient consent is not required to share data because healthcare providers retain control of patient data and clinical records.

As health IT evolves to improve how healthcare providers share patient data, providers will rely less on directed exchange and will rely more on the use of third-party intermediaries to execute electronic data transfers. As a result, providers will not directly control patient data during the exchange; instead, intermediaries will assume at least some responsibility for storing and processing patient data and records. In a centralized data storage model, a centralized database retains patient data and records, making them available to authorized users upon request. Providers may retain copies of patient records in a local EHR, but the intermediary's centralized database also contains patient data and records.

In a federated storage model, patient data and records are stored in databases at each provider location, hospital, or laboratory. The intermediaries serve as hubs that control the ability of authorized users to access and retrieve patient data and records from different databases using an RLS. Although these intermediaries do not store patient data and records, they maintain a master index of patients in the RLS to accurately locate and route queries.

Recommendation:

Any time PDMP data are shared with an intermediary that operates a centralized model, a federated model, or any other architecture in which a patient's provider or organized healthcare arrangement (OHCA) no longer directly controls the collection, use, or disclosure of PDMP data, such collection, use, or disclosure must comply with applicable agreements, MOUs, and state and federal laws and regulations.

5.3 Unexplored Topics

There were some important issues that the members did not have time to address or that were outside the scope of the Work Group. These issues should be addressed in the near future, either by a similar body chartered by HHS or another group of professionals. This section provides a brief summary of these key issues and questions.

5.3.1 Inclusion of Methadone and Veterans Administration Data in PDMP Systems

The Law Work Group agreed that prescribers, dispensers, and other healthcare practitioners authorized to access PDMPs receive an incomplete picture of a patient's prescribing history when records do not include data regarding methadone dispensing by licensed Opioid Treatment Programs (OTP) or data from the U.S. Department of Veterans Affairs (VA). Congress is currently working on a remedy to include VA data in the future. Members expect that federal legislation eventually will enable the VA to share prescription data with state PDMP systems.

The members acknowledge a much greater challenge to sharing methadone data due to federal confidentiality laws that specifically prohibit sharing methadone information (see the Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment and Rehabilitation Act of 1970 and the Drug Abuse Prevention, Treatment and Rehabilitation Act of 1972, currently found in 42 C.F.R., Part 2).[77] 42 C.F.R., Part 2 prohibits sharing any methadone data from an OTP.

The purpose of strict confidentiality was to encourage addicts to participate in methadone programs without worrying that their data would be shared with law enforcement, family, or others who might harbor prejudices against addicts. Such a disclosure could discourage potential program participants from taking advantage of drug programs.

Members acknowledge that public sentiment regarding the stigma attached to addiction has evolved since the early 1970s. As a result, the members hope that federal legislators and policy makers can eventually incorporate the data into PDMP reports without compromising the privacy and confidentiality of affected patients. At the very least, the members agree that this issue should be addressed by another body at some point soon in the future.

[77] 42 C.F.R. § 2.1, et seq. (2012).

5.3.2 Funding for PDMP Systems

The Law Work Group agrees that insufficient funding poses a significant challenge to the future success of state PDMPs. Funding was not an issue within the direct purview of the Work Group's scope, but it is an issue that affects all PDMPs. A few members made brief recommendations regarding potential solutions, which ranged from full federal support to additional state taxes on controlled substance prescriptions. While these suggestions garnered some resistance from within the Work Group, members generally agreed that the financial sustainability of PDMP programs merits a more serious and thoughtful discussion.

5.4 Legal Comparison: Work Group Recommendations and Model State Drug Laws

The Law Work Group comprised active leaders in the promotion of PDMPs who are aware of activities within national organizations such as the National Alliance for Model State Drug Laws (NAMSDL). Although the Work Group did not specifically cite NAMSDL's Model Prescription Monitoring Program (PMP) Act (NMA)[78] as a reference many key components of the NMA can be found in the recommendations. Key issues the Work group tackled—such as the need to expand access, education, and legal immunity—are well known by the PDMP community as issues that need to be addressed in order to further the use and development of PDMPs as a tool to prevent prescription drug abuse. This understanding permeated the discussion and, within the project parameters, the Work Group produced recommendations that reflected both their independent reasoned analysis and what had already been suggested through documents such as the NMA.

The Work Group recommendations do not have a direct correlation to all sections that appear in the NMA. The Work Group did not contemplate certain topics, in part, because of project scope limitations. However, there are enough similarities that the two documents can be considered to complement one another and provide well-reasoned guidelines for a path forward.

Table 7 describes the sections covered by the NAMSDL Model Act (NMA) that are similar or have a limited relationship to the Law Work Group recommendations. Ten Work Group recommendations map to entries in the NMA.

[78] National Alliance for Model State Drug Laws (NAMSDL), "Model Prescription Monitoring Program (PMP) Act," 2011. Available: http://www.namsdl.org/documents/ModelPMPAct111911withoutcommentary_001.pdf.

Table 7. NAMSDL Model Act Sections Aligned with Work Group Recommendations

NAMSDL Model Act (NMA)	Law Work Group	Comments
Section 7: Reporting of Prescription Monitoring Information Information submitted – 7(a)(i)-(xiv)	Related in Section 5.2.1.2: Data Elements Section 5.2.1.2.1: Authorized PDMP Users and Patients Should Be Able to View Information from PDMP Databases in Their EHR	The information recommended by the NMA to be submitted into the PDMP by each dispenser is similar to the Work Group's recommendation for viewable information in a patient's EHR. Note that the Work Groups addressed the data elements that patients should see (not all the data elements that should be captured by the PDMP system). The Usability and Vocabulary Work Groups addressed the latter issue.
Section 8: Access to and Use of the Prescription Monitoring Information; Confidentiality * Confidentiality – 8(a) * Also referenced in NAMSDL June 2012 Components of a Strong Prescription Drug Monitoring Statute/Program-Section (9)	Related in Section 5.2.1.3.7: Privileged and Confidential Information Not Admissible in Civil Action: Access for Bona Fide Investigations	The NMA provides that PDMP data is confidential and is not subject to public or open records laws.
Section 8: Access to and Use of the Prescription Monitoring Information; Confidentiality * Other uses of PDMP data – 8(d) * Also referenced in NAMSDL June 2012 Components of a Strong Prescription Drug Monitoring Statute/Program-Section (3)	Related in Section 5.2.2.1.2: Data Sensitivity	The NMA provides PDMP data may be used for statistical, public research, public policy, or educational purposes after removing personal information and identifiers. The Law Work Group acknowledges these concepts but goes further to state that PDMP data should never be sold or used for marketing purposes.

NAMSDL Model Act (NMA)	Law Work Group	Comments
Section 8: Access to and Use of the Prescription Monitoring Information; Confidentiality * Access by delegates – 8(e)(i) and (ii) * Also referenced in NAMSDL June 2012 Components of a Strong Prescription Drug Monitoring Statute/Program- Section (4)	Section 5.2.1.1.1: Prescribers and Dispensers May Delegate Access	The NMA provides that prescribers, dispensers, and their delegates may access PDMP data after completion of training and education. The Law Work Group also recommends this.
Section 8: Access to and Use of the Prescription Monitoring Information; Confidentiality 8 (e) (iii) and (iv)	Related to Section 5.2.1.3.7: Privileged and Confidential Information Not Admissible in Civil Actions: access for Bona Fide Investigations	The NMA designates law enforcement agent or designated representative from a Licensing agency or board involved in bona fide investigation as having access to the PDMP.
Section 8: Access to and Use of the Prescription Monitoring Information; Confidentiality 8 (e) (v)	Related to section 5.2.2: Use of Third-Party Intermediaries to Exchange PDMP Data	The NMA allows access to any vendor or contractor as necessary for the establishment or maintenance of the PMP. The Work Group acknowledges the role of intermediaries and identified the parameters around their access and responsibilities.
Section 8: Access to and Use of the Prescription Monitoring Information; Confidentiality * Access by drug treatment professionals - 8(e)(vii) * Also referenced in NAMSDL June 2012 Components of a Strong Prescription Drug Monitoring Statute/Program- Section (4)	Section 5.2.1.1.2: Access and Delegation by Other Authorized Healthcare Professionals	The NMA provides that physicians of an alcohol or other drug addiction treatment program should be able to access PDMP data. The Law Work Group also recommended this but went beyond physicians to include any healthcare provider (could be a nurse, assistant, etc.) in a drug treatment program as long as they are helping a bona fide patient.
Section 8: Access to and Use of the Prescription Monitoring Information; Confidentiality Access by patients – 8(g)	Section 5.2.1.1.3: Patients Should Be Able to Access Their Own PDMP Data	The NMA provides that patients should be able to see their own data in accordance with procedures established by the state agency. The Work Group recommends the same.

NAMSDL Model Act (NMA)	Law Work Group	Comments
Section 9: Education and Treatment * Education – 9(a) * Also referenced in NAMSDL June 2012 Components of a Strong Prescription Drug Monitoring Statute/Program-Section (5)	Section 5.2.1.3.4: Increase PDMP Use through Education	The NMA provides for PDMP education programs and training for people who access the PDMP system. The Law Work Group recommends the same.
Section 10: Immunity	Section 5.2.1.3.5: Civil Immunity Section 5.2.1.3.6: Civil and Criminal Immunity for Good-Faith Disclosure to Law Enforcement; Disclosure for Treatment Section 5.2.1.3.7: Privileged and Confidential Information Not Admissible in Civil Actions: Access for Bona Fide Investigations	The NMA goes further than the Work Group regarding immunity for users of the PDMP system. The Work Group limited immunity to (1) complying with law, (2) sharing with law enforcement in a bona fide investigation, or (3) sharing with fellow healthcare providers in the treatment of a patient. The NMA provides immunity for releasing factually incorrect data or releasing data to the wrong person.

Table 8 describes the sections of the NAMSDL Model Act that do not have a corresponding section in the Work Group's recommendations.

Table 8. NAMSDL Model Act Sections Not Covered by Work Group Recommendations

NMA	Law Work Group	Comments
Section 6: Advisory Committee	Not discussed within the scope of Work Group activities	A detailed overview of Advisory Committee formation and membership is provided.
Section 7: Reporting of Prescription Monitoring Information Frequency of reporting – 7(b)	Not clearly represented in Work Group recommendations	The NMA provides a seven-day reporting cycle, with an aspirational clause to adopt real-time reporting ASAP.
Section 8: Access to and Use of the Prescription Monitoring Information; Confidentiality 8 (h)	Not clearly represented in Work Group recommendations	The NMA allows access to PMP officials from other states via interoperability agreements.
Section 8: Access to and Use of the Prescription Monitoring Information; Confidentiality 8 (i)	Not clearly represented in Work Group recommendations	NMA requires designated licensing agencies, etc. to establish standards and procedures for access and use of patient information available via the PMP.
Section 8: Access to and Use of the Prescription Monitoring Information; Confidentiality 8 (j)	Not clearly represented in Work Group recommendations	NMA indicates that no one shall hinder an eligible pharmacist from requesting and receiving information.
Section 8: Access to and Use of the Prescription Monitoring Information; Confidentiality 8 (k)	Not clearly represented in Work Group recommendations	NMA discusses the removal of information from the PMP and the duration of time before this can be done.
Section 9: Education and Treatment * Education - 9(b) * Also referenced in NAMSDL June 2012 Components of a Strong Prescription Drug Monitoring Statute/Program-Section (4)	Not clearly represented in Work Group recommendations	NMA provides for a referral process of prescribers and dispensers in cases of suspected impairment.

Section 9: Education and Treatment * Education – 9(b) * Also referenced in NAMSDL June 2012 Components of a Strong Prescription Drug Monitoring Statute/Program-Section (4)	Not clearly represented in Work Group recommendations	NMA establishes a referral process for patients identified through the PMP as potentially having a substance abuse problem.
Section 11: Unlawful Acts and Penalties	Not clearly represented in Work Group recommendations	The NMA describes procedures for administrative and criminal sanctions. The Work Group's recommendations focused on methods to encourage use and not on the penalties for non-use.
Section 12: Evaluation, Data Analysis and Reporting * Also referenced in NAMSDL June 2012 Components of a Strong Prescription Drug Monitoring Statute/Program-Section (10)	Not clearly represented in Work Group recommendations	The NMA provides a framework for review of the effectiveness of the PDMP.

NAMSDL: Components of a Strong Prescription Drug Monitoring Statute/Program (revised June 2012) not represented in the Law Work Group recommendations:

- Drugs monitored
- Unsolicited and proactive disclosure
- Standards and procedures for access to and use of PMPs
- Linkage to addiction treatment professionals
- Interstate Sharing of PMP data
- Evaluation Component

Recommendations by the Law Work Group (without a clear connection to the NMA) to address some of the issues identified by members and within the scope of the Work Group's assignment:

- 5.2.1.3.1: No statutory duty to access data
- 5.2.1.3.2: Optimal circumstances for querying PDMP databases
- 5.2.1.3.3: Encourage PDMP use through mandatory registration
- 5.2.2.1.2: Data sensitivity
- 5.2.2.1.3: Data sharing agreements
- 5.2.2.2.1: Electronic exchanges and storage of PDMP data with intermediaries

6 Business Agreements for Intermediaries

6.1 Introduction

The Business Agreements for Intermediaries Work Group, also known as the Business Agreements Work Group, explored the existing PDMP and health IT business landscape and developed an agreement framework to help facilitate data sharing through "intermediaries." This term is defined as organizations that serve to connect PDMPs and data users with data flows in both directions, and it includes entities such as HIEs and benefit management switches.

The Business Agreements Work Group set out to achieve three primary goals:

1. Analyze the current business landscape (i.e., major players, stakeholders, interests, regulatory forces, etc.) relevant to the use of intermediaries as conduits for transmissions between PDMPs and data recipients.
2. Address the issue of storage or secondary use of patient information by intermediaries.
3. Produce a set of appropriate reusable model agreements and a framework for implementing them (in conjunction with other supporting legal instruments).

The Business Agreements Work Group identified existing legal instruments that were consistent with the proposed framework and used these instruments to create model agreements for use in a variety of common scenarios. These model agreements should be supplemented with other prescribed instruments as needed within the framework. The content and language of the agreements also may be adjusted to suit specific circumstances. The Work Group assumed that the medical practitioner community would be the primary users of PDMP data transmitted through intermediaries.

6.1.1 Relevant Background

As they mature and are used more widely, PDMPs are expected to make more extensive connections to other parts of the health IT ecosystem. As part of this maturation, strong and enforceable agreements that govern the collection, use, disclosure, storage, and other aspects of PDMP data will become increasingly important. This will apply especially to situations involving third-party intermediaries in the health IT ecosystem. Third-party intermediaries are entities that enable data transport between the producers, custodians, and consumers of electronic healthcare data. In addition to enabling data flows, intermediaries also may perform other business functions, such as generating and marketing secondary data use products. PDMPs may benefit from joining the existing health IT infrastructure for data sharing by working with intermediaries, though this strategy also increases both the operational complexity and the potential for inappropriate exposure (e.g., data breach). See Section 5.2.2 for a more complete and detailed description of the nature of intermediaries and their role.

Though other intermediary types exist, the Business Agreements Work Group focused on pharmacy benefit management switches ("switches") and HIEs, the most common representatives of this category. Both types of intermediaries route transmissions between PDMPs and data recipients, supporting both queries and responses. Other types of intermediaries

also may use the proposed agreements (both model and example) and tailor the instruments to their unique situations.

6.2 Summary of Conclusions

Unlike other Work Groups, the Business Agreements Work Group was primarily charged with drafting and acquiring tangible products rather than focusing on generating implementable (or aspirational) recommendations. The agreement framework and affiliated model and example agreements may provide value to PDMP staffs today rather than suggest useful changes to existing architectures, technologies, laws, or policies for the future.

The model agreements generated by the Work Group can be found in Appendix F. These agreements offer a strong foundation for defining the obligations, duties, and remedies for both public and private parties that wish to share data. The following sections provide an overview of the agreement framework structure, functional descriptions of each model or example agreement, and definitions of the roles of participating entities and organizations that may use these agreements. Finally, the chapter closes with usage guidance and underlying assumptions applied to both the framework and the agreements (Section 6.2.5).

6.2.1 Overall Agreement Framework

The Business Agreements Work Group recommends the implementation of an umbrella agreement framework for PDMP data sharing through intermediaries, as shown in Figure 15. The framework consists of three components:

1. Business associate agreements
2. State boilerplate language
3. “Master” business agreements

Sections 6.2.2 and 6.2.4 describe the nature and use of these instruments. In the framework, the business agreement is the central or “master” agreement, and it is required in all cases. This forms the foundation of the agreement framework. Effective implementation of the agreement framework also requires an understanding of the roles and relationships of entities involved in PDMP data exchange (Section 6.2.3).

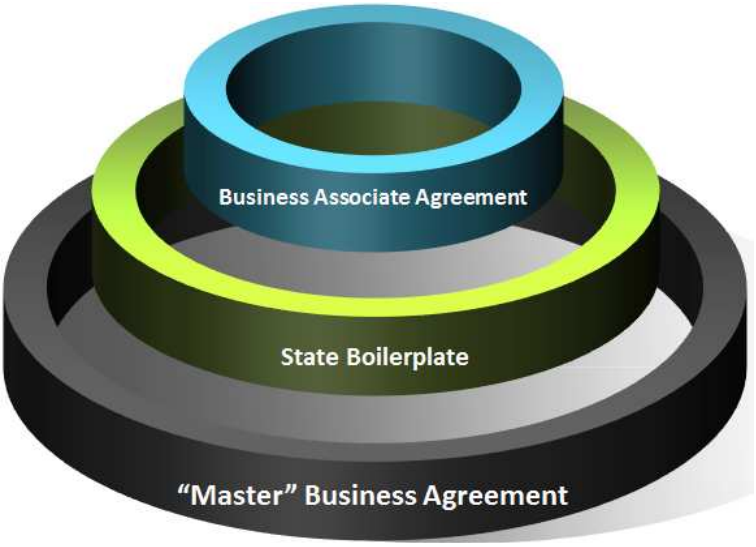


Figure 15. Umbrella Framework

6.2.2 Specific Details on Agreement Types

This section provides an overview of the nature of the individual agreements (both model and example) for use within the proposed agreements framework. This collection of agreements is tailored for use by PDMPs and their prospective data recipients. See Section 6.2.4 for details on the optimal use of these instruments.

6.2.2.1 Business Agreements

The business agreement is the primary legal instrument between the PDMP and the entity that transmits the data to a consumer or downstream intermediary. It is the central agreement, or "master agreement," and it is required in all cases under an implementation of the agreement framework (see Section 6.2.4.1). "Clean" (ready for use) and "marked-up" (annotated with the reasoning behind provisions) versions of these model agreements are provided in Appendix F. There are two types of business agreements based on the types of entities involved in the data exchange: (1) business agreements between two public entities ("Public Entity to Public Entity Business Agreement") and (2) business agreements between a public organization and a private entity ("Public Entity to Private Entity Business Agreement"). To comply with the proposed framework and to serve as its foundational instrument, both types of business agreements must contain the following eight elements:

1. Scope of work and transaction standards (as needed)
2. Downstream pass-through requirements
3. Liabilities*
4. Indemnifications*
5. Payments (if any)
6. Sanctions/terms*
7. Authorized users
8. Secondary data uses

Elements with an asterisk ("*") indicate fields that may be covered by state boilerplate language (see Section 6.2.2.3); they are therefore situational, depending on the state's existing laws and policies.

Appendix F.5 shows the detailed mapping of these eight elements to particular sections of the Public Entity to Public Entity and Public Entity to Private Entity Business Agreements provided in Appendix F.

6.2.2.2 Business Associate Agreements

Business associate agreements (BAAs) are a well-known part of the health IT landscape. They are typically required when at least one party qualifies as a business associate (BA) of a covered entity (CE) under HIPAA[79] and HITECH[80]. PDMP data reporters (e.g., pharmacists) and users (e.g., pharmacists, physicians) typically are covered entities, while the PDMPs themselves typically are not. Switches (e.g., pharmacy benefit management switches) and HIEs typically are BAs because they process PHI on behalf of covered entities. In some cases, the entities involved in data exchange already have a BAA in place prior to implementing the framework.

Typical BAAs and those consistent with the proposed framework contain the following minimum elements:

1. Definitions
2. Obligations and activities of BAs
3. Permitted uses and disclosures by BAs of PHI
4. Term and termination

Appendix F.7 provides an example BAA from the public domain, the West Virginia State Government HIPAA Business Associate Addendum. This instrument is automatically made a term and condition of every state contract that may involve the disclosure of PHI in West Virginia, as per the requirements of the state boilerplate (see Section 6.2.2.3). The Work Group considered this a good example of this type of instrument.

6.2.2.3 State Boilerplate Language

State boilerplate language contains the compliance provisions that are typical and necessary for state agreements and procurement contracts. PDMPs usually are created by state statutes and are administered by government bodies that pass rules and regulations that govern how PDMPs operate, and as such these terms are germane. The Work Group assumed that each state has its own specific statutory language based on its own contract and procurement laws and policies. These terms can be introduced either as an addendum to other instruments in the framework or through a separate agreement.

The state boilerplate example instrument provided in Appendix F.7 is the *West Virginia General Terms and Conditions for Purchase Orders and Contracts*. This document is used in conjunction with the BA addendum in Appendix F.6 as described in Section 6.2.2.2. State boilerplate

[79] Health Insurance Portability and Accountability Act of 1996, Public Law (PL) 104-191 ("HIPAA"), 45 C.F.R. Parts 160 and 164 ("the Privacy Rule").

[80] HITECH: PL 111–5—FEB. 17, 2009 123 STAT. 227.

language may be more or less restrictive than this example. The Work Group does not recommend specific state boilerplate language.

6.2.3 Roles

This section provides specific details about the roles of various entities within a PDMP exchange business landscape under the framework view. Figure 16 illustrates these roles and relationships, and Table 9 describes each role. Understanding and appropriately assigning these roles to the entities is critical for using the proposed agreement framework. Under the framework, switch and HIE intermediaries are treated as functionally identical entities. This provided a considerable simplification for the framework development as well as for subsequent implementation.

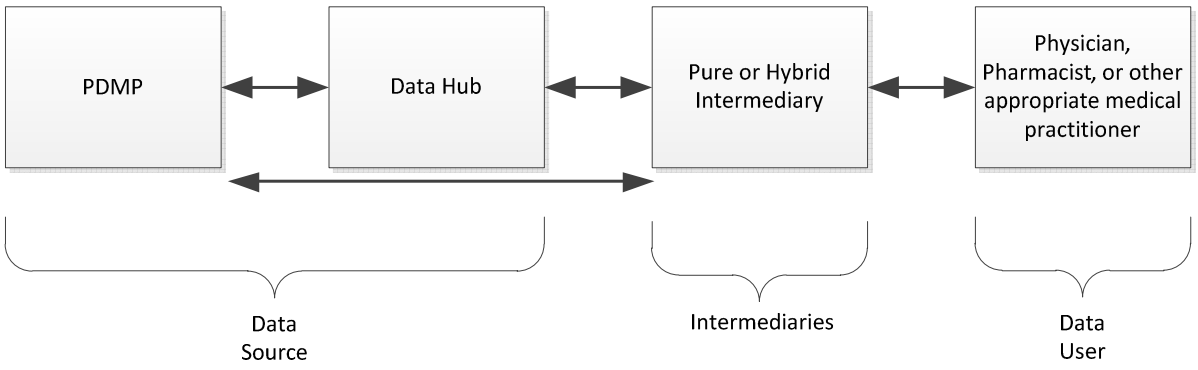


Figure 16. Business Landscape Roles and Data Flow

Table 9. Description of Roles

Role	Description
Data Source	The source of the prescription drug monitoring data. This is typically the PDMP, sometimes in conjunction with a Data Hub (see next row). When a PDMP and Data Hub both comprise the Data Source, it may be referred to as a "Compound Data Source."
Data Hub	Typically an interstate PDMP Data Exchange (e.g., PMPi, RxCheck).
Packager	The holder of the "master agreement" (see Section 6.2.2.1) with the Data Source and typically a "hybrid" intermediary (see next row). Identification of this entity is a key factor for correctly implementing the agreement framework.
Hybrid Intermediary	An intermediary that assembles data from different sources and stores, changes, or aggregates PDMP data. Switches often are hybrid intermediaries, while HIEs can be either pure or hybrid intermediaries, depending on their specific activities and role(s).
Pure Intermediary	An intermediary that provides a "blind pipe" pass-through service for the PDMP data. By definition, pure intermediaries cannot assemble, store, change, aggregate, or otherwise use PDMP data.

Role	Description
Data User	The consumer of the PDMP data, such as an ambulatory provider, emergency department physician, or pharmacist, and typically a covered entity. Other potential user types (pharmacy boards, law enforcement) were not specifically addressed in detail in this framework, but they may be relevant to participants.

6.2.4 Using the Agreements and the Framework

This section provides details that PDMP data-exchange participants need to effectively implement the agreement framework. The Business Agreements Work Group offered the following detailed guidance for using the framework and component agreements.

6.2.4.1 Full Framework Application

The Work Group recommended that the agreement framework and role definitions, as described in Figures 15 and 16, be followed when selecting which agreements to use. The Work Group strongly believes that the BA is always necessary and desirable, whereas the BAA and state boilerplate language will vary based on circumstances. For example, state boilerplate language is typically less necessary in cases where all intermediaries between the Data Source and Recipient are public entities within the same state.

The issue of whether a new BAA must be introduced between two entities may be complex and will depend on what agreements are already in place and the relationship between the entities. In general, a BAA will add helpful provisions and will increase the overall strength of a Public Entity to Public Entity Business Agreement, but it may not always be necessary in this case. This will depend on circumstances, and the Work Group analysis enumerated examples of both scenarios. However, use of a BAA is strongly recommended when considering Public Entity to Private Entity Business Agreements. Finally, the Work Group determined that using a BAA alone would be considerably less desirable than including it in conjunction with a Business Agreement ("Master"), as per the framework.

The order of entities in a data flow (Figure 16) may matter in some situations as to the agreements to be put in place, but identifying the Packager is by far the most important issue when deciding on which agreements to use at which position. The connection between the Data Source and the Packager is the link least likely to have an adequate existing agreement. Conversely, a pre-existing agreement (typically BAA) between a PDMP and a Data Hub that resides within a Compound Data Source (see Table 9) is likely sufficient for that transaction.

The Business Agreements Work Group determined that the use of lesser agreement types as a substitute for BAAs, such as typical MOUs, should be avoided. This is based not only on the strength and comprehensiveness of the BAA but also on the understanding that states and private entities prefer formal agreements that are enforceable in courts.

6.2.4.2 Customization

The model business agreements are intended to be highly configurable so that they may be easily adapted to unique circumstances. By design, they are a partial solution, allowing parties to focus

on fine-tuning rather than developing new agreements from scratch. Nevertheless, the effort required to draft the remaining 20 percent of the agreement may be considerable.

6.2.4.3 Sub-Agreements

In cases where multiple agreements are necessary for the data flow (i.e., more than one intermediary between Data Source and Data User), all sub-agreements should originate from the primary business agreement between the Data Source and Packager ("master agreement"). In this way, the Packager becomes the "Agreement Hub"; all entities will be subcontractors of this entity. This produces a significant simplification in the agreement structure: all agreements will originate from this one document.

6.2.4.4 Unilateral Modification Requirement

The Packager should have the authority to unilaterally amend the "master" business agreement and all instruments emanating from it, but only to ensure conformity to legislative changes and updates to privacy and security laws. Renegotiation can be lengthy and expensive, so enabling the Packager to update the master business agreement allows all the parties to rapidly address and conform to changes in the law.

The Work Group also found that states typically desire a "termination of convenience" clause in agreements with nonpublic entities (and perhaps public entities of other states). States usually prefer to avoid expensive and time-consuming remedies such as arbitration or litigation that often are the result of "termination for cause" clauses.

6.2.5 Assumptions

The Work Group noted the following assumptions when designing the agreement framework and crafting the model agreements. Deviation from these assumptions may require re-analysis of the agreements needed.

6.2.5.1 Treatment, Payment, and Operations Focus

The agreements are focused on TPO activities; other services are not necessarily well supported under this agreement framework or by these instruments. Moving too deeply into other issues, such as secondary uses of data or marketing health data for profit, can drastically increase the complexity of the agreements necessary for execution.

6.2.5.2 Authorized Users

All participants must ensure that all Data Users and intermediaries have the authorization to access the PDMP information that they need to see. The model agreements provide areas to enumerate these users, but they do not address how users come to be defined as authorized. Statutory requirements, both state and federal, must be met in all cases.

6.2.5.3 Data Custody View

The focus of the agreements should be on data custody, not data ownership. The Work Group believes the issue of ownership has larger legal ramifications than can be addressed in the framework or by the model agreements. The Work Group acknowledges that there may be a degree of disagreement in the PDMP community regarding this posture.

6.2.5.4 In-Place "Compound Data Source" Agreements

The relationship between a PDMP partnering with an interstate Data Hub to create a "Compound Data Source" is likely to be covered already by appropriate existing agreements. This is discussed in Section 6.2.4.1.

6.2.5.5 State PDMP Focus

The impact of a non-state (i.e., non-public entity) PDMP in the framework has not been comprehensively addressed here. Based on a survey of the emerging business landscape, the Work Group believed that this is a realistic option, especially given the existence of a commercial intermediary acting as a PDMP or a PDMP that resides entirely within an HIE entity.

6.2.5.6 Intermediaries Present

Direct PDMP data sharing between Data Source and Data Recipient (i.e., not through intermediaries) is not addressed, by definition, in the output of the Work Group.

6.2.5.7 Medical Use Prioritized

The Work Group operated under the premise that use by the medical practitioner community, not that of law enforcement or licensing agencies, would be the focus of the agreements. This view is typically described in the "recitals" present in the model agreements. This view may not be fully consistent with that of all states, and the agreements should be modified to reflect each state's requirements as part of the customization process.

7 Discussion

7.1 Future Directions

In addition to the recommendations, conclusions, and artifacts described in Sections 1–6, the Work Groups identified areas that could not be addressed fully within the context of the existing mandates. The Work Groups declared these items outside of project scope, but they are captured in this section for future investigation and action.

7.1.1 Records Maintenance

The length of time that medical records are kept may not be well established in some states, and this could be an issue. Some existing policies are based on a law enforcement perspective. In other cases, contracts and payers as well as tort claims are driving the retention period (e.g., some obstetricians keep records for18 years to cover themselves from birthing error damage claims). A more comprehensive review could lead to a clearer set of guidelines for this important topic.

7.1.2 Access at Individual and System Levels

A clear case can be made for the value that can be added by developing a directory to identify users and authorization information. This also would ideally include specifics of how to interact with authorized users (e.g., delivery of reports via email, fax, etc.). The establishment of such a directory is a precondition of the next logical step: implementing a framework to enable transparent system-to-system communications for which passing of credentials is the key element (not username, but system authorization credentials). Such an architecture would need to possess the ability to support both synchronous and asynchronous requests and the delivery of information to the requesting user or application, as these are the expected use cases. This would considerably reduce the overhead some users face for PDMP data access (e.g., multiple passwords for practitioners who work at multiple venues).

7.1.3 Unification of PDMP with the Risk Evaluation and Mitigation Strategy

The existing REMS infrastructure, including support for strong audit trails and inventory control, operates as a *de facto* parallel (and more stringent) PDMP infrastructure. This bifurcation may not be desirable from the standpoint of reducing total costs.

7.1.4 Unification of ASAP with the SCRIPT Standard

Pharmacies submit data to PDMPs via the ASAP standard, yet a parallel data stream also is in place: the NCPDP SCRIPT Standard. Established in 1997, this standard facilitates transferring prescription data among prescribers, pharmacies, payers, and other entities. It supports prescriptions, refill requests, fill status notification, and other related events. This standard has been extended to support alerts for DUR and medication allergies as well as standardized medication nomenclature. Electronic prescription exchanges that use this standard typically are well integrated into standard business processes and workflows in the health IT arena. Consolidating these two standards may yield the highest degree of data capture for PDMPs while minimizing impingement on existing workflows.

7.1.5 Unified Interface Architecture

The recommendations provided in this report move the PDMP community toward a common set of interface specifications. However, the recommendations are not fully comprehensive, in part because the effort required to completely parameterize all expected use cases is beyond the scope of Work Group activities. A unified view of parameters for report-generating interfaces would be of considerable value to the PDMP community. This information should be developed as formal interface specifications for system implementers.

7.1.6 Data Input and Error Correction

While the Work Groups examined existing methods involved in PDMP data submission, they did not fully explore the engineering of optimal mechanisms to ensure timely and accurate PDMP data for use by practitioners. Members identified a mechanism for patients and prescribers to identify and correct errors in PDMP records as necessary, but they did not identify a path forward.

7.2 Conclusions

The United States has a growing problem with prescription drug abuse and misuse. Currently, separate state-run PDMP systems collect data on the dispensation of controlled substances. However, system and policy barriers make using PDMP information at the point of care difficult. The purpose of this project was to address issues with PDMP access and interoperability.

The five Work Groups discussed the primary problems facing the transport and use of PDMP data today. The members discussed these issues and developed recommendations concerning a variety of topics. First, Work Groups provided recommendations to address the presentation of PDMP information for dispensers and prescribers, also known as the Users of PDMP data. Ideally, these Users should be able to easily and efficiently view the PDMP information without diverting from their normal workflow. Second, several recommendations concerned the exchange of PDMP information. The members recommended that data standards and technical specifications be used for transmitting PDMP data across systems. The Work Groups also developed generic and business-agreement frameworks to help facilitate data sharing. Finally, the members produced several policy recommendations meant to improve PDMP data access and sharing.

Ultimately, these recommendations should facilitate PDMP information sharing so that dispensers and prescribers can more efficiently and effectively use the information to make clinical judgments.

Acronyms

ADT	Admission, Discharge, Transfer
API	Application Programming Interface
ASAP	American Society for Automation in Pharmacy
BA	Business Associate
BAA	Business Associate Agreement (by HIPAA definition)
BJA	Bureau of Justice Assistance
CE	Covered Entity
CDC	Centers for Disease Control and Prevention
CS	Controlled Substance
DEA	Drug Enforcement Agency
DUR	Drug Utilization Review
EA	Enterprise architecture
ED	Emergency Department
EAF	Enterprise Architecture Framework
EHR	Electronic Health Records
ESRD	End-Stage Renal Disease
FDA	Food and Drug Administration
FIPP	Fair Information Practice Principles
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act of 2002
HHS	Department of Health and Human Services
HIE	Health Information Exchange
HIPAA	Health Insurance Portability and Accountability Act
HITECH	Health Information Technology for Economic and Clinical Health Act
HITSP	Health Information Technology Standards Panel
ID	Identification
IEPD	Information Exchange Package Documentation
IP	Internet Protocol
IPSEC	Internet Protocol Security
IT	Information Technology
MOU	Memorandum of Understanding
NABP	National Association of Boards of Pharmacy
NAMSDL	National Alliance for Model State Drug Laws
NCPDP	National Council for Prescription Drug Programs

NDC	National Drug Code
NIEM	National Information Exchange Model
NIST	National Institute of Standards and Technology
NMA	NAMSDL Model Act
NPI	National Provider Identifier
OECD	Organization for Economic Co-operation and Development
OHCA	Organized Healthcare Arrangement
ONC	Office of the National Coordinator for Health Information Technology
OTP	Opioid Treatment Program
PDMP	Prescription Drug Monitoring Program
PHI	Protected Health Information
PMIX	Prescription Monitoring Information Exchange
PMP	Prescription Monitoring Program
PMPi	Prescription Monitoring Program Interconnect (a Data Hub of NABP)
REMS	Risk Evaluation and Mitigation Strategy
REST	Representational State Transfer
RLS	Record Locator Service
SAMHSA	Substance Abuse and Mental Health Services Administration
SOA	Service-Oriented Architecture
SOAP	Simple Object Access Protocol
SSL	Secure Sockets Layer
SSO	Single Sign-On
TLS	Transport Layer Security
TPO	Treatment, Payment, and Operations
UCD	User-Centered Design
UI	User Interface
VA	Department of Veterans Affairs
VPN	Virtual Private Network
XML	Extensible Markup Language

Appendix A Mapping of Recommendations and Products to Tasks in the Action Plan

Table 10 maps the Work Group recommendations and products to the original tasks listed in the Obama Administration's 2011 Action Plan to address the prescription drug abuse crisis.[81] This mapping also applies to the pilot activities described in greater detail in the following sections of this appendix.

Table 10. Task Mapping of PDMP Recommendations and Products

Task #	Task Description	Recommendations	Products	PROV-A	PROV-B	PROV-C	ED-A	ED-B	ED-C	ED-D	PHARM-A	PHARM-B
1a	Harmonize data messaging and formatting standards for communicating with interstate data exchanges	2.2.1-2, 3.2.1.1-3, 3.2.2.1-4, 3.2.3.4, 4.2.1-3	C1, 3.2.1.2 - C2, 3.2.1.3 - C3, 3.2.3.4 - C4	X	X	X	X	X	X	X	X	X
2a	Develop standards for the user interfaces and identify the data elements and format for EHR presentation	2.2.1-2, 2.2.1.4, 2.2.2.3-5, 2.2.3.1, 5.2.1.2.1, 3.2.3.4, 4.2.8	C1, 3.2.1.2 - C2, 3.2.3.4 - C4, D1 (4.2.2)		X	X		X	X	X		
3a	Develop standards for the user interfaces and identify the data elements and format for pharmacy system presentation	2.2.1-2, 2.2.1.4, 2.2.2.3-5, 2.2.3.1, 5.2.1.2.1, 3.2.3.4, 4.2.8	C1, 3.2.1.2 - C2, 3.2.3.4 - C4, D1 (4.2.2)									X
4a	Review state laws and current policies for PDMP use of intermediaries	5.2.2.1.1, 5.2.2.1.3, 5.2.2.2.1, 6.2.1	6.2.2.1-3		X	X			X	X		X
4b	Review state laws for delegation by the pharmacist to the pharmacy and the physician to the hospital	5.2.1.1.1-2					X	X	X			X
4c	Review current (legal) policies and practices for "Dummy BINs"	4.2.7										X

[81] Prescription Drug Abuse and Health Information Technology Work Group. (2011). "Action Plan for Improving Access to Prescription Drug Monitoring Programs through Health Information Technology." http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_0_9025_3814_28322_43/http%3B/wci-pubcontent/publish/onc/public_communities/_content/files/063012_final_action_plan_clearance.pdf

Task #	Task Description	Recommendations	Products	PROV-A	PROV-B	PROV-C	ED-A	ED-B	ED-C	ED-D	PHARM-A	PHARM-B
4d	Reviewing current policies and practices for role based access (pharmacy, ED)	5.2.1.1.1-2						X	X			X
5a	Review current (technical) policies and practices for “Dummy BINs”	4.2.7										X
6a	Review current pharmacy chain policies and practices for to delegating access to PDMP data	5.2.1.1.1-2										X
7a	Analyze current protocols for switch organizations to participate in routing queries between PDMPs and recipients	4.2.5, 4.2.7			X	X						X
7b	Develop a model business agreement for switch organization data sharing	6.2.1	6.2.2.1-3		X	X						X

A.1 Pilot Studies

Table 11. Pilot Study Table

Technology Enabler	Ambulatory Provider	ED Provider	Pharmacist
Direct Messaging	PROV-A	ED-A	PHARM-A
Query Trigger		ED-B	
Trigger/Switch	PROV-B		PHARM-B
Trigger/HIE		ED-C	
Trigger/Switch & HIE	PROV-C		
HIE		ED-D	

Common Recommendations

A common set of recommendations and products apply to all nine pilot studies, as outlined in Tables 12 and 13. These recommendations should be championed by a single or coordinated set of organizations and rolled out to individual states and vendors. These prescribed standards and specifications, if applied universally, would benefit all stakeholders.

Table 12. Common Recommendations for All Pilot Studies

Recommendations	Relevant Sections
Complete list of data elements for PDMP reports	2.2.1-2 3.2.3.4
Adopt the proposed common set of PDMP Data Elements for storage purposes, largely based on ASAP format	3.2.1.1
Adopt the proposed Data Element Exchange Standard via the NIEM Prescription Monitoring Program specifications and use this as the domain standard for PDMP data exchange	3.2.1.2 4.2.1
Adopt the proposed Cross-Reference Guide to facilitate consistent, accurate, and unambiguous data exchange between systems	3.2.1.3
Use the proposed set of minimum information required to uniquely identify a patient, dispenser, prescriber, and authorized user	3.2.2.1-4
Leverage the NIEM-based information exchange specification to develop a common PDMP API to be used for XML-based data transport	4.2.2-3

Table 13. Common Products for All Pilot Studies

Products	Relevant Sections
Data Elements	C1
PDMP Data Element Exchange Standard	3.2.1.2 - C2
Cross-Reference Guide for PDMP Data Elements and Specifications	3.2.1.3 - C3
Data Element Usage in PDMP Reports	3.2.3.4 - C4

A.1.1 Provider Pilot Study A

PDMP system identifies patients at risk and sends a message via Direct to all providers that have previously prescribed to the patient (patients at risk – minimal patient information) with link back to the PDMP (provider accesses PDMP for patient scheduled drug history). Alternatively, the Direct message may contain more detailed patient records. Note that the cutoff for patients at risk varies by state. Integration of the message with the EHR system is implied.

In addition to implementing the actual technology, this pilot requires only the common recommendations and products in Tables 12 and 13 to succeed. Figure 17 illustrates this pilot overview.

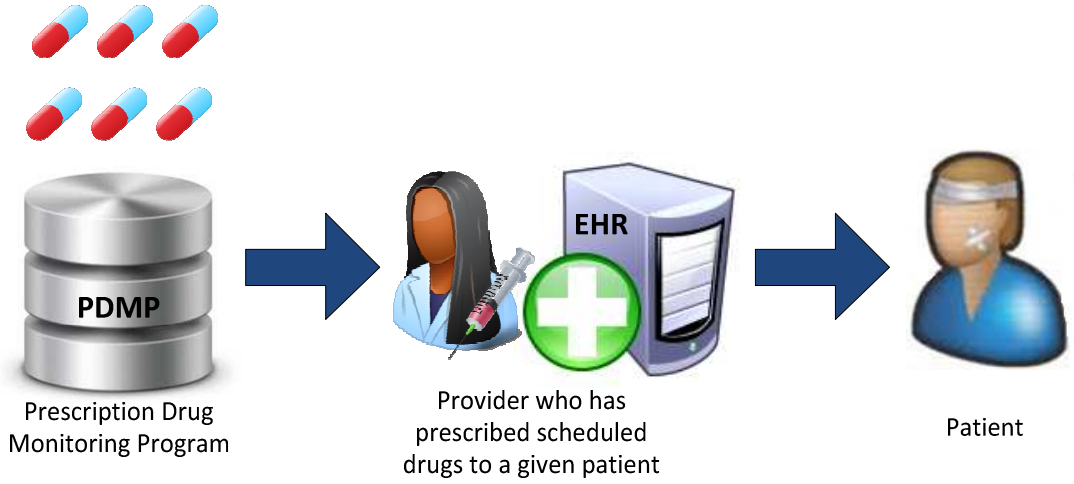


Figure 17. Provider A Pilot Overview

A.1.2 Provider Pilot Study B

Provider EHR, Switch, PDMP/Solicited Report

Patient makes an appointment or visits the doctor. When appointment/visit is logged into the provider's EHR, this triggers an eligibility check via a switch, which triggers a (switch) drug history and PDMP query. PDMP returns patient at risk – scheduled drug history via the switch. Figure 18 illustrates this pilot overview. In addition to the common recommendations and products, the pilot also requires those listed in Tables 14 and 15.

Table 14. Additional Recommendations for Provider Pilot Study B

Recommendations	Relevant Sections
Full integration of PDMP information in user systems (EHR, pharmacy), with storage and smart sorting/filtering	2.2.2.4 5.2.1.2.1
Users should receive a minimum of six months of a patient's controlled substance (CS) history	2.2.1.4
Enablers of workflow integration (SSO, links)	2.2.2.3
At-risk filter and alerting options, for both solicited and unsolicited usage	2.2.2.5 2.2.3.1 4.2.8
Sharing of PDMP data through third-party intermediaries must comply with state and federal laws and regulations, as well as applicable legally binding agreements (e.g., MOUs)	5.2.2.1.1 5.2.2.2.1 5.2.2.1.3
For intermediary-enabled sharing, entities should utilize the proposed agreement framework to minimize risk	6.2.1
Co-transmission of queries to PDMPs is deemed technically and operationally inadvisable	4.2.7
An appropriate framework for message security should be applied to ensure compliance with HIPAA and state privacy laws	4.2.5

Table 15. Additional Products for Provider Pilot Study B

Products	Relevant Sections
Template for Interface Parameters Supported by PDMP by Report	D1 (4.2.2)
Master Business Agreement	6.2.2.1
Exemplar BAA	6.2.2.2
State Boilerplate Language Example	6.2.2.3

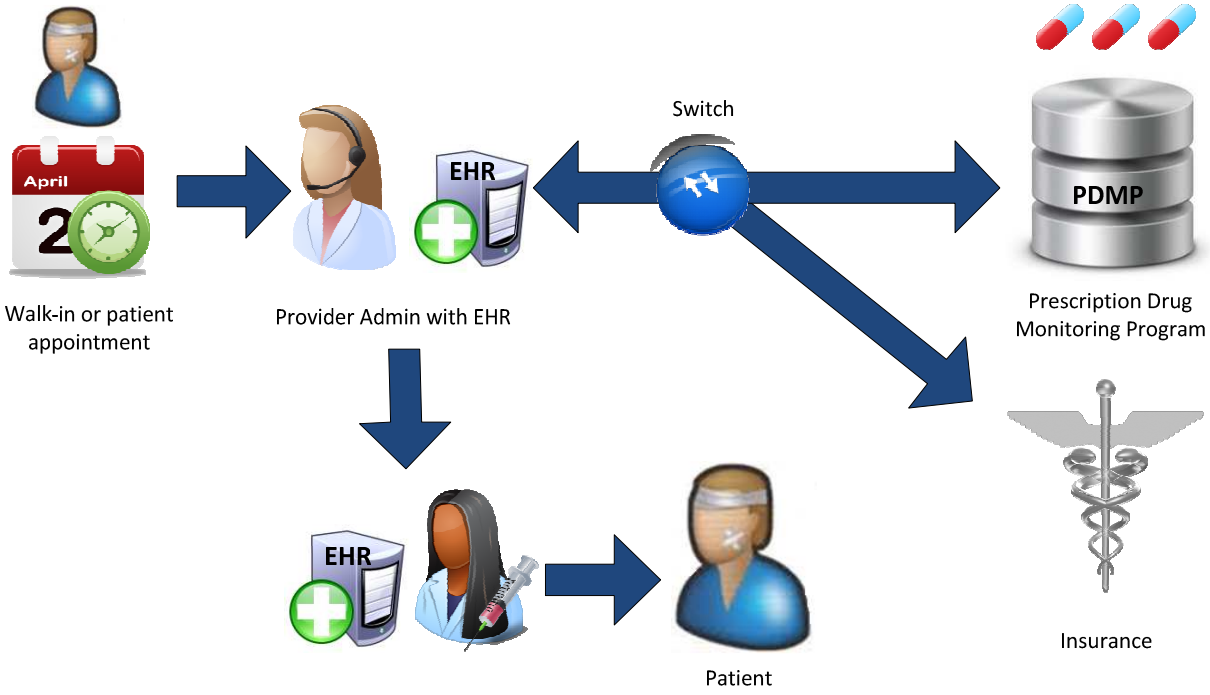


Figure 18. Provider B Pilot Overview

A.1.3 Provider Pilot Study C

Provider EHR, Switch, HIE, PDMP/Solicited Report

Patient makes an appointment or visits the doctor. When appointment/visit is logged into the provider's EHR, this triggers an eligibility check via a Switch, which triggers a (switch) drug history and PDMP query via an HIE. PDMP returns patient at risk – scheduled drug history via the HIE and the switch. Figure 19 illustrates this pilot overview. In addition to the common recommendations and products, the pilot also requires those listed in Tables 16 and 17.

Table 16. Additional Recommendations for Provider Pilot Study C

Recommendations	Relevant Sections
Full integration of PDMP information in user systems (EHR, pharmacy), with storage and smart sorting/filtering	2.2.2.4 5.2.1.2.1
Users should receive a minimum of six months of a patient's CS history	2.2.1.4
Enablers of workflow integration (SSO, links)	2.2.2.3
At-risk filter and alerting options, for both solicited and unsolicited usage	2.2.2.5 2.2.3.1 4.2.8
Sharing of PDMP data through third-party intermediaries must comply with state and federal laws and regulations, as well as applicable legally binding agreements (e.g., MOUs)	5.2.2.1.1 5.2.2.1.3 5.2.2.2.1
For intermediary-enabled sharing, entities should utilize the proposed agreement framework to minimize risk	6.2.1
Co-transmission of queries to PDMPs is deemed technically and operationally inadvisable	4.2.7
An appropriate framework for message security should be applied to ensure compliance with HIPAA and state privacy laws	4.2.5

Table 17. Additional Products for Provider Pilot Study C

Products	Relevant Sections
Template for Interface Parameters Supported by PDMP by Report	D1 (4.2.2)
Master Business Agreement	6.2.2.1
Exemplar BAA	6.2.2.2
State Boilerplate Language Example	6.2.2.3

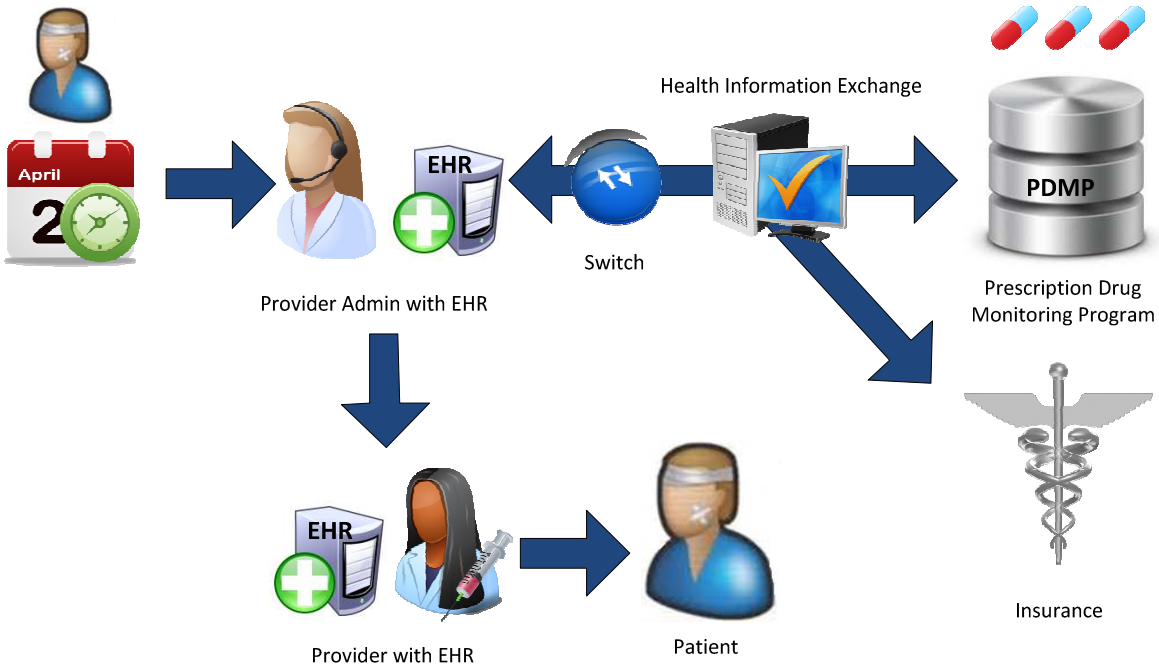


Figure 19. Provider C Pilot Overview

A.1.4 Emergency Department Pilot Study A

PDMP, Direct, ED EHR /Unsolicited Report

The PDMP sends a secure Direct message to the patient's providers, which includes minimal patient information, but alerts the provider/pharmacist to check the PDMP and the link. Alternatively, the message is sent via secure Direct message to the patient's providers and includes the patient's scheduled drug history. Note that the cutoff for patients at risk varies by state. Integration of the message with the EHR system is implied. Figure 20 illustrates this pilot overview. In addition to the common recommendations and products, the pilot also requires those listed in Table 18.

Table 18. Additional Recommendations for ED Pilot Study A

Recommendations	Relevant Sections
Prescribers, dispensers, and other healthcare professionals should have PDMP access and the ability to appoint delegates	5.2.1.1.1-2

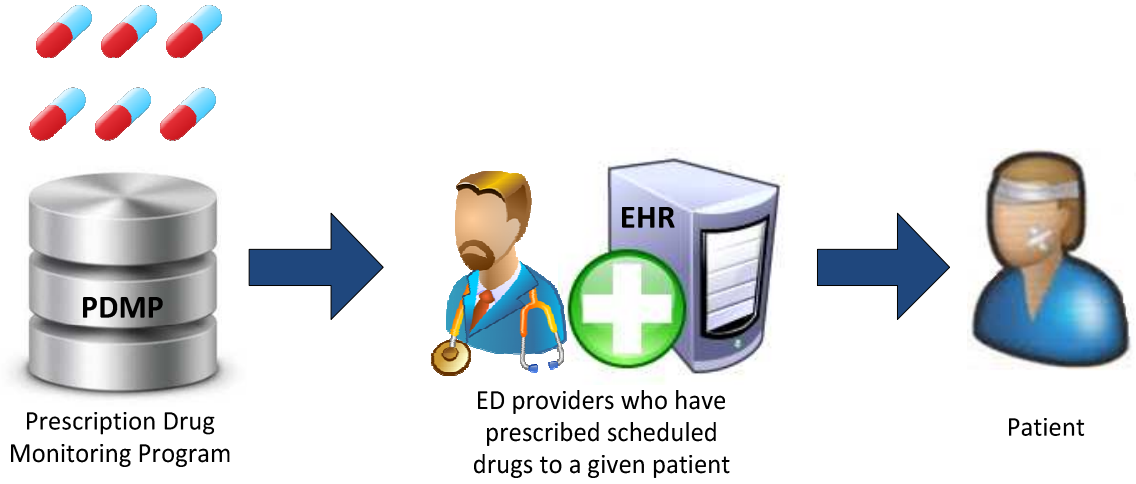


Figure 20. Emergency Department A Pilot Overview

A.1.5 Emergency Department Pilot Study B

ED EHR, Admission, Discharge and Transfer (ADT) Message, PDMP/Solicited Report

The patient checks in to the ED and an ADT message is created. The ADT triggers a query to the PDMP, which returns a patient-at-risk / scheduled drug history to ED EHR. Figure 21 illustrates this pilot overview. In addition to the common recommendations and products, the pilot also requires those listed in Tables 19 and 20.

Table 19. Additional Recommendations for ED Pilot Study B

Recommendations	Relevant Sections
Full integration of PDMP information in user systems (EHR, pharmacy), with storage and smart sorting/filtering	2.2.2.4 5.2.1.2.1
Users should receive a minimum of six months of a patient's CS history	2.2.1.4
Enablers of workflow integration (SSO, links)	2.2.2.3
At-risk filter and alerting options, for both solicited and unsolicited usage	2.2.2.5 2.2.3.1 4.2.8
Prescribers, dispensers, and other healthcare professionals should have PDMP access and the ability to appoint delegates	5.2.1.1.1-2

Table 20. Additional Products for ED Pilot Study B

Products	Relevant Sections
Template for Interface Parameters Supported by PDMP by Report	D1 (4.2.2)

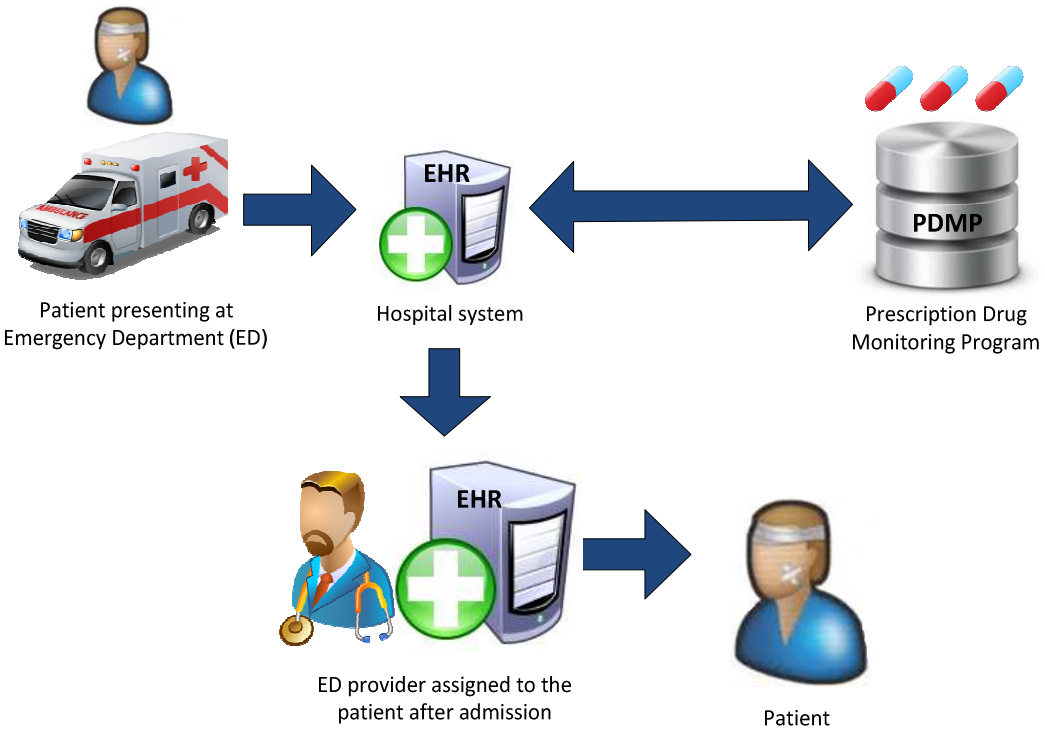


Figure 21. Emergency Department B Pilot Overview

A.1.6 Emergency Department Pilot Study C

ED EHR, Admission, Discharge and Transfer (ADT) Message, HIE, PDMP/Solicited Report

The patient checks in to the ED and an ADT message is created. The ADT triggers a query to the PDMP via the HIE. PDMP returns patient-at-risk / scheduled drug history to ED EHR via the HIE. Figure 22 illustrates this pilot overview. In addition to the common recommendations and products, the pilot also requires those listed in Tables 21 and 22.

Table 21. Additional Recommendations for ED Pilot Study C

Recommendations	Relevant Sections
Full integration of PDMP information in user systems (EHR, pharmacy), with storage and smart sorting/filtering	2.2.2.4 5.2.1.2.1
Users should receive a minimum of six months of a patient's CS history	2.2.1.4
Enablers of workflow integration (SSO, links)	2.2.2.3
At-risk filter and alerting options, for both solicited and unsolicited usage	2.2.2.5 2.2.3.1 4.2.8
Sharing of PDMP data through third-party intermediaries must comply with state and federal laws and regulations, as well as applicable legally binding agreements (e.g., MOUs)	5.2.2.1.1 5.2.2.1.3 5.2.2.2.1

Recommendations	Relevant Sections
For intermediary-enabled sharing, entities should utilize the proposed agreement framework to minimize risk	6.2.1
Prescribers, dispensers, and other healthcare professionals should have PDMP access and the ability to appoint delegates	5.2.1.1.1-2

Table 22. Additional Products for ED Pilot Study C

Products	Relevant Sections
Template for Interface Parameters Supported by PDMP by Report	D1 (4.2.2)
Master Business Agreement	6.2.2.1
Exemplar BAA	6.2.2.2
State Boilerplate Language Example	6.2.2.3

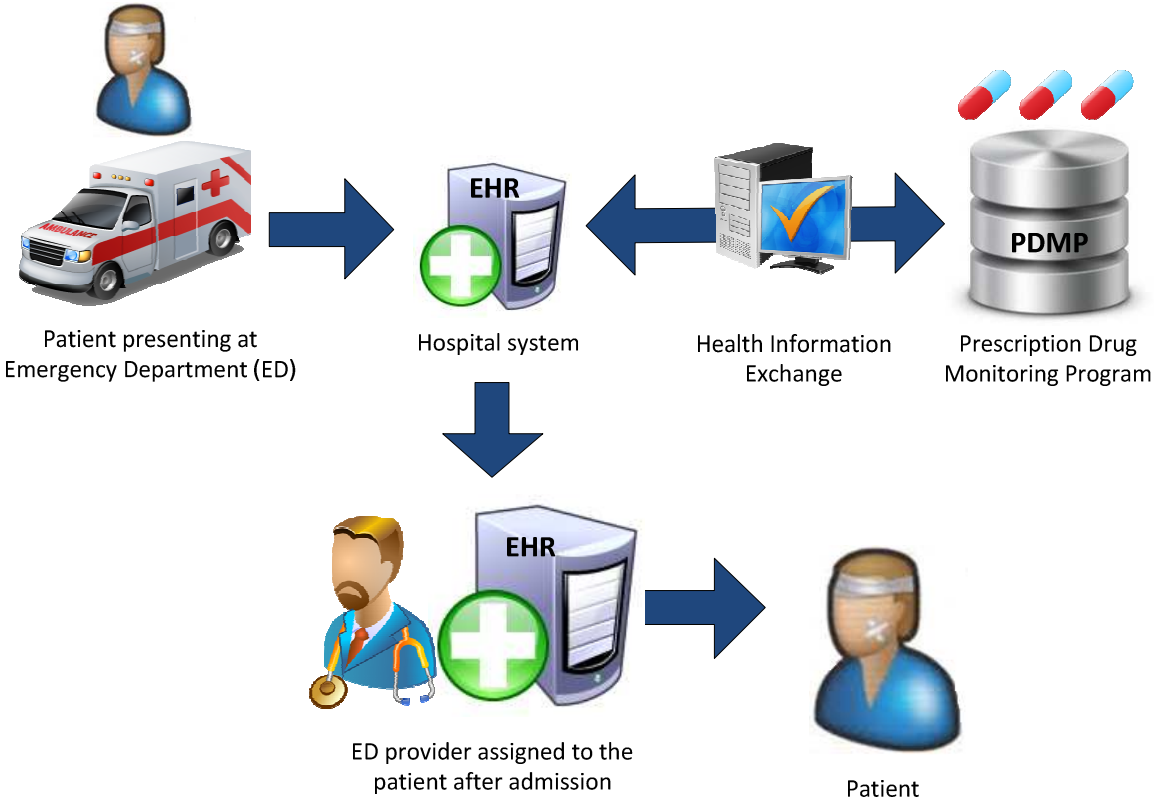


Figure 22. Emergency Department C Pilot Overview

A.1.7 Emergency Department Pilot Study D

ED Manual Query Terminal, HIE, PDMP/Solicited Report

Patient is assigned to a provider. Provider accesses existing manual query terminal to access the patient care summary from the HIE. The patient care summary query triggers a PDMP query by the HIE to the PDMP. PDMP returns a patient-at-risk / scheduled drug history through the HIE to the ED manual query terminal. Figure 23 illustrates this pilot overview. In addition to the common recommendations and products, the pilot also requires those listed in Tables 23 and 24.

Table 23. Additional Recommendations for ED Pilot Study D

Recommendations	Relevant Sections
Full integration of PDMP information in user systems (EHR, pharmacy), with storage and smart sorting/filtering	2.2.2.4 5.2.1.2.1
Users should receive a minimum of six months of a patient's CS history	2.2.1.4
Enablers of workflow integration (SSO, links)	2.2.2.3
At-risk filter and alerting options, for both solicited and unsolicited usage	2.2.2.5 2.2.3.1 4.2.8
Sharing of PDMP data through third-party intermediaries must comply with state and federal laws and regulations, as well as applicable legally binding agreements (e.g., MOUs)	5.2.2.1.1 5.2.2.1.3 5.2.2.2.1
For intermediary-enabled sharing, entities should utilize the proposed agreement framework to minimize risk	6.2.1

Table 24. Additional Products for ED Pilot Study D

Products	Relevant Sections
Master Business Agreement	6.2.2.1
Exemplar BAA	6.2.2.2
State Boilerplate Language Example	6.2.2.3

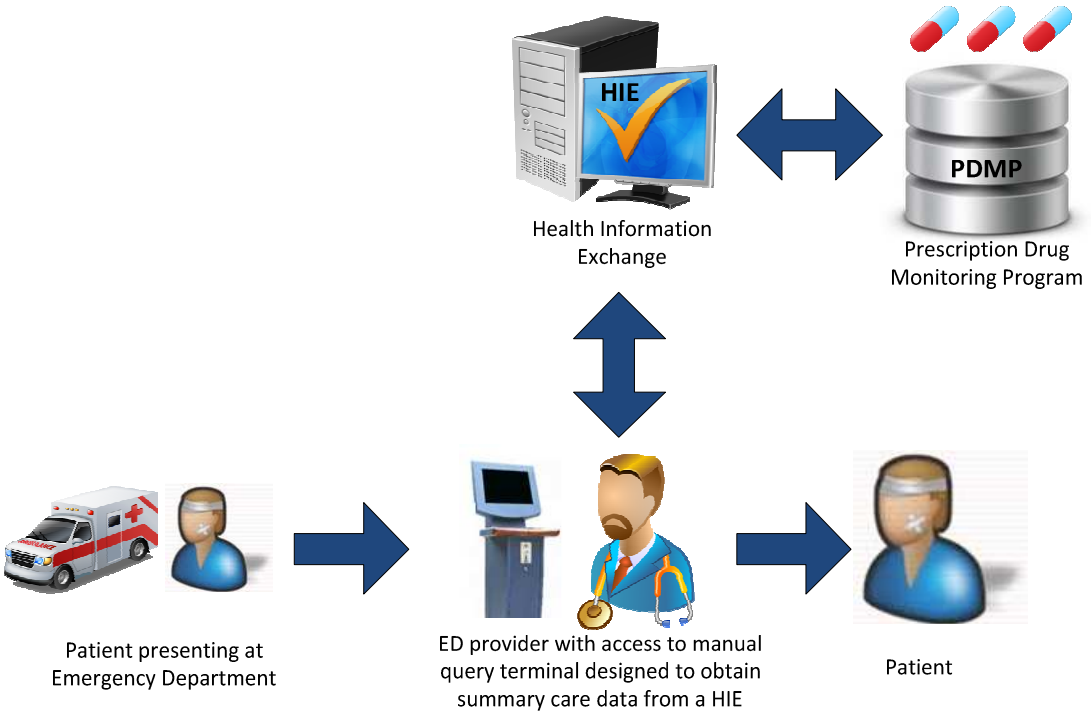


Figure 23. Emergency Department D Pilot Overview

A.1.8 Pharmacy Pilot Study A

PDMP, Direct, Pharmacy System / Unsolicited Report

PDMP system identifies patients at risk and sends a message via Direct to all pharmacists who have previously dispensed to the patient (patients at risk – minimal patient information) with link back to PDMP (pharmacies can query PDMP for full information). Alternatively, the Direct message may contain more detailed information. Note that the cutoff for patients at risk varies by state. Integration of the message with the Pharmacy System is implied. Figure 24 illustrates this pilot overview. This pilot requires only the common recommendations and products in Tables 11 and 12 to succeed.

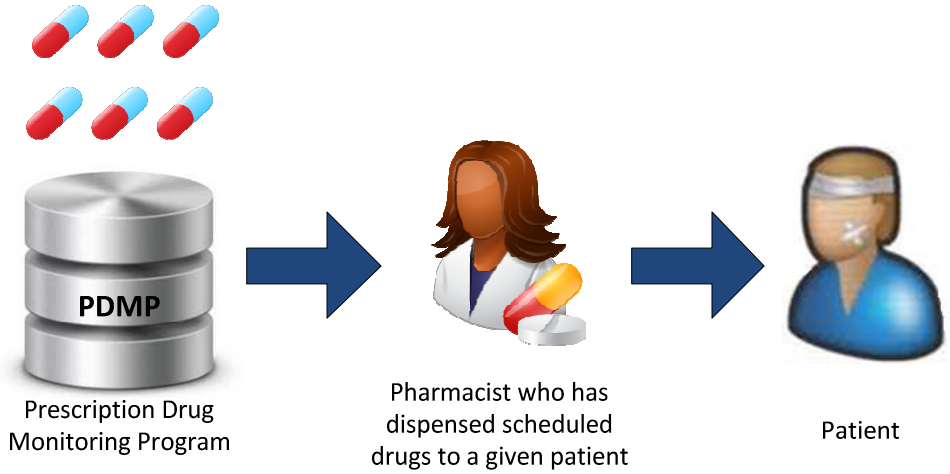


Figure 24. Pharmacy A Pilot Overview

A.1.9 Pharmacy Pilot Study B

Pharmacy system, Switch, PDMP/Solicited Report

A patient drops off the paper prescription at the pharmacy or the controlled substance is electronically prescribed. Prior to dispensing the medication, the pharmacist performs a claims check. Cash prescriptions that do not require a claims check will get labeled with a unique code. The claims check will go through an existing switch. The claims check acts as a trigger to query the PDMP. If there is a match, the PDMP will send the patient's scheduled drug history back through the switch to the pharmacist/pharmacy system. Figure 25 illustrates this pilot overview. In addition to the common recommendations and products, the pilot also requires those listed in Tables 25 and 26.

Table 25. Additional Recommendations for Pharmacy Pilot Study B

Recommendations	Relevant Sections
Full integration of PDMP information in user systems (EHR, pharmacy), with storage and smart sorting/filtering	2.2.2.4 5.2.1.2.1
Users should receive a minimum of six months of a patient's CS history	2.2.1.4
Enablers of workflow integration (SSO, links)	2.2.2.3
At-risk filter and alerting options, for both solicited and unsolicited usage	2.2.2.5 2.2.3.1 4.2.8
Sharing of PDMP data through third-party intermediaries must comply with state and federal laws and regulations, as well as applicable legally binding agreements (e.g., MOUs)	5.2.2.1.1 5.2.2.1.3 5.2.2.2.1
For intermediary-enabled sharing, entities should utilize the proposed agreement framework to minimize risk	6.2.1
Prescribers, dispensers, and other healthcare professionals should have PDMP access and the ability to appoint delegates	5.2.1.1.1-2

Recommendations	Relevant Sections
Co-transmission of queries to PDMPs is deemed technically and operationally inadvisable	4.2.7
An appropriate framework for message security should be applied to ensure compliance with HIPAA and state privacy laws	4.2.5

Table 26. Additional Products for Pharmacy Pilot Study B

Products	Relevant Sections
Template for Interface Parameters Supported by PDMP by Report	D1 (4.2.2)
Master Business Agreement	6.2.2.1
Exemplar BAA	6.2.2.2
State Boilerplate Language Example	6.2.2.3

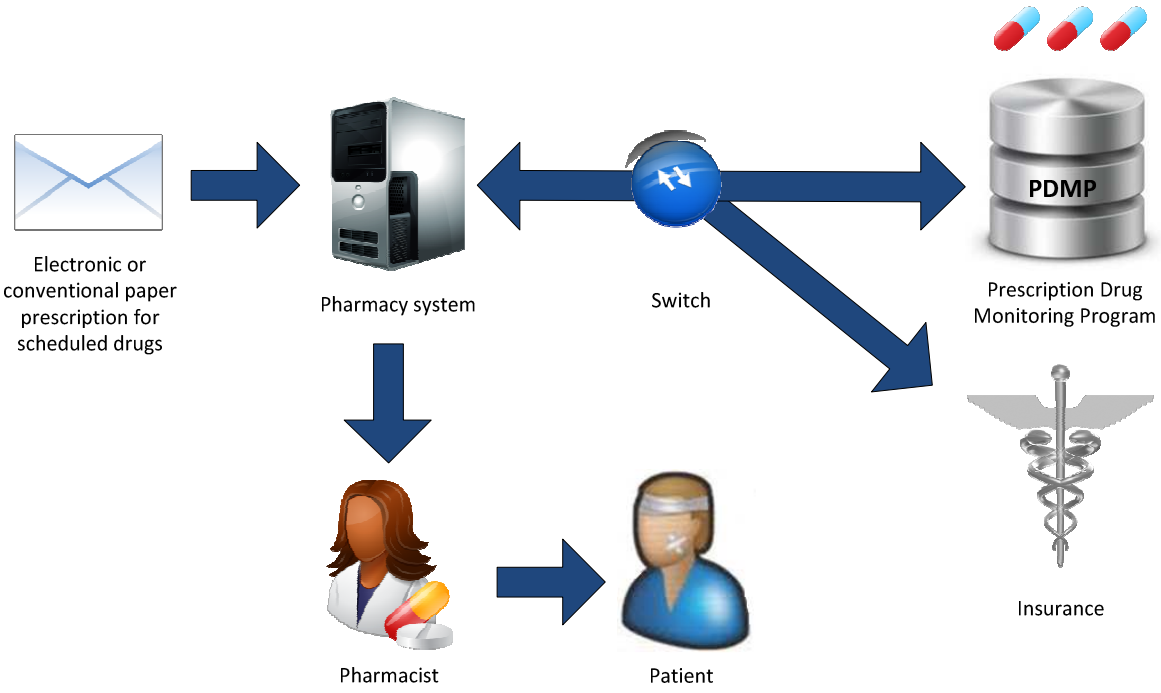


Figure 25. Pharmacy B Pilot Overview

Appendix B Work Group Participant List

The following table lists the participants of each Work Group. Each section is alphabetized except for the Work Group chair, whose name appears in bold at the top of the list.

Last Name	First Name	Affiliation
Data Content and Vocabulary		
Lockwood	**William**	**The American Society for Automation in Pharmacy**
Baumgartner	Chris	Alliance of States w/ PMPs
Bizzaro	Tom	First DataBank
Casar	Joe	KY PMP (KASPER)
Choi	Mera	ONC
Daniel	James	ONC
Darbouze	Farrah	ONC
Degbo	Adjoa	ESAC for ONC/OSI
Dharia	Apurva	ESAC for ONC/OSI
Jenkins	Danielle	Appriss
Ladwa	Sweta	ESAC for ONC/OSI
Lockwood	Bill	The American Society for Automation in Pharmacy
MacDonald	Jason	OARRS (Ohio PMP)
Manglani	Rajesh	Surescripts
Morgan	Drew	CMS
Parker	Jamie	ESAC for ONC/OSI
Powers	Chris	CMS
Sommerville	Robbie	HID
Spiro	Shelly	Pharmacy e-HIT Collaborative
Spitznas	Cecelia	ONDCP
Theberge	Henry	Global Sage Group (MA)
Traver	Chris	DOJ
Vocci	Frank	Friends Research Institute
Information Usability and Presentation		
Orr	**Ralph**	**VA PMP**
Choi	Mera	ONC
Darbouze	Farrah	ONC
Degbo	Adjoa	ESAC for ONC/OSI
Dharia	Apurva	ESAC for ONC/OSI
Dhavle	Ajit	Surescripts
Droz	Danna	OARRS (Ohio PMP)

Last Name	First Name	Affiliation
Espy	Steve	HID
Fiellin	David	Yale University School of Medicine
George	Tomson	Walgreens
Knue	Patrick	PMP Center of Excellence
Ladwa	Sweta	ESAC for ONC/OSI
Lee	Jinhee	SAMHSA
Ondra	Steve	OSTP
Parker	Jamie	ESAC for ONC/OSI
Patterson	Vickie	QS/1
Podgurski	Mike	Rite Aid
Reuter	Nick	SAMHSA
Rogers	Clay	Appriss
Slotnick	Jeff	OK Bureau of Narcotics and Dangerous Drugs Control
Spiro	Shelly	Pharmacy e-HIT Collaborative
Spitznas	Cecelia	ONDCP
Terman	Gregory	American Pain Society / Washington State
Vogt	Don	OK PDMP
Wilson	Kristin	QHN (Colorado HIE)
Transport and Architecture		
Garner	**Chad**	**OARRS (Ohio PMP)**
Basham	Chad	Maryland Alcohol and Drug Abuse Administration
Bolin	Josh	NABP
Chan	Bill	MD HIE
Choi	Mera	ONC
Cowan	Robert	NABP
Daniel	James	ONC
Darbouze	Farrah	ONC
Davis	Timothy	NCPA
Dharia	Apurva	ESAC for ONC/OSI
George	Tomson	Walgreens
Heath	Jason	Apriss
Jones	Chris	CDC
Keith	Rusty	Surescripts
Ladwa	Sweta	ESAC for ONC/OSI
Lockwood	Bill	The American Society for Automation in Pharmacy
Majkowski	Ken	Surescripts
McCullough	Sheila	HID (PMP provider)
Mullenix	Stephen	NCPDP

Last Name	First Name	Affiliation
Newman	Mike	TN
Parker	Jamie	ESAC for ONC/OSI
Pinsonneault	Roger	RelayHealth
Powers	Chris	CMS
Rancourt	John	ONC
Reuter	Nick	SAMHSA
Rice	Will	TN Office of e-Health Initiatives
Serich	Scott	IJIS
Sharp	David	MD HIE
Shoup	Rick	MeHI
Slaski	Bob	Open Networks
Slotnick	Jeff	OK Bureau of Narcotics and Dangerous Drugs Control
Spitznas	Cecelia	ONDCP
Szarvas-Kidd	Danica	DOJ
Willard	Ketih	Surescripts
Law and Policy		
Giglio	**Jim**	**Alliance of States w/ PMPs**
Banks	Peter	ONC
Bolin	Josh	NABP
Daniel	James	ONC
Davis	Timothy	NCPA
Dharia	Apurva	ESAC for ONC/OSI
Eadie	John	Brandeis Center of Excellence
Fan	Jennifer	SAMHSA
Fisher	Nancy	CMS
Green	Sherry	NAMSDL
Harkness	Eric	TN
Hatfield	Ron	Appriss
Jones	Chris	CDC
Kloth	David	ASIPP
LaBelle	Regina	ONDCP
Ladwa	Sweta	ESAC for ONC/OSI
Lee	Jinhee	SAMHSA
Martello	Kendra	PhRMA
Morris	Christina	KS State Board of Pharmacy
Nehme	Donna	MeHI
Orr	Ralph	VA PMP
Parker	Jamie	ESAC for ONC/OSI

Last Name	First Name	Affiliation
Parsons	Amanda	NY Department of Health and Mental Hygiene
Poston	Rebecca	FL PDMP
Reuter	Nick	SAMHSA
Robin	Lisa	Federation of State Medical Boards
Russell	Scotti	NABP
Sharp	David	MD HIE
Spiro	Shelly	Pharmacy e-HIT Collaborative
Szarvas-Kidd	Danica	DOJ
Terman	Gregory	American Pain Society / Washington State
Tipping	Kate	ONC
Twillman	Bob	American Academy of Pain Management
Uhrig	Paul	SureScripts
Wirth	Gary	CMS
Business Agreements for Intermediaries		
Guice	**Lee**	**KY PMP (KASPER)**
Baier	Michael	MD Department of Health and Mental Hygiene
Bizzaro	Tom	First DataBank
Daniel	James	ONC
Dharia	Apurva	ESAC for ONC/OSI
Fan	Jennifer	SAMHSA
Ladwa	Sweta	ESAC for ONC/OSI
LeCraw	Linda	Surescripts
Lee	Jinhee	SAMHSA
Morris	Christina	KS State Board of Pharmacy
Parker	Jamie	ESAC for ONC/OSI
Smith	April	KY HIE
Sohl	Henry	Appriss
Thompson	Dick	QHN (Colorado HIE)
Wickizer	Phil	INSPECT / Indiana
Xavier	Frank	Optimum Technology, Inc

Appendix C PDMP Data

C.1 PDMP Data Elements

The following table organizes the PDMP Data Elements into a higher-level structure that is meaningful for users. For example, a patient has a name that is decomposed into separate data elements for the first and last names. Organizing and identifying data elements enables the development of a data element exchange standard for requesting and receiving data from PDMP systems. The data elements also facilitate development of a cross-reference among the data elements in the various specifications for PDMP-related data.

	Data Elements	Definition	Synonyms
Patient		**Reports the patient's name and basic information as contained in the pharmacy record**	
Name (first and last)			
	First Name	First name of patient	Given name
	Last Name	Last name of patient	Family name, surname
Address (including ZIP code)			
	1. Address Information – 1 [Required] 2. Address Information – 2 [Situational]	1. Address information 2. Additional address information	
	City Address	City name	
	State Address	U.S. Postal Service state code	
	ZIP Code Address	U.S. Postal Service ZIP code	ZIP, postal code
	Country	Country of residency	
DOB	Date of Birth	Date patient was born	Date of birth, birthday, DOB, birth date
Identifier		Patient identifier	
	Identification Qualifier of Patient Identifier	Code identifying the jurisdiction that issues identifier	
	Identification Qualifier	Code to identify the type of ID	
	Identification of Patient	Identification number for the patient (e.g., driver's license number)	
Gender (situational)	Gender Code	Code indicating the sex of the patient	Gender, sex, sex code
Species (situational)	Species Code	Differentiates a prescription for an individual from one prescribed for an animal	
Phone number (Situational)	Phone Number	Complete phone number, including area code	Phone, contact number

	Data Elements	Definition	Synonyms
Prescriber		**Identifies the prescriber of the prescription**	
Name (first and last, suffix)			
	First Name	Prescriber's first name	Given name
	Last Name	Prescriber's last name	Family name, surname
	Generational Suffix		
Specialty (situational)	Specialty	Type of medicine practiced	
Address (including ZIP code)			
	1. Address Information – 1 [Required] 2. Address Information – 2 [Situational]	1. Address information 2. Additional address information	
	City Address	City name	
	State Address	U.S. Postal Service state code	
	ZIP Code Address	U.S. Postal Service ZIP code	ZIP, postal code
Phone number (situational)	Phone Number	The prescriber's primary phone number	Phone, contact number
Prescriber DEA number (situational)	DEA Number	Identifying number assigned to a prescriber or an institution by the DEA	
Dispenser		**To identify the pharmacy or the dispensing prescriber.**	
Name of Dispenser	Pharmacy or Dispensing Prescriber Name	Freeform name of the pharmacy or dispensing prescriber. If dispensing prescriber, include professional degree—e.g., MD.	Pharmacy, Dispenser
Address			
	1. Address Information – 1 [required] 2. Address Information – 2 [situational]	1. Address information 2. Additional address information	
	City Address	City name	
	State Address	U.S. Postal Service state code	
	ZIP Code Address	U.S. Postal service ZIP code	ZIP, postal code
Phone	Phone Number	Full telephone number	Phone, contact number
Identification		Dispenser Identification	
	DEA Number	Identifier assigned to the pharmacy by the DEA	
	NCPDP/NABP Provider ID	Identifier assigned to pharmacy by the NCPDP	
	National Provider Identifier (NPI)	Identifier assigned to the pharmacy by CMS	

	Data Elements	Definition	Synonyms
Prescription		**Identifies the basic components of a dispensing of a given prescription order, including the date and quantity**	
NDC Number	NDC Code	The National Drug Code (NDC) number is a unique product identifier used in the United States.	
Name of Drug	Name of Drug	Derived from product ID, such as NDC. It will be the generic ingredients as opposed to the brand name.	
Federal Drug Schedule	Schedule	Federal Drug Schedule for classifying controlled substances (string value II, III, IV, V, NS Not Scheduled). "I" would not be returned because "I" substances are illegal.	Schedules of controlled substances
Compound	Compound	Indicates if a drug is a compound	
Strength	Strength	Derived from product ID, such as NDC	
Form (tablet, capsule, etc.)	Form	Derived from product ID, such as NDC	
Quantity	Quantity Dispensed	Number of metric units dispensed in metric decimal format	
Days' Supply	Days' Supply Dispensed	Calculated or estimated number of days the medication will cover	
Date Filled	Date Prescription Filled	Date prescription was dispensed	
Date Prescribed	Date Written	Date the prescription was written (authorized)	
Refill Status			
	Refills Authorized	Number of refills authorized by the prescriber	
	Refill Number	Number of the fill of the prescription	
Partial Fill	Partial Fill	Prescription was only partially filled	
Prescription Number	Prescription Number	Serial number assigned to the prescription by the pharmacy	
Payment Type	Payment Type	Source of payment for prescription	
Additional Information			
Pharmacist's Name		Pharmacist who filled the prescription	
	First Name	First name or initial	
	Last Name	Last name	
Prescription Serial Number			
	State Issuing Serial Number	State that issued the prescription serial number	
	Prescription Serial Number	State-issued serial number for the prescription	
Dropping Off / Picking Up Qualifier	Dropping Off / Picking Up Qualifier	Indicates whether someone other than the patient is person picking up or dropping off the prescription	

	Data Elements	Definition	Synonyms
Dropping Off / Picking Up Person Name (first and last)		Name of person requesting or receiving the prescription if different than the patient	
	First Name	First name of person	
	Last Name	Last name of person	
Dropping Off / Picking Up Person Relationship to Patient	Relationship	Relationship of the patient to the person dropping off or picking up the prescription	
Dropping Off / Picking Up Person Identifier			
	Issuing Jurisdiction for Dropping Off / Picking Up Person Identifier	Jurisdiction for the person's identification	
	Dropping Off / Picking Up Person Identification	Identification number for the person (e.g., driver's license number)	
Authorized User			
Authentication Information		Information that authenticates the user to use the system and make requests	User credentials
Name (first and last)			
	First Name	Report requestor's first name	Given name
	Last Name	Report requestor's last name	Family name, surname
Role	Role	Function of the person in interactions with a PDMP system	PMIX roles
Case Number	Case Number	Law enforcement case number	Investigation number

C.2 Data Element Exchange Standard

The following table contains the PDMP Data Element Exchange Standard. The National Information Exchange Model (NIEM) and the NIEM Prescription Monitoring Program (PMP) Extension are used for the XML element names and element types.

	Data Elements	XML Element Name	XML Element Type	Defined Values / Rules of Use
Patient			**PatientType uses and extends PersonType**	
Name (first and last)				
	First Name	PersonName PersonGivenName	PersonNameTextType	
	Last Name	PersonName PersonSurName	PersonNameTextType	

	Data Elements	XML Element Name	XML Element Type	Defined Values / Rules of Use
Address (including ZIP code)		PersonPrimaryContactInformation	NIEM-core/2.0 ContactInformationType	
	Street Address (first line)	StructuredAddress LocationStreet	StreetType	
	Street address (second line if needed)	StructuredAddress LocationStreet	StreetType	
	City	StructuredAddress LocationCityName	ProperNameTextType	
	State	StructuredAddress LocationState	USStateCodeType	Type and Values for Canada are also available
	ZIP Code	StructuredAddress LocationPostalCode	Niem-xsd:string	
	Country			
DOB	Patient Date of Birth	PersonBirthDate	DateType	CCYY-MM-DD
Identifier		PersonIdentifier abstract	IdentificationType	Numerous identifiers including driver's license, military IDs, Passport, Social Security Number, Tribal Identifiers, etc.
Gender	Patient Gender	PersonSex	SEXCodeSimpleType	Valid values are: M – Male F – Female U – Undifferentiated
Species	Species	SpeciesCode	SpeciesCodeType	Valid values are: 01 – human 02 – veterinary patient
Phone number	Phone Number	FullTelephoneNumber	FullTelephoneNumberType	
Prescriber			**PrescriberType extends PersonType**	
Name (first and last, suffix)				
	First Name	PersonName PersonGivenName	PersonNameTextType	
	Last Name	PersonName PersonSurName	PersonNameTextType	
	Generational Suffix	PersonName PersonNameSuffixText	TextType	

	Data Elements	XML Element Name	XML Element Type	Defined Values / Rules of Use
Specialty (situational)	Specialty			
Address (including ZIP code)		NIEM-core/2.0 StructuredAddress	NIEM-core/2.0 StructuredAddressType	
	Street Address (first line)	StructuredAddress LocationStreet	StreetType	
	Street Address (second line if needed)	StructuredAddress LocationStreet	StreetType	
	City	StructuredAddress LocationCityName	ProperNameTextType	
	State	StructuredAddress LocationState	USStateCodeType	Type and Values for Canada are also available
	ZIP Code	StructuredAddress LocationPostalCode	Niem-xsd:string	
Phone number	Phone Number	FullTelephoneNumber	FullTelephoneNumberType	
Prescriber DEA number	Prescriber Identifier Number	DEANumberIdentifier	IdentificationType	
Dispenser			**DispenserType extends OrganizationType**	
Name of Dispenser	Name of Dispenser	OrganizationDoingBusinessAsName		
Address			NIEM-core/2.0 StructuredAddress	
	Street Address (first line)	StructuredAddress LocationStreet	StreetType	
	Street Address (second line if needed)	StructuredAddress LocationStreet	StreetType	
	City	StructuredAddress LocationCityName	ProperNameTextType	
	State	StructuredAddress LocationState	USStateCodeType	Type and Values for Canada are also available
	ZIP Code	StructuredAddress LocationPostalCode	Niem-xsd:string	
Phone	Phone Number	FullTelephoneNumber	FullTelephoneNumberType	
Identification	Dispenser Identification Number	DEANumberIdentifier	IdentificationType	

	Data Elements	XML Element Name	XML Element Type	Defined Values / Rules of Use
Prescription			**PrescriptionType**	
NDC Number	NDC Number	DrugNDCProductIdentifier DrugProductIdentifier	IdentificationType	
Name of Drug	Name of Drug	DrugProductNameText	TextType	
Federal Drug Schedule	Schedule	DEAClassScheduleText	TextType	Valid Values (2-5, blank) 2 – Schedule II Narcotic 3 – Schedule III Narcotic 4 – Schedule IV substance 5 – Schedule V substance Blank – not specified
Compound	Compound	DrugCPDProductIdentifier	IdentificationType	
Strength	Strength	DrugStrengthText	TextType	
Form (tablet, capsule, etc.)	Form	DrugDosageUnitsCode	DrugDosageUnitsCodeType	Valid values: 01 package 02 milliliters 03 grams
Quantity	Quantity Dispensed	DispensedQuantity	Decimal	
Days' Supply	Days' Supply Dispensed	DaysSupplyCount	Non-negative integers	
Date Filled	Date Prescription Filled	PrescriptionFilledDate	DateType	CCYY-MM-DD
Date Prescribed	Date Prescribed by the Prescriber	PrescriptionWrittenDate	DateType	CCYY-MM-DD
Refill Status				
	Number of Refills Ordered	RefillsAuthorizedCount	Non-negative integers	
	Refill Number	DrugRefillNumberCount	Non-negative integers	
Partial Fill	Partial Fill	PartialFillIndicator	Boolean	
Prescription Number	Prescription Number	PrescriptionNumberText	TextType	
Payment Type		MethodOfPaymentCode	MethodOfPaymentCodeType	

	Data Elements	XML Element Name	XML Element Type	Defined Values / Rules of Use
Additional Information				
Pharmacist's Name			PharmacistType extends PersonType	
	First Name	PersonName PersonGivenName	PersonNameTextType	
	Last Name	PersonName PersonSurName	PersonNameTextType	
Prescription Serial Number				
	State Issuing Serial Number	StateIssuedRxSerialNumberIdentifier	IdentificationType has IdentificationID	Valid values are two-letter state codes
	Prescription Serial Number	StateIssuedRxSerialNumberIdentifier	IdentificationType has IdentificationJurisdiction	String
Dropping Off / Picking Up Qualifier	Dropping Off / Picking Up Qualifier (if used)			Assumed Picking Up is default
Dropping Off / Picking Up Person Name			PersonIdentifier has PersonName	
	First Name	PersonName PersonGivenName	PersonPickingUpRx has PersonIdentifier	
	Last Name	PersonName PersonSurName	PersonNameTextType	
Dropping Off / Picking Up Person Relationship to Patient	Relationship	PersonPickingUpRx has RelationshipToPatientCode	RelationshipToPatientCode Type	Valid Values 01 Patient 02 Parent/ Legal Guardian 03 Spouse 04 Caregiver 99 Other
Dropping Off / Picking Up Person Identifier			PersonPickingUpRx has PersonIdentifier	
	Issuing Jurisdiction for Dropping Off / Picking Up Person Identifier	PersonIdentifier abstract	IdentificationType has IdentificationJurisdiction	
	Dropping Off / Picking Up Person Identification	PersonIdentifier abstract	IdentificationType has IdentificationID	Numerous identifiers, including driver's license, military IDs, Passport, Social Security Number, Tribal Identifiers, etc.

	Data Elements	XML Element Name	XML Element Type	Defined Values / Rules of Use
Authorized User				
Authentication Information				
Name (first and last)			PersonType	
	First Name	PersonName PersonGivenName	PersonNameTextType	
	Last Name	PersonName PersonSurName	PersonNameTextType	
Role	Role			PMIX has a set of defined role values
Case Number	Case Number			

C.3 Cross-Reference Guide

The Vocabulary Work Group developed a cross-reference between the PDMP Data Elements and the corresponding data elements in related specifications to ensure the completeness and feasibility of the recommended Data Exchange Standard. This Cross-Reference Guide covers ASAP, Healthcare Information Technology Standards Panel (HITSP) C32 Continuity of Care Component, and the NIEM-based information exchange specification used by the Prescription Monitoring Information Exchange (PMIX) and the Prescription Monitoring Program interconnect (PMPi). The members recommended that this Cross-Reference Guide be made available to system implementers that must exchange data among systems that use different data element representations. This will ensure a consistent, accurate, and unambiguous exchange of PDMP information.

The following table contains the cross-reference between the PDMP Data Elements and related specifications containing prescription data. Entries in the table provide the data elements from the specification that correspond to the PDMP Data Element. This mapping of the PDMP Data Elements to the related specifications was used to define the data elements needed to create the PDMP Data Exchange Standard. This table uses red shading and the phrase “Not Specified” to indicate that a particular PDMP Data Element is not defined in the specification.

	ASAP 4.2	HL 7 CDA R2	NIEM and PMP Extension
Patient	**PAT Segment**	**HITSP v2.01 C83 CDA Content Module for Patients** **/cda:ClinicalDocument/cda:recordTarget/cda:patientRole**	**NIEM plus extension (PMP_NIEM_2.0_Domain_Extension_Schema)** **PatientType uses PersonType and extends it.**

	ASAP 4.2	HL 7 CDA R2	NIEM and PMP Extension
Name (first and last)	PAT07 Last Name AN 50 PAT08 First Name AN 50	cda:patient/cda:name given given family	PersonName PersonNamePrefixText PersonGivenName PersonMiddleName PersonSurName PersonNameSuffixText PersonFullName
Address (including ZIP code)	PAT12 Address Information – 1 AN 35 PAT13 Address Information – 2 AN 35 PAT14 City Address AN 20 PAT15 State Address AN 10 PAT16 ZIP Code Address AN 9 PAT22 Country of non-US resident	cda:addr streetAddressLine city state postalCode country	StructuredAddress LocationStreet StreetFullText LocationCityName LocationStateUSPostalServiceCode LocationPostalCode LocationPostalExtensionCode Also has CanadianProvinceCodes
DOB	PAT18 Date of Birth DT 8 Format: CCYYMMDD	cda:patient/cda:birthtime CCYYMMDD	PersonBirthDate CCYY-MM-DD
Identifier (patient reference number)	PAT01 ID Qualifier of Patient Identifier AN 2 See Appendix A for list of jurisdictions. PAT02 ID Qualifier N 2 Code to identify the type of ID in PAT03. If PAT02 is used, PAT03 is required. 01 Military ID 02 State Issued ID 03 Unique System ID 04 Permanent Resident Card (Green Card) 05 Passport ID 06 Driver's License ID 07 Social Security Number 08 Tribal ID 99 Other (Trading partner agreed upon ID, such as cardholder ID.) PAT03 ID of Patient AN 20 Identification number for the patient as indicated in PAT02. An example would be the driver's license number.	cda:id id extension root	PersonIdentifier abstract PersonDriverLicenseIdentifier, PersonMilitaryIdentifier, PersonOtherIdentifier, PersonPassportIdentifier, PersonSocialSecurityNumberIdentifier, PersonStateIssuedIdentifer, PersonTribalIdentifier or PersonUniqueSystemIdentifier

	ASAP 4.2	HL 7 CDA R2	NIEM and PMP Extension
Gender (situational)	PAT19 Gender Code AN 1 F Female M Male U Unknown	cda:patient/ cda:administrativeGender Code/@code F Female M Male U Undifferentiated	SEXCodeSimpleType F, M, U
Species (situational)	PAT20 Species Code N 2 01 Human 02 Veterinary Patient	Not Specified	PatientType has SpeciesCode 01 Human 02 Veterinary Patient
Phone number (situational)	PAT17 Phone Number AN 10	cda:telecom (555)555-1212	FullTelephoneNumber string
Prescriber	**PRE Segment**	**HITSP v2.01 C83 CDA Content Module for Healthcare Providers /cda:ClinicalDocument/cda:documentationOf/ cda:serviceEvent/cda:performer**	**PrescriberType extends PersonType**
Name (first and last)	PRE05 Last Name AN 50 PRE06 First Name AN 50	cda:assignedEntity/cda:assignedPerson/cda:name	PersonName PersonNamePrefixText PersonGivenName PersonMiddleName PersonNameSuffixText PersonFullName
Generational Suffix (situational)	Not Specified	cda name <suffix> qualifier	PersonName PersonNameSuffixText
Specialty (situational)	Not Specified	Not Specified	Not Specified
Address (including ZIP code)	Can be derived from the DEA Number	cda:assignedEntity /cda:addr	StructuredAddress LocationStreet StreetFullText LocationCityName LocationStateUSPostalServiceCode LocationPostalCode LocationPostalExtensionCode
Phone number (Situational)	PRE08 Phone Number N 10	cda:assignedEntity /cda:telecom	FullTelephoneNumber string
Prescriber DEA number (Situational)	PRE02 DEA Number AN 9 PRE03 DEA Number Suffix AN 7	cda:assignedEntity /cda:id National Provider ID	DEANumberIdentifier

	ASAP 4.2	HL 7 CDA R2	NIEM and PMP Extension
Dispenser	**PHA segment**	**HITSP v2.01 C83 CDA Content Module for Medication - Prescription** **cda:substanceAdministration**	**DispenserType extends OrganizationType**
Name of Pharmacy	PHA04 or Dispensing Prescriber Name AN 60	cda:entryRelationship/ cda:supply[@moodCode='EVN'] / cda:performer / cda:assignedEntity	OrganizationDoingBusinessAsName
Pharmacist's Name (first and last)	PHA11 Contact Name		ContactNameText
Address	PHA05 Address Information – 1 AN 30 PHA06 Address Information – 2 AN 25 PHA07 City Address AN 20 PHA08 State Address AN 2 PHA09 ZIP Code Address AN 9	cda:entryRelationship/ cda:supply[@moodCode='EVN'] / cda:performer/cda:assignedEntity/cda:addr	OrganizationLocation
Phone	PHA10 Phone Number AN 10	Not Specified	OrganizationPrimaryContactInformation
Identification	PHA03 DEA Number AN 9 PHA02 NCPDP/NABP Provider ID AN 7 PHA01 National Provider Identifier (NPI) AN 10	Not Specified	DEANumberIdentifier
Prescription	**DSP Segment**	**HITSP v2.01 C83 CDA Content Module for Medication – Prescription and Non-Prescription** **cda:substanceAdministration**	**PrescriptionType**
NDC Number	Can be derived from lookup tables using name of drug	Can be derived from lookup tables	Can be derived from NCPDPIdentifier in PrescriptionDrugType
Name of Drug	DSP07 Product ID Qualifier (Required) N 2 DSP08 Product ID (Required) AN 15	cda:consumable/cda:manufacturedProduct / cda:manufacturedMaterial/ cda:code/@code	DrugProductIdentifier DrugDINProductIdentifier, DrugHRIProductIdentifier, DrugNDCProductIdentifier, DrupUPCProductIdentifier or DrugUPNProductIdentifier
Federal Drug Schedule	Can be derived from lookup tables	Can be derived from lookup tables	Can be derived from DEAClassScheduleText in PrescriptionDrugType.

	ASAP 4.2	HL 7 CDA R2	NIEM and PMP Extension
Compound	DSP 07 Product ID Qualifier has value 06 for compounds.	Probably derivable from cda:manufacturedProduct	DrugCPDProductIdentifier
Strength	Can be derived from a combination of DSP09 Quantity Dispensed and DSP11 Drug Dosage Units Code	When the coded product or brand name describes the strength or concentration of the medication, and the dosing is in administration units (e.g., 1 tablet, 2 capsules), units SHOULD contain the preferred name of the presentation units within braces { } using the units of presentation from the NCI Thesaurus.	DrugStrengthText - string
Form (tablet, capsule, etc.)	Can be obtained from NDC Product codes, if transmitted	cda:doseQuantity units attribute has value from http://www.fda.gov/ForIndustry/DataStandards/StructuredProductLabeling/ucm162049.htm	Can be obtained from NDC Product codes
Quantity	DSP09 Quantity Dispensed DSP 11 in metric units	cda:doseQuantity	DispensedQuantity – decimal; DrugDosageUnitsCode is unit of measure for DispensedQuantity – 01 package 02 milliliters 03 grams
Days' Supply	DSP10 Days Supply N 3	Not Specified	DaysSupplyCount non-negative integer
Date Filled	DSP05 Date Filled DT 8	cda:entryRelationship/ cda:act/cda:supply[@moodCode='EVN'] / cda:effectiveTime	PrescriptionFilledDate CCYY-MM-DD
Date Prescribed	DSP03 Date Written DT 8 CCYYMMDD	cda:entryRelationship[@typeCode='REFR']/ cda:supply[moodCode='INT']/cda:author/cda:time	PrescriptionWrittenDate CCYY-MM-DD
Refill Status	DSP04 Refills Authorized N 2 DSP05 Refill Number N 2	cda:entryRelationship[@typeCode='COMP'] / cda:sequenceNumber is fill number cda:repeatNumber	DrugRefillNumberCount RefillsAuthorizedCount Non-negative integers
Partial Fill	DSP06 Partial Fill Indicator N 2	Not Specified	PartialFillIndicator Non-negative integers
Prescription Number	DSP02 Prescription Number AN 25	cda:supply[@moodCode='EVN']/cda:effectiveTime	PrescriptionNumberText PrescriptionElectronicReferenceNumberText
Payment Type	DSP16 Classification Code for Payment Type N 2		MethodOfPaymentCode

	ASAP 4.2	HL 7 CDA R2	NIEM and PMP Extension
Additional Information			
Pharmacist Name	AIR09 Last name AIR10 First name	Not Specified	PharmacistType uses PersonType and extends it. Person Type has PersonName.
Prescription Serial Number and State Issuing Prescription Serial Number	AIR01 State Issuing Rx Serial Number AN 2 AIR02 State Issued Rx Serial Number AN 20	Not Specified	StateIssuedRxSerialNumberIdentifier includes the identifier (serial number) and the jurisdiction
Dropping Off / Picking Up Qualifier	AIR03 Issuing Jurisdiction AN 2	Not Specified	PersonPickingUpRxType uses PersonType and extends it.
Dropping Off / Picking Up Person Name (first and last)	AIR 05 ID of Person Dropping Off or Picking Up Rx	Not Specified	Person Type has PersonName.
Dropping Off / Picking Up Person Relationship to Patient	AIR 08 First Name and AIR07 Last Name of Person Dropping Off or Picking Up Rx	Not Specified	PersonPickingUpRx has RelationshipToPatientCode.
Dropping Off / Picking Up Person Identifier	AIR 05 ID of Person Dropping Off or Picking Up Rx	Not Specified	PersonPickingUpRx has PersonIdentifier.
Authorized User			
Authentication information	Not Specified	Not Specified	Not Specified
Name (first and last)	Not Specified	Not Specified	PersonName PersonNamePrefixText PersonGivenName PersonMiddleName PersonSurName PersonNameSuffixText PersonFullName
Role	Not Specified	Not Specified	Not Specified
Case Number	Not Specified	Not Specified	Not Specified

C.4 Data Element Usage

The PDMP Report Data Element Usage table uses the following nomenclature:

An “X” indicates that the data elements are included in the report, if available.

A dash (“–”) indicates that the data elements are not included in the report.

All data will be provided if available under the prevailing conditions. Not all PDMP systems contain all of the data or can report all of the data. Therefore, this table was built with the assumption that data will be reported if it is available under the prevailing conditions, which will

depend on state specifications for implementing PDMP reporting as well as legal and legislative considerations that will vary by state.

The following table defines the information recommended for PDMP reports for patients, prescribers, and dispensers.

	Patient Report	Prescriber Self-Check Report	Prescriber Report	Dispenser Self-Check Report	Dispenser Report
Patient					
Name (first and last)	X	X	X	X	X
Address (including ZIP code)	X	X	X	X	X
DOB	X	X	X	X	X
Identifier	X	X	X	X	X
Gender	X	X	X	X	X
Species	X	X	X	X	X
Phone Number	X	X	X	X	X
Prescriber					
Name (first and last, suffix)	X	X	X	–	X
Specialty	X	X	X	–	X
Address (including ZIP code)	X	–	X	–	X
Phone Number	X	–	X	–	X
Prescriber DEA Number	X	X	X	–	X
Dispenser					
Name of Dispenser	X	X	X	–	X
Pharmacist's Name (first and last)	X	X	X	–	X
Address	X	X	X	–	X
Phone	X	X	X	–	X
Identification	X	X	X	–	X
Prescription					
NDC Number	X	X	X	X	X
Name of Drug	X	X	X	X	X
Federal Drug Schedule	X	X	X	X	X
Compound	X	X	X	X	X
Strength	X	X	X	X	X
Form (tablet, capsule, etc.)	X	X	X	X	X
Quantity	X	X	X	X	X
Days' Supply	X	X	X	X	X
Date Filled	X	X	X	X	X
Date Prescribed	X	X	X	X	X
Refill Status	X	X	X	X	X

	Patient Report	Prescriber Self-Check Report	Prescriber Report	Dispenser Self-Check Report	Dispenser Report
Partial Fill	X	X	X	X	X
Prescription Number	X	X	X	X	X
Payment Type	X	X	X	X	X
Additional Information (for Prescriptions)					
Pharmacist's Name (first and last)	X	X	X	X	X
Prescription Serial Number and State Issuing Prescription Serial Number	X	X	X	X	X
Dropping Off / Picking Up Qualifier	X	X	X	X	X
Dropping Off / Picking Up Person Name (first and last)	X	X	X	X	X
Dropping Off / Picking Up Person Relationship to Patient	X	X	X	X	X
Dropping Off / Picking Up Person Identifier	X	X	X	X	X
Authorized User (Person Requesting the Report)					
Authentication Information	–	–	–	–	–
Name (first and last)	–	–	–	–	–
Role	–	–	–	–	–
Case Number	–	–	–	–	–

Appendix D Transport and Architecture

D.1 PDMP Interface Parameter Template

The Transport and Architecture Work Group developed the following template to capture information about the Web service or application-level interfaces provided by the PDMP systems. This template defines the parameters needed for each type of report identified in the use cases. Most of the PDMP systems do not have an application programming interface (API) or a service specification that would advertise the interfaces and parameters supported by the interfaces.

In lieu of the availability of APIs for PDMP systems, this template is provided as an example for identifying the interface parameters supported by a PDMP for each type of report.

Use Cases / Report Parameters	Push Unsolicited Patient Report	Pull Prescriber or Dispenser Self Report	Pull Patient Report	Pull Prescriber or Dispenser Report	Push Unsolicited Prescriber or Dispenser Report	Triggered Patient Report without Intermediary	Triggered Patient Report with Intermediary
Requests							
• Identify object of report	Patient	Dispenser or Prescriber	Patient	Prescriber or Dispenser	Prescriber or Dispenser	Patient	Patient
• User authorized to make request							
Report Content Options							
• Time-frame of report							
• Level of report detail (alert, summary, full details)							
• Sort or filter options							
Report Delivery Options							
• Format of report (PDF, text, XML,)							
• Delivery method (email, FTP, eFAX,)							
• Delivery Address (IP, email, etc.)							
• User(s) authorized to receive results							

D.2 Use of Parameters in PDMP Interfaces

The following table shows where the parameters would be defined for solicited and unsolicited reports. Specific parameter values from the PDMP vocabulary are supplied to identify a specific object for the report (patient, prescriber, etc.). Setup Parameter values are defined in advance and apply to all reports produced. Request Parameter values are defined in each report request, and the parameter values apply only to an individual request. As shown by the parameters, three report interfaces are needed: patient, dispenser, and prescriber.

Use Cases / Report Parameters	Push Unsolicited Patient Report	Pull Prescriber or Dispenser Self Report	Pull Patient Report	Pull Prescriber or Dispenser Report	Push Unsolicited Prescriber or Dispenser Report	Triggered Patient Report without Intermediary	Triggered Patient Report with Intermediary
Requests							
• Identify object of report	Patient	Dispenser, Prescriber	Patient	Prescriber, Dispenser	Prescriber, Dispenser	Patient	Patient
• User authorized to make request	Setup	Request	Request	Request	Setup	Request	Request
Report Content Options							
• Time-frame of report	Setup	Request	Request	Request	Setup	Request	Request
• Level of report detail (alert, summary, full details)	Setup	Request	Request	Request	Setup	Request	Request
• Sort or filter options	Setup	Request	Request	Request	Setup	Request	Request
Report Delivery Options							
• Format of report (PDF, text, XML,)	Setup	Request	Request	Request	Setup	Request	Request
• Delivery method (email, FTP, eFAX,)	Setup	Request	Request	Request	Setup	Request	Request
• Delivery Address (IP, email, etc.)	Setup	Request	Request	Request	Setup	Request	Request
• User(s) authorized to receive results	Setup	Request	Request	Request	Setup	Request	Request

D.3 Interface Example for Patient Data Requests

The current Patient Request used for interstate exchanges uses the NIEM PMP extension. This request currently only has two parameters, as shown in the following table. Support for the remaining parameters will need to be added to the interface, and the Work Group recommends this addition.

Use Cases / Report Parameters	Parameter Value	Element for Parameter Value	Element Type
Requests			
• Identify object of report	Patient	PMIX NIEM 2.0 Request Schema RequestPatient	NIEM 2.0 PMP Extension PatientType
• User authorized to make request			
Report Content Options			
• Time-frame of report		PMIX NIEM 2.0 Request Schema RequestPrescriptionDateRange	NIEM 2.0 PMP Extension RequestPrescriptionDateRangeType
• Level of report detail (alert, summary, full details)			
• Sort or filter options			
Report Delivery Options			
• Format of report (PDF, text, XML,)			
• Delivery method (email, FTP, eFAX,)			
• Delivery Address (IP, email, etc.)			
• User(s) authorized to receive results			

D.4 PDMP Query-Enabled Pharmacy Workflow

After conducting a detailed analysis, the Pharmacy Subgroup produced the following detailed depiction of an "ideal" PDMP query-enabled pharmacy workflow. "DUR" stands for Drug Utilization Review.

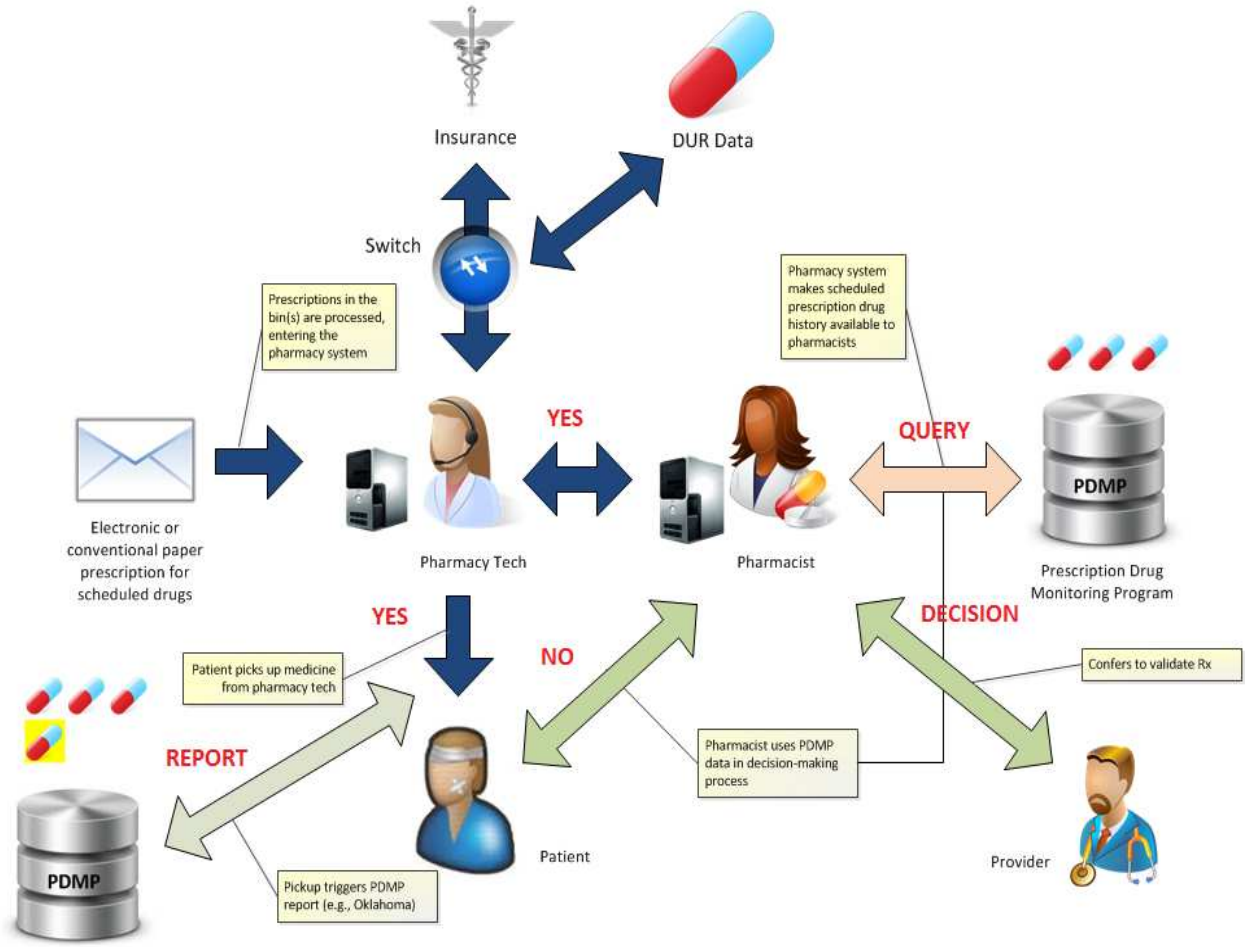


Figure 26. PDMP Query-Enabled Pharmacy Workflow

Appendix E Guiding Privacy Principles

E.1 OECD Guidelines Governing the Protection of Privacy (1980)

General Definitions

"Data controller" means a party who, according to domestic law, is competent to decide the contents and use of personal data regardless of whether or not such data are collected, stored, processed, or disseminated by that party or by an agent on its behalf.

“Personal data" means any information relating to an identified or identifiable individual (data subject).

"Transborder flows of personal data" means movements of personal data across national borders.

Data Quality and Integrity

Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete, and kept up to date.

Data Limitation

There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Purpose Specification

The purposes for which personal data are collected should be specified no later than at the time of data collection, and the subsequent use should be limited to the fulfillment of those purposes or such others not incompatible with those purposes and as specified on each occasion of change of purpose.

Use Limitation

Personal data should not be disclosed, made available, or otherwise used for purposes other than those specified in accordance with the Purpose Specification, except:

- With the consent of the data subject
- By the authority of law.

Security Safeguards

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification, or disclosure of data.

Openness and Transparency

There should be a general policy of openness about developments, practices, and policies with respect to personal data. Means should be readily available to establish the existence and nature of personal data and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation

Individuals should have the right:

- To obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them
- To have communicated to them data relating to them within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to them
- To be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial
- To challenge data relating to them and, if the challenge is successful, to have the data erased, rectified, completed, or amended.

Accountability

A data controller should be accountable for complying with measures that give effect to the principles stated above.

E.2 Fair Information Practice Principles

Notice/Awareness

Consumers should be given notice of an entity's information practices before any personal information is collected from them. Notice should include:

- Identification of the entity collecting the data
- Identification of the uses to which the data will be put
- Identification of any potential recipients of the data
- The nature of the data collected and the means by which it is collected, if not obvious
- Whether the provision of the requested data is voluntary or required, and the consequences of a refusal to provide the requested information
- The steps taken by the data collector to ensure the confidentiality, integrity, and quality of the data
- Any choice respecting the use of the data
- Whether the consumer has been given a right of access to the data
- The ability of the consumer to contest inaccuracies
- The availability of redress for violations of the practice code
- How such rights can be exercised.

Choice/Consent	Choice means giving consumers options as to how any personal information collected from them may be used, specifically, choice relates to secondary uses of information—i.e., uses beyond those necessary to complete the contemplated transaction.
Data Limitation	An individual's ability both to access data about himself or herself—i.e., to view the data in an entity's files—and to contest that data's accuracy and completeness.
Integrity/Security	Data must be accurate and secure. To assure data integrity, collectors must take reasonable steps, such as using only reputable sources of data and cross referencing data against multiple sources, providing consumer access to data, and destroying untimely data or converting it to anonymous form. Security involves both managerial and technical measures to protect against loss and the unauthorized access, destruction, use, or disclosure of the data.
Enforcement/Redress	A method to enforce core privacy principles and protections. Enforcement approaches include industry self-regulation, legislation that would create private remedies for consumers, and/or regulatory schemes enforceable through civil and criminal sanctions.

Appendix F Model Business Agreements

F.1 Public Entity to Public Entity Business Agreement (clean version)

This Data Use Agreement (the "Agreement") is effective as of _____ (the "Agreement Effective Date") by and between Prescription Monitoring Program ("PMP") and _____ ("Data Deliverer").

RECITALS

WHEREAS, PMP possesses Individually Identifiable Health Information that is or may be protected under state privacy law as well as HIPAA (as hereinafter defined) and the HIPAA Regulations (as hereinafter defined), and is permitted to use or disclose such information only in accordance with HIPAA and the HIPAA Regulations;

WHEREAS, Data Deliverer performs certain Activities (as hereinafter defined);

WHEREAS, PMP wishes to disclose a Limited Data Set (as hereinafter defined) to Data Deliverer for use by Data Deliverer in performance of the Activities (as hereinafter defined);

WHEREAS, PMP wishes to ensure that Data Deliverer will appropriately safeguard the Limited Data Set in accordance with applicable (state) law as well as HIPAA and the HIPAA Regulations; and

WHEREAS, Data Deliverer agrees to protect the privacy of the Limited Data Set in accordance with the terms and conditions of this Agreement, HIPAA and the HIPAA Regulations and applicable state law;

NOW THEREFORE, PMP and Data Deliverer agree as follows:

1. Definitions. The parties agree that the following terms, when used in this Agreement, shall have the following meanings, provided that the terms set forth below shall be deemed to be modified to reflect any changes made to such terms from time to time as defined in HIPAA and the HIPAA Regulations.

a. "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191.

b. "HIPAA Regulations" means the regulations promulgated under HIPAA by the United States Department of Health and Human Services, including, but not limited to, 45 C.F.R. Part 160 and 45 C.F.R. Part 164.

c. "PMP" means _____

d. "Individually Identifiable Health Information" means information that is a subset of health information, including demographic information collected from an individual, and;

(1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

(2) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

a) that identifies the individual; or

b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

e. "Protected Health Information" or "PHI" means Individually Identifiable Health Information that is transmitted by electronic media; maintained in any medium described in the definition of the term electronic media in the HIPAA Regulations; or transmitted or maintained in any other form or medium. Protected Health Information excludes Individually Identifiable Health Information in education records covered by the Family Educational Right and Privacy Act, as amended, 20 U.S.C. § 1232g, and records described at 20 U.S.C. § 1232g(a)(4)(B)(iv).

2. Obligations of PMP.

a. Limited Data Set. PMP agrees to disclose the following Protected Health Information to Data Deliverer: _____ (the "Limited Data Set"). Such Limited Data Set shall not contain any of the following identifiers of the individual who is the subject of the Protected Health Information: telephone numbers; fax numbers; electronic mail addresses; social security numbers; medical record numbers; health plan beneficiary numbers; account numbers; certificate/license numbers; vehicle identifiers and serial numbers, including license plate numbers; device identifiers and serial numbers; Web Universal Resource Locators (URLs); Internet Protocol (IP) address numbers; biometric identifiers, including finger and voice prints; and full face photographic images and any comparable images.

3. Obligations of Data Deliverer.

a. Performance of Activities. Data Deliverer may use and disclose the Limited Data Set received from PMP only in connection with the performance of the treatment, payment or operations as set out in applicable state law. Data Deliverer shall limit the receipt of the Limited Data Set to the following individuals or classes of individuals who need the Limited Data Set for the performance of the Activities:

List Authorized "Data Users"

_____

_____

_____

b. Nondisclosure Except As Provided In Agreement. Data Deliverer shall not use or further disclose the Limited Data Set except as permitted or required by this Agreement.

c. Use Or Disclosure As If a Covered Entity. Data Deliverer may not use or disclose the Limited Data Set in any manner that would violate the requirements of HIPAA or the HIPAA Regulations if Data Deliverer were a Covered Entity.

d. Identification Of Individual. Data Deliverer may not use the Limited Data Set to identify or contact any individual who is the subject of the PHI from which the Limited Data Set was created.

e. Disclosures Required By Law. Data Deliverer shall not, without the prior written consent of PMP, disclose the Limited Data Set on the basis that such disclosure is required by law without notifying PMP within the timeframe required by applicable law so that PMP shall have an opportunity to object to the disclosure and to seek appropriate relief. If PMP objects to such disclosure, Data Deliverer shall refrain from disclosing the Limited Data Set until PMP has exhausted all alternatives for relief.

f. Safeguards. Data Deliverer shall use any and all appropriate safeguards to prevent use or disclosure of the Limited Data Set other than as provided by this Agreement.

g. Data Deliverer's Agents. Data Deliverer shall not disclose the Limited Data Set to any agent or subcontractor of Data Deliverer except with the prior written consent of PMP. Data Deliverer shall ensure that any agents, including subcontractors, to whom it provides the Limited Data Set agree in writing to be bound by the same restrictions and conditions that apply to Data Deliverer with respect to such Limited Data Set.

h. Reporting. Each party shall report to each other within ____ hours of either party becoming aware of any use or disclosure of the Limited Data Set in violation of this Agreement, HIPPA and HITECH.

4. Material Breach, Enforcement and Termination.

a. Term. This Agreement shall be effective as of the Agreement Effective Date, and shall continue until the Agreement is terminated in accordance with the provisions of Section 4.c.

b. PMP's Rights of Access and Inspection. Upon 30 days notice, or upon a reasonable determination by PMP that Data Deliverer has materially breached this Agreement, defined as risk of significant loss or damage, or significant violation of state or federal law, PMP may inspect the facilities, systems, books and records of Data Deliverer to monitor compliance with this Agreement. This inspection shall be conducted with due consideration of the Data Deliverer's business functions. The fact that PMP inspects, or fails to inspect, or has the right to inspect, Data Deliverer's facilities, systems and procedures does not relieve Data Deliverer of its responsibility to comply with this Agreement, nor does PMP's (1) failure to detect or (2) detection of, but failure to notify Data Deliverer or require Data Deliverer's remediation of, any unsatisfactory practices constitute acceptance of such practice or a waiver of State Agency's enforcement or termination rights under this Agreement. The parties' respective rights and obligations under this Section 4.b. shall survive termination of the Agreement.

c. Termination. PMP may terminate this Agreement:

(1) immediately if Data Deliverer is named as a defendant in a criminal proceeding for a violation of applicable state law, HIPAA or the HIPAA Regulations;

(2) immediately if a finding or stipulation that Data Deliverer has violated any standard or requirement of HIPAA, the HIPAA Regulations, or any other security or privacy laws is made in any administrative or civil proceeding in which Data Deliverer has been joined; or

(3) pursuant to Sections 4.d.(3) or 5.b. of this Agreement

(4) upon 30 written days notice for the convenience of the state agency.

d. Remedies. If PMP determines that Data Deliverer has breached or violated a material term of this Agreement, PMP may, at its option, pursue any and all of the following remedies:

(1) exercise any of its rights of access and inspection under Section 4.b. of this Agreement;

(2) take any other reasonable steps that PMP, in its sole discretion, shall deem necessary to cure such breach or end such violation including reporting possible criminal violations; and/or

(3) terminate this Agreement immediately.

e. Knowledge of Non-Compliance. Any non-compliance by Data Deliverer with this Agreement, applicable state law, or with HIPAA or the HIPAA Regulations automatically will be considered a breach or violation of a material term of this Agreement if Data Deliverer knew or reasonably should have known of such non-compliance and failed to take reasonable steps to cure the non-compliance.

f. Reporting to United States Department of Health and Human Services. If PMP's efforts to cure any breach or end any violation are unsuccessful, and if termination of this Agreement is not feasible, PMP shall report Data User's breach or violation to the Secretary of the United States Department of Health and Human Services, and Data Deliverer agrees that it shall not have or make any claim(s), whether at law, in equity, or under this Agreement, against PMP with respect to such report(s).

g. Return or Destruction of Records _____

h. Injunctions. PMP and Data Deliverer agree that any violation of the provisions of this Agreement may cause irreparable harm to either party. Accordingly, in addition to any other remedies available to either party at law, in equity, or under this Agreement, in the event of any violation by Data Deliverer of any of the provisions of this Agreement, or any explicit threat thereof, either party shall be entitled to an injunction or other decree of specific performance with respect to such violation or explicit threat thereof, without any bond or other security being required and without the necessity of demonstrating actual damages. The parties' respective rights and obligations under this Section 4.h. shall survive termination of the Agreement.

i. Indemnification. Data Deliverer shall indemnify, hold harmless and defend PMP from and against any and all claims, losses, liabilities, costs and other expenses resulting from, or relating to, the acts or omissions of Data Deliverer in connection with the representations, duties and obligations of Data Deliverer under this Agreement. The parties' respective rights and obligations under this Section 4.i. shall survive termination of the Agreement.

5. Miscellaneous Terms.

a. Amendment. PMP and Data Deliverer agree that amendment of this Agreement may be required to ensure that PMP and Data Deliverer comply with changes in state and federal laws and regulations relating to the privacy, security, and confidentiality of PHI or the Limited Data Set. PMP may terminate this Agreement upon ___ days written notice in the event that Data Deliverer does not promptly enter into an amendment that PMP, in its sole discretion, deems sufficient to ensure that PMP will be able to comply with such laws and regulations.

b. No Third Party Beneficiaries. Nothing express or implied in this Agreement is intended or shall be deemed to confer upon any person other than PMP and Data Deliverer, and their respective successors and assigns, any rights, obligations, remedies or liabilities.

c. Ambiguities. The parties agree that any ambiguity in this Agreement shall be resolved in favor of a meaning that complies and is consistent with applicable state and federal law protecting the privacy, security and confidentiality of PHI and the Limited Data Set, including, but not limited to, HIPAA and the HIPAA Regulations.

d. Primacy. To the extent that any provisions of this Agreement conflict with the provisions of any other agreement or understanding between the parties, this Agreement shall control with respect to the subject matter of this Agreement.

IN WITNESS WHEREOF, the parties hereto have duly executed this Agreement as of the Agreement Effective Date.

Name of PMP	Name of Data User
Signature of Authorized Representative	Signature of Authorized Representative
Name of Authorized Representative	Name of Authorized Representative
Title of Authorized Representative	Title of Authorized Representative

F.2 Public Entity to Public Entity Business Agreement (marked version)

This Data Use Agreement (the "Agreement") is effective as of _____ (the "Agreement Effective Date") by and between Prescription Monitoring Program ("PMP") and _____ ("Data Deliverer").

This business agreement is designed to be between two public entities. It could have appended to it another agreement (e.g., BAA) in some circumstances, or be supplemented with state "boilerplate" language (likely). Note that the origin of this document is a DUA for the State of Kentucky, and as such it contains a certain amount of residual context.

RECITALS

WHEREAS, PMP possesses Individually Identifiable Health Information that is or may be protected under state privacy law as well as HIPAA (as hereinafter defined) and the HIPAA Regulations (as hereinafter defined), and is permitted to use or disclose such information only in accordance with HIPAA and the HIPAA Regulations;

WHEREAS, Data Deliverer performs certain Activities (as hereinafter defined);

WHEREAS, PMP wishes to disclose a Limited Data Set (as hereinafter defined) to Data Deliverer for use by Data Deliverer in performance of the Activities (as hereinafter defined);

WHEREAS, PMP wishes to ensure that Data Deliverer will appropriately safeguard the Limited Data Set in accordance with applicable (state) law as well as HIPAA and the HIPAA Regulations; and

WHEREAS, Data Deliverer agrees to protect the privacy of the Limited Data Set in accordance with the terms and conditions of this Agreement, HIPAA and the HIPAA Regulations and applicable state law;

NOW THEREFORE, PMP and Data Deliverer agree as follows:

1. Definitions. The parties agree that the following terms, when used in this Agreement, shall have the following meanings, provided that the terms set forth below shall be deemed to be modified to reflect any changes made to such terms from time to time as defined in HIPAA and the HIPAA Regulations.

a. "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191.

b. "HIPAA Regulations" means the regulations promulgated under HIPAA by the United States Department of Health and Human Services, including, but not limited to, 45 C.F.R. Part 160 and 45 C.F.R. Part 164.

c. "PMP" means [a health plan (as defined by HIPAA and the HIPAA Regulations), a health care clearinghouse (as defined by HIPAA and the HIPAA Regulations), or a health care provider (as defined by HIPAA and the HIPAA Regulations) who transmits any health information in electronic form in connection with a transaction covered by the HIPAA Regulations.]

This is the original definition used here. The issue of interstate hubs would be appropriate to address in this section in some cases. Note that this is based on the Kentucky model, with

PDMP as a CE (clearinghouse), a decision that remains in flux. For non-CE states (most), this will require modification. A definition should be put here, but it can vary considerably.

d. "Individually Identifiable Health Information" means information that is a subset of health information, including demographic information collected from an individual, and;

(1) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

(2) relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

a) that identifies the individual; or

b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

e. "Protected Health Information" or "PHI" means Individually Identifiable Health Information that is transmitted by electronic media; maintained in any medium described in the definition of the term electronic media in the HIPAA Regulations; or transmitted or maintained in any other form or medium. Protected Health Information excludes Individually Identifiable Health Information in education records covered by the Family Educational Right and Privacy Act, as amended, 20 U.S.C. § 1232g, and records described at 20 U.S.C. § 1232g(a)(4)(B)(iv).

f. Authorized users: _____

Some early versions had additional definitions of authorized users here instead of in 3A

2. Obligations of PMP.

a. Limited Data Set. PMP agrees to disclose the following Protected Health Information to Data Deliverer: _____ (the "Limited Data Set"). Such Limited Data Set shall not contain any of the following identifiers of the individual who is the subject of the Protected Health Information: telephone numbers; fax numbers; electronic mail addresses; social security numbers; medical record numbers; health plan beneficiary numbers; account numbers; certificate/license numbers; vehicle identifiers and serial numbers, including license plate numbers; device identifiers and serial numbers; Web Universal Resource Locators (URLs); Internet Protocol (IP) address numbers; biometric identifiers, including finger and voice prints; and full face photographic images and any comparable images.

It may be worthwhile to list the fields within the limited data set (not just the ones that cannot be there), perhaps in an addendum

3. Obligations of Data Deliverer.

a. Performance of Activities. Data Deliverer may use and disclose the Limited Data Set received from PMP only in connection with the performance of the treatment, payment or operations as set out in applicable state law. Data Deliverer shall limit the receipt of the Limited Data Set to the following individuals or classes of individuals who need the Limited Data Set for the performance of the Activities:

TPO callout and/or as provided in a separate exhibit, perhaps supplemented with language to the effect of "duties as applicable under existing law and regulation"

List Authorized "Data Users"

Recipients go here. It was noted that two tracks are possible: citation of statutory/regulatory authority or listing, as a way of handling the authentication issue.

b. Nondisclosure Except As Provided In Agreement. Data Deliverer shall not use or further disclose the Limited Data Set except as permitted or required by this Agreement [or as permitted by applicable state and/or federal law].

Not enumerating uses keeps it short. MOUs typically align with state/federal law. Broader may be better. Permitting no secondary uses is a good fallback option.

c. Use Or Disclosure As If a Covered Entity. Data Deliverer may not use or disclose the Limited Data Set in any manner that would violate the requirements of HIPAA or the HIPAA Regulations if Data Deliverer were a Covered Entity.

d. Identification Of Individual. Data Deliverer may not use the Limited Data Set to identify or contact any individual who is the subject of the PHI from which the Limited Data Set was created.

e. Disclosures Required By Law. Data Deliverer shall not, without the prior written consent of PMP, disclose the Limited Data Set on the basis that such disclosure is required by law without notifying PMP within the timeframe required by applicable law so that PMP shall have an opportunity to object to the disclosure and to seek appropriate relief. If PMP objects to such disclosure, Data Deliverer shall refrain from disclosing the Limited Data Set until PMP has exhausted all alternatives for relief.

There was some concern about this section regarding the role of the deliverer. For example, if the HIE receives a court order to turn over PDMP data, the HIE would need to notify the PDMP so they can decide if they want to object. It was also noted that various states have various rules regarding what law enforcement needs to do to get access – and these strictures can be more or less stringent. Some PDMPs are in law enforcement agencies as well, and this may render this section impractical. Likewise, the case of Santa Cruz Prison is an example of a HIE/law enforcement tie in. In addition, a BA with a CE would redirect the court order back to the CE, but would yet be required to comply. CE motion to quash may be filed Applicable law may also include local trial law.

f. Safeguards. Data Deliverer shall use any and all appropriate safeguards to prevent use or disclosure of the Limited Data Set other than as provided by this Agreement.

g. Data Deliverer's Agents. Data Deliverer shall not disclose the Limited Data Set to any agent or subcontractor of Data Deliverer except with the prior written consent of PMP. Data Deliverer shall ensure that any agents, including subcontractors, to whom it provides the Limited Data Set agree in writing to be bound by the same restrictions and conditions that apply to Data Deliverer with respect to such Limited Data Set.

h. Reporting. Each party shall report to each other within ____ hours of either party becoming aware of any use or disclosure of the Limited Data Set in violation of this Agreement, HIPPA and HITECH.

There is a difference between a breach by legitimate HIE user and the actions of hackers. This used to be "data deliverer" instead of "each party".

4. Material Breach, Enforcement and Termination.

Note that a security breach and a contract breach are different. See H above

a. Term. This Agreement shall be effective as of the Agreement Effective Date, and shall continue until the Agreement is terminated in accordance with the provisions of Section 4.c. [or the _____ Agreement between the parties terminates].

This was the original option

b. PMP's Rights of Access and Inspection. Upon 30 days notice, or upon a reasonable determination by PMP that Data Deliverer has materially breached this Agreement, defined as risk of significant loss or damage, or significant violation of state or federal law, PMP may inspect the facilities, systems, books and records of Data Deliverer to monitor compliance with this Agreement. This inspection shall be conducted with due consideration of the Data Deliverer's business functions. The fact that PMP inspects, or fails to inspect, or has the right to inspect, Data Deliverer's facilities, systems and procedures does not relieve Data Deliverer of its responsibility to comply with this Agreement, nor does PMP's (1) failure to detect or (2) detection of, but failure to notify Data Deliverer or require Data Deliverer's remediation of, any unsatisfactory practices constitute acceptance of such practice or a waiver of State Agency's enforcement or termination rights under this Agreement. The parties' respective rights and obligations under this Section 4.b. shall survive termination of the Agreement.

The fact that "reasonable determination" is by 1 party may be an issue. This may be helped by explicit material breach clause. Breach means that 30 days notice not required for an audit. A DURSA may set specific turnaround times, and these are less than 30 days, and should have its own breach notification clause(s). There was also some discussion of how much this may cost, and possibly capping this or demanding pay-as-you-go for extensive inspections.

c. Termination. PMP may terminate this Agreement:

(1) immediately if Data Deliverer is named as a defendant in a criminal proceeding for a violation of applicable state law, HIPAA or the HIPAA Regulations;

(2) immediately if a finding or stipulation that Data Deliverer has violated any standard or requirement of HIPAA, the HIPAA Regulations, or any other security or privacy laws is made in any administrative or civil proceeding in which Data Deliverer has been joined; or

(3) pursuant to Sections 4.d.(3) or 5.b. of this Agreement

(4) upon 30 written days notice for the convenience of the state agency [or lack of funding].

This was the original option. It was noted that Kentucky very much likes this convenience clause as a fallback option. Other states may as well.

d. Remedies. If PMP determines that Data Deliverer has breached or violated a material term of this Agreement, PMP may, at its option, pursue any and all of the following remedies:

(1) exercise any of its rights of access and inspection under Section 4.b. of this Agreement;

(2) take any other reasonable steps that PMP, in its sole discretion, shall deem necessary to cure such breach or end such violation including reporting possible criminal violations; and/or

"Criminal violations" may be a good place to get law enforcement input

(3) terminate this Agreement immediately.

e. Knowledge of Non-Compliance. Any non-compliance by Data Deliverer with this Agreement, applicable state law, or with HIPAA or the HIPAA Regulations automatically will

be considered a breach or violation of a material term of this Agreement if Data Deliverer knew or reasonably should have known of such non-compliance and failed to take reasonable steps to cure the non-compliance.

f. Reporting to United States Department of Health and Human Services. If PMP's efforts to cure any breach or end any violation are unsuccessful, and if termination of this Agreement is not feasible, PMP shall report Data User's breach or violation to the Secretary of the United States Department of Health and Human Services, and Data Deliverer agrees that it shall not have or make any claim(s), whether at law, in equity, or under this Agreement, against PMP with respect to such report(s).

g. Return or Destruction of Records - [Upon termination of this Agreement for any reason, Data Deliverer shall return or destroy, as specified by PMP, the Limited Data Set that Data Deliverer still maintains in any form, and shall retain no copies of such Limited Data Set [but can retain evidence of data access]. If PMP, in its sole discretion, requires that Data Deliverer destroy the Limited Data Set, Data Deliverer shall certify to PMP that the Limited Data Set has been destroyed. If return or destruction is not feasible, Data Deliverer shall inform PMP of the reason it is not feasible and shall continue to extend the protections of this Agreement to such Limited Data Set and limit further use and disclosure of such Limited Data Set to those purposes that make the return or destruction of such Limited Data Set infeasible.]

This was the original option, and is common in Kentucky and some other states (not specified). It was also noted that if a clinician makes a decision based on that data, at least some portion may need to be kept. Retaining evidence of data access can be important.

h. Injunctions. PMP and Data Deliverer agree that any violation of the provisions of this Agreement may cause irreparable harm to either party. Accordingly, in addition to any other remedies available to either party at law, in equity, or under this Agreement, in the event of any violation by Data Deliverer of any of the provisions of this Agreement, or any explicit threat thereof, either party shall be entitled to an injunction or other decree of specific performance with respect to such violation or explicit threat thereof, without any bond or other security being required and without the necessity of demonstrating actual damages. The parties' respective rights and obligations under this Section 4.h. shall survive termination of the Agreement.

Use of "either party" is intentional.

i. Indemnification. Data Deliverer shall indemnify, hold harmless and defend PMP from and against any and all claims, losses, liabilities, costs and other expenses resulting from, or relating to, the acts or omissions of Data Deliverer in connection with the representations, duties and obligations of Data Deliverer under this Agreement. The parties' respective rights and obligations under this Section 4.i. shall survive termination of the Agreement.

5. Miscellaneous Terms.

a. [State Law. Nothing in this Agreement shall be construed to require Data Deliverer to use or disclose the Limited Data Set without a written authorization from an individual who is a subject of the PHI from which the Limited Data Set was created, or written authorization from any other person, where such authorization would be required under state law for such use or disclosure]

This was the original option, and some may wish to make a portion or all of this optional. HIPAA carve-outs may be highly relevant. It would be very impractical to get consent from abusers, and as such notice may suffice. This section was not fully resolved, but was our best

effort. Some argued for deletion, and as such, this section is not in the "clean version" (starts with Amendment)

b. Amendment. PMP and Data Deliverer agree that amendment of this Agreement may be required to ensure that PMP and Data Deliverer comply with changes in state and federal laws and regulations relating to the privacy, security, and confidentiality of PHI or the Limited Data Set. PMP may terminate this Agreement upon ___ days written notice in the event that Data Deliverer does not promptly enter into an amendment that PMP, in its sole discretion, deems sufficient to ensure that PMP will be able to comply with such laws and regulations.

b. No Third Party Beneficiaries. Nothing express or implied in this Agreement is intended or shall be deemed to confer upon any person other than PMP and Data Deliverer, and their respective successors and assigns, any rights, obligations, remedies or liabilities.

c. Ambiguities. The parties agree that any ambiguity in this Agreement shall be resolved in favor of a meaning that complies and is consistent with applicable state and federal law protecting the privacy, security and confidentiality of PHI and the Limited Data Set, including, but not limited to, HIPAA and the HIPAA Regulations.

d. Primacy. To the extent that any provisions of this Agreement conflict with the provisions of any other agreement or understanding between the parties, this Agreement shall control with respect to the subject matter of this Agreement.

IN WITNESS WHEREOF, the parties hereto have duly executed this Agreement as of the Agreement Effective Date.

Name of PMP	Name of Data User
Signature of Authorized Representative	Signature of Authorized Representative
Name of Authorized Representative	Name of Authorized Representative
Title of Authorized Representative	Title of Authorized Representative

Substitute own statutory page as needed and appropriate

F.3 Public Entity to Private Entity Business Agreement (clean version)

Master Agreement/Contract

("Agreement")

"PARTICIPANT"

_____

_____

Address of Participant

_____

_____

Tax I.D. No.:

"HIE" Health Information Exchange

Address of HIE:

RECITALS

A. HIE provides a Clinical Messaging System, as hereinafter defined, to improve the quality of health care in the community and to enhance health care providers' ability to exchange electronic data. HIE may also provide other products or services from time to time.

B. Participant is a PMP which HIE has agreed to accept for enrollment. Participant desires to Use the Clinical Messaging System provided by HIE for purposes of promoting the improvement of health care treatment, payment and operations.

C. In order to send or receive data through the HIE Clinical Messaging System, Participant must first make various covenants, warranties and representations to HIE, as hereinafter set forth, concerning the Use of the Clinical Messaging System and related tools and services. In providing the Clinical Messaging System and related tools and services to Participant, HIE must first make various covenants, warranties, and representations to Participant as hereinafter set forth.

D. The relationship between HIE and Participant created under the terms of this Agreement results in HIE's classification as a "Business Associate" under HIPAA. The HIPAA regulations require Participant to enter agreements that include certain mandated provisions, which are included as part of this Agreement, with all vendors and contractors that are classified as "Business Associates."

NOW, THEREFORE, in consideration of the recitals set forth above and the mutual promises set forth below, the parties agree as follows:

A. Services. HIE will manage and administer the Clinical Messaging System and its Use. So long as this Agreement is in effect and Participant and Participant Users comply with all terms of this Agreement, HIE will provide Participant and Participant Users access to Use the Clinical Messaging System. HIE and Participant agree to all Terms and Conditions, attached.

B. Fees. Participant agrees to pay HIE the amounts referenced on attached Exhibit ___, along with applicable taxes, associated with various Uses of the Clinical Messaging System as required by the Order and Invoice. Any amounts not paid when due shall bear interest at the rate of eighteen percent (18%) per annum. Participant agrees that payment amounts and the interest rate are subject to change upon sixty (60) days written notice to Participant from HIE, subject to Participant's right to terminate the Agreement as provided herein. HIE may refuse Participant and Participant Users access to Uses of the

Clinical Messaging System if payment is not timely made by Participant.

C. Addendums ____

This Agreement is dated and shall be effective on the date set forth below by HIE as the effective date.

SIGNATURE PAGE BETWEEN PARTICIPANT AND HIE

Effective Date _____

TERMS AND CONDITIONS:

1. Definitions. Terms used but not otherwise defined in this Agreement shall have the same meaning as those terms in 45 C.F.R. 160.103 and 164.501. All terms defined in this Agreement shall have a meaning consistent with terms defined in 45 C.F.R. 160.103 and 164.501. Capitalized terms in this Agreement are defined as follows:

1.1. "Board of Directors" shall mean the Board of Directors of HIE.

1.2. "Breach" shall mean the unauthorized acquisition, access, use, or disclosure of PHI as defined in Section 13400 of HITECH and 45 C.F.R. 164.402.

1.3. "Business Associate" shall mean a person or entity who performs a function for or assists a Covered Entity or organized health care arrangement with the performance of a function or activity involving the use or disclosure of PHI. Examples of functions include, but are not limited to: data analysis, consulting, data aggregation, management, administrative or financial services. The provision of the service involves the disclosure of PHI from the Covered Entity or organized health care arrangement, or from another Business Associate of the Covered Entity or organized health care arrangement, to the person or entity.

1.4. "Clinical Messaging System" or "System" shall mean the technology tools, services and systems HIE provides and/ or maintains.

1.5. "Covered Entity" shall mean a Participant in the Clinical Messaging System that meets the definition of a Covered Entity under HIPAA.

1.6. "De-identification" shall mean to remove, encode, encrypt, or otherwise eliminate or conceal data which identifies an Individual, or modifies information so that there is no reasonable basis to believe that the information can be used to identify an Individual. De-identification includes, without limitation, any process meeting the requirements for De-identification set forth in 45 C.F.R. § 164.514, as such provision is currently drafted and as it may be subsequently updated, amended, or revised.

1.7. "Designated Record Set" means Protected Health Information maintained by or for Participant that is: (1) the medical records and billing records about Individuals maintained by or for a covered health care provider; (2) the enrollment, payment, claims adjudication, and case or

medical management record systems maintained by or for a health plan; or (3) used, in whole or in part, by or for Participant to make decisions about Individuals.

1.8. "Disclose," "Disclosing," or "Disclosure" means the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information.

1.09. "HITECH" means the Health Information Technology for Economic and Clinical Health Act in the American Recovery and Reinvestment Act of 2009, including any implementing regulations.

1.10. "Individual" means a natural person who is the subject of PHI.

1.11. "Information Privacy and Protection Laws" mean (i) the Health Insurance Portability and Accountability Act of 1996, as amended and including any implementing regulations ("HIPAA"); (ii) HITECH; (iii) the Gramm-Leach-Bliley Act, as amended and including any implementing regulations; (iv) any statute, regulation, administrative or judicial ruling requiring a party to protect the privacy or security of information pertaining to the health or medical status or condition of an Individual, and/or the payment for health or medical care for an Individual; (v) any statute, regulation, administrative or judicial ruling requiring a party to protect the privacy of information pertaining to the financial or credit status or condition of an individual; (vi) any statute, regulation, administrative or judicial ruling requiring a party to protect information pertaining to individuals based upon the individuals' status as consumers; and (vii) any other statute, regulation, administrative or judicial ruling requiring a party to protect the confidentiality, privacy and/or security of information pertaining to individuals; all to the extent that such Information Privacy and Protection Laws have been enacted, promulgated, issued or published by any federal or state governmental authority with jurisdiction over an individual, a Participant or HIE.

1.12. "Message Content" shall mean that information which is requested or sent by a Participant to another user of the Clinical Messaging System through the HIE, including but not limited to, PHI, individually identifiable information, de-identified data, pseudonymized data, metadata, digital certificates issued by HIE to any Participant, and schema.

1.13. "Network Account" shall mean the right given to Participant to access and Use the Clinical Messaging System by Participant and Participant Users.

1.14. "Participant User" shall mean any person accepted by HIE and who is authorized to use the Clinical Messaging System through Participant's right of Use set forth in this Agreement. Participant shall designate Participant Users.

1.15. "Protected Health Information," or "PHI," means any information that identifies or could reasonably be used to identify an Individual, which in any way concerns that Individual's health status, health care, or payments for his or her health care, or which a party is otherwise legally required to protect under an Information Privacy and Protection Law applicable to that party, and includes as well any information derived by the processing of such information that is not De-Identified with respect to any Individual who is the subject of the information.

1.16. "HIE's Standards" shall mean those standards, policies and procedures adopted by the Board of Directors and subject to revision, modification or change by the Board of Directors, which address requirements and standards with regard to Use of the Clinical Messaging System. HIE's Standards may include, but are not limited to: activity on the System, operating rules, definitions and specifications of format, content, and transmission of electronic data, support descriptions and details of connecting to the System.

1.17. “Receive,” “Receiving,” and “Receipt” means (i) to take physical delivery of media containing information, or (ii) in the case of electronic delivery, for information to come into existence in a party’s information processing system in a form capable of being processed by or perceived from a system of that type by the Receiving party if the Receiving party has designated that system or address as a place for Receipt of information to a Disclosing party and the Disclosing party does not know that the information cannot be accessed from the particular system.

1.18. “Security Rule” means the Security Standards for Protection of Electronic Protected Health Information at 45 C.F.R. Part 164, Subpart C.

1.19. “Third Party” means any individual, person, or organization not a party to this Agreement.

1.20. “Transaction” means the Transmission of information between parties to this Agreement.

1.21. “Transmit,” “Transmitted,” or “Transmission” means the transfer of information by one party to another, regardless of the method or technology used to transfer the information.

1.22. “Use” shall mean the sharing, employment, application, utilization, examination, analysis, De-identification, or commingling with other information, of information by a party that holds that information.

2. Duties and Obligations of HIE.

2.1. Training. HIE will provide training for Participant and Participant Users as regards the Clinical Messaging System in accordance with a reasonable schedule that will be mutually agreed to by the parties.

2.2. Use of Clinical Messaging System. HIE will provide Participant and Participant Users products and services and access to the Uses of the Clinical Messaging System described on Exhibit ___ provided such Use is consistent with HIE’s Standards. HIE shall furnish each Participant User a unique identification method (i.e.: login, password, PIN, etc.) with which each Participant User will be able to initially access and Use the Clinical Messaging System. Participant User shall change the initial password they receive immediately after initial login to the System. The Participant User shall not share the Participant User’s password or any other security measures issued to the Participant User by HIE with any person. All access to the System shall use full SSL security, message tracing and message acknowledgement.

2.3. Data Storage and Distribution. Data within the Clinical Messaging System will be available to Participant Users pursuant to HIE’s Standards and subject to compliance with applicable laws. The Uses of the Clinical Messaging System that are provided to Participant Users are described on Exhibit ___.

2.4. Data Backup. HIE shall make available requisite disk space for the storage of software and data as may be required for HIE, as a Business Associate, to comply with applicable law, but in any event there shall be available sufficient disk space to permit Participants to retain an estimated five (5) years of clinical data, or as required to comply with applicable law. If HIE and Participant dispute whether a Participant’s use is “normal use” the parties shall resolve such disputes in accordance with paragraph 5 of this Agreement. Tape backups will be regularly performed and stored in a secured off-site location.

2.5. Inquiries from Individuals. Should HIE receive from an Individual a request for data specific to such Individual, which data the Individual believes is contained in the Clinical Messaging System, HIE shall redirect the Individual to the health care provider from whom the Individual

received the services which the data references. HIE will not provide medical record data or other information stored within the Clinical Messaging System to such Individuals other than as required by law.

2.6. Right to Audit. HIE shall have the right to audit Participant's and Participant Users' Use of the Clinical Messaging System to ascertain compliance with HIE's Standards and applicable law with regard to Use of the Clinical Messaging System. The results of such audits shall be shared with Participant and the HIE Board of Directors.

2.7. Right to Impose Sanctions. HIE shall have the right to impose sanctions as described in HIE's Standards on a Participant User should Participant User's Use of the Clinical Messaging System be in violation of the terms of this Agreement or HIE's Standards.

2.8. Liability Insurance. HIE shall purchase and/or maintain liability insurance or a self-insurance plan which provides coverage to HIE of not less than one million dollars ($1,000,000) per incident per year for any claims arising from or in connection with the provision of services under this Agreement.

2.9. Indemnity. HIE agrees to indemnify Participant from any and all claims, demands, actions, and causes of action asserted by a third party against Participant which may result or arise out of any actions or omissions of HIE or any of HIE's agents, employees, or representatives due to HIE's failure to comply with privacy or security obligations under this Agreement or imposed by law or HIE's failure to comply with the terms of this Agreement. This indemnity shall include the payment to Participant for attorney's fees, court costs and expert witness fees Participant incurs in defending itself from any such claims, demands, actions or cause of action. For this indemnity obligation to apply, Participant shall (a) provide HIE notice in writing upon the discovery of the claim, (b) fully cooperate with HIE in the defense of the claim, and (c) not settle the claim without the prior written consent of HIE, which consent shall not be unreasonably withheld. If there is a Breach by HIE and/or HIE's agents or subcontractors in the course of HIE providing services to Participant and Participant is required by law to notify the involved Individual(s) of whom such Breach pertains and/or any governmental entity as may be required by law, HIE shall pay all Participant's reasonable notification costs and, as mutually agreed by the parties, reasonable costs associated with mitigating any harmful effects of such Breach. For purposes of this paragraph, a HIE agent or subcontractor shall mean those persons or entities that have a contract with HIE to provide HIE with products or services. HIE's liability under this paragraph shall not exceed the greater of coverage for such liability as may be provided by insurance held by HIE or the total amount paid by Participant to HIE to obtain services under this Agreement for the twelve (12) month period preceding the date such liability arose.

2.10. DISCLAIMER. HIE MAKES NO WARRANTIES, EXPRESS OR IMPLIED, WITH REGARD TO THE CLINICALMESSAGING SYSTEM, INCLUDING BUTNOT LIMITED TO, ANY WARRANTY OFNONINFRINGEMENT, OR THE IMPLIEDWARRANTY OF MERCHANTABILITYAND FITNESS FOR A PARTICULARPURPOSE REGARDLESS OF THESERVICES OR RESOURCES PROVIDED BYIT. HIE DISCLAIMS ANY LIABILITY FORTHE FAILURE OF PERSON WHO USESTHE CLINCIAL MESSAGING SYSTEM TOCOMPLY WITH HIE'S STANDARDS ORAPPLICABLE LAW OR THE CONTENT ORUSE OF THE CLINICAL MESSAGINGSYSTEM BY ANY SUCH PERSON. HIEDOES NOT WARRANT UNINTERRUPTEDOR ERROR FREE OPERATION OF THECLINICAL MESSAGING SYSTEM OR THECOMPATIBILITY OF THE CLINICALMESSAGING SYSTEM WITH ANYPARTICULAR HARDWARE, SOFTWAREOR INTER-CONNECTIVITY WITH OTHERNETWORKS OR SERVICES.

2.11. LIMITATION OF LIABILITY.EXCEPT FOR HIE'S LIABILITYOBLIGATIONS AS EXPRESSLY SETFORTH IN THE INDEMNITY PARAGRAPHOF THIS AGREEMENT, REGARDLESS OFWHETHER ANY REMEDY FAILS OF ITSESSENTIAL PURPOSE, THE MAXIMUMLIABILITY OF HIE UNDER THISAGREEMENT SHALL NOT EXCEED THETOTAL AMOUNT PAID BY PARTICIPANTTO HIE TO OBTAIN SERVICES UNDERTHIS AGREEMENT FOR THE TWELVE (12) MONTH PERIOD PRECEDING THEDATE THE LIABILITY AROSE. IN NOEVENT SHALL HIE BE LIABLE FORSPECIAL, INCIDENTAL, CONSEQUENTIAL, OR EXEMPLARYDAMAGES INCLUDING WITHOUTLIMITATION, LOST DATA OR LOSTPROFITS.

3. Duties and Obligations of Participant.

3.1. Assistance and Cooperation with HIE in Providing Products and Services. Participant, at its sole cost and expense, shall cooperate and work in good faith with HIE to assist HIE in working with Participant to provide the products and services described in Exhibit___.

3.2. Complying with HIE's Standards In Use of Clinical Messaging System. In Using the Clinical Messaging System, Participant shall Use the System in a manner consistent with and shall comply with HIE's Standards and applicable law. Participant specifically agrees to comply with and to be subject to HIE's Standards. HIE's Standards are subject to amendment, revision and modification by the Board of Directors solely in its discretion. Changes to HIE's Standards may reflect changes in applicable law or the need to adopt new technologies, systems, or desired functionality or changes in HIE's operational policies. Participant is encouraged to provide input to HIE's Standards and to propose changes. Copies of all HIE's Standards may be reviewed upon request.

3.3 Participant Responsibility for Data. HIE provides tools for Participant Users to use the Clinical Messaging System but does not act in any other way for Participant or any other person or entity that Uses the Clinical Messaging System. HIE is not responsible for and does not inspect the contents of data that any Participant or any other persons or entity places in or obtains from the Clinical Messaging System. Participant's decision to place certain data in and Use the Clinical Messaging System is based on Participant's sole discretion. By placing an Individual's PHI in the Clinical Messaging System, Participant is certifying to HIE that such PHI can be Disclosed to Covered Entities for purposes of health care treatment. To the maximum extent permitted by applicable law, as between Participant and HIE, Participant is solely responsible for establishing the connection to the Clinical Messaging System, the proper transmission and receipt of data, for implementing sufficient safeguards and procedures to satisfy particular requirements for security, privacy and accuracy of data placed in or transmitted by Participant in Using the Clinical Messaging System. Backup of data located on Participant's own computer components is Participant's responsibility; HIE will backup data on the Clinical Messaging System as described in paragraph 2.4 of this Agreement.

3.4. Contact Information. Participant agrees to notify HIE in writing as soon as possible as to any change in status of a Participant User. Participant is responsible to provide HIE with the most current name and contact information for Participant and all Participant Users.

3.5. Training of Staff. Compliance with applicable federal and state laws, rules and regulations concerning adequate training of staff is the sole responsibility of the Participant.

3.6. Resources. Except as otherwise provided by Exhibit__, Participant, at Participant's own expense, shall provide and maintain necessary hardware, software, equipment and services necessary to Use the Clinical Messaging System. In addition to the services described in

Exhibit__, HIE may provide services as ancillary services, but such services would be performed under the terms of a separate addendum or agreement (an "Order "as defined in Exhibit___) between HIE and Participant. Support services which may be available under the terms of a separate addendum or agreement include: (a) help desk services during business hours and limited holiday and weekend hours, and (b) onsite support services at Participant's location.

3.7. Responsibility for Network Account. Participant shall be solely responsible for all Use of its Network Account, for payment of charges incurred for such Use, and for violations of the terms of this Agreement by anyone using the Network Account.

3.8. Warranties with Use. By its Use of the Clinical Messaging System, Participant warrants (1) that Participant's and Participant Users' Use is in compliance with the terms of this Agreement, and (2) that Participant's and Participant Users' Use is in compliance with applicable law.

3.9. Indemnity. Participant agrees to indemnify HIE and hold HIE harmless from any and all claims, demands, actions, and causes of action asserted by a third party against HIE which may result or arise out of any actions of Participant or any Participant User who becomes an authorized user through this Agreement or any Use through Participant's Network Account. This indemnity shall include the payment to HIE for attorney's fees, court costs and expert witness fees HIE incurs in defending itself from any such claims, demands, actions or cause of action. For this indemnity obligation to apply, HIE shall (a) provide Participant notice in writing upon the discovery of the claim, (b) fully cooperate with Participant in the defense of the claim, and (c) not settle the claim without the prior written consent of Participant, which consent shall not be unreasonably withheld. If there is a Breach by Participant and/or Participant's agents or subcontractors in the course of HIE providing services to Participant and HIE is required by law to notify the involved Individual(s) of whom such Breach pertains and/or any governmental entity as may be required by law, Participant shall pay all HIE's reasonable notification costs and, as mutually agreed by the parties, reasonable costs associated with mitigating any harmful effects of such Breach. For purposes of this paragraph, a Participant agent or subcontractor shall mean those persons or entities that have a contract with Participant to provide Participant with products or services.

3.10. Rights in Products. Participant shall not assert and shall not have any ownership rights or other property rights in any of HIE's Standards, the Clinical Messaging System or any information or materials furnished by HIE to Participant. Participant agrees that the parties from whom HIE licenses the software products and related documentation ("Products") which may be used in the Clinical Messaging System, own all right, title and interest in such Products. Participant will not delete or in any manner alter the copyright, trademark or other proprietary rights or notices of the parties from whom HIE licenses the Products or from HIE appearing on the Products as delivered to Participant. Participant will reproduce such notices on all copies it makes of the Products. Participant will treat this Agreement, source codes and other business and technical information relating to the Products and relating to HIE's Standards or the Clinical Messaging System as confidential information and will not disclose the same except as may be required under applicable law or as may be necessary to perform its duties and obligations under this Agreement.

3.11. HIE Right to Access. Participant shall give HIE access at all reasonable times to its computer hardware and software used in the operation of the Clinical Messaging System for purposes of HIE ensuring that the System is operating properly, and for performance of needed maintenance and upgrades.

4. Confidentiality and Privacy.

4.1. Permitted Uses and Disclosures of PHI by HIE. The scope of PHI that may be Used, Disclosed, or accessed and/or the functions performed by HIE includes PHI necessary to perform functions required by this Agreement. HIE will not Use, Disclose, or access PHI in violation of any applicable Information Privacy and Protection Laws. HIE further agrees to not Use or further Disclose PHI other than as permitted or required by this Agreement or by law. HIE shall comply with the requirements of HITECH applicable to HIE as a Business Associate.

4.2. Access to Records. To the extent HIE has possession of PHI in a Designated Record Set, HIE agrees to provide access, at the request of Participant to PHI in a Designated Record Set to Participant (but not to an Individual) as may be necessary to meet the requirements under 45 CFR 164.524.

4.3. Accounting for Disclosure of Records. HIE shall maintain an accounting or record of all Disclosures of PHI it makes only as required by and in accordance with 45 C.F.R164.528. Records of Disclosures shall be retained by HIE for a period of time that complies with HIPAA and other applicable federal or state law requirements pertaining to record retention. The record of the Disclosure shall include the following information: (a) the date of the Disclosure, (b) the name and address of the organization and/or individual receiving the information; (c) a brief description of the information Disclosed; and (d) a copy of all requests for Disclosures. HIE agrees to provide to Participant (but not an Individual), in the time and manner designated by Participant, information collected in accordance with this section, to permit Participant to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR164.528.

4.4. Mitigation. HIE agrees to mitigate, to the extent practicable, any harmful effect that is known to HIE of a Use or Disclosure of PHI by HIE in violation of the requirements of this Agreement.

4.5. Safeguards and Security Incidents. At all times following the Receipt of PHI, until such time as the PHI is no longer in HIE's possession or subject to its control:

4.5.1. HIE shall implement administrative, physical, and technical safeguards, as required by the Security Rule, that reasonably and appropriately protect the confidentiality, integrity and availability of PHI that it Receives, maintains, or Transmits on behalf of Participant. Such administrative, physical, and technical safeguards shall be implemented in order to prevent any Use or Disclosure of PHI other than those permitted under this Agreement;

4.5.2. HIE shall notify Participant of any Use or Disclosure of PHI not permitted by or contrary to the terms of this Agreement of which HIE becomes aware;

4.5.3. HIE shall notify Participant of any security incident of which it becomes aware;

4.5.4. HIE shall comply with the requirements of the Information Privacy and Protection Laws in order to notify Participant of any Breach of unsecured PHI following the discovery of such Breach. In any event, such notice will be provided without unreasonable delay and in no case later than the time required by Information Privacy and Protection Laws for providing such notice. Such notice shall include the identification of each Individual whose unsecured protected health information has been, or is reasonably believed by HIE to have been, accessed, acquired or disclosed during such Breach. HIE and Participant will cooperate with each other with regard to reporting of such a Breach if such reporting is required by law.

4.6. Disclosure of PHI to Third Parties. HIE may not Disclose PHI to third parties except under the following conditions:

4.6.1. The Disclosure is of the "minimum necessary" (as that term is defined in HIPAA) information for the purposes of the Disclosure, if such standard is required by applicable law; and

4.6.2. The Disclosure is necessary to accomplish a purpose for which the PHI was Disclosed to the Receiving party and is permitted under applicable Information Privacy and Protection Laws and this Agreement. For purposes of this Agreement, a Participant or Participant User's access and Use of the Clinical Messaging System shall not be considered a Disclosure of PHI by HIE under this Agreement.

4.7. Subcontractors. HIE agrees to ensure that any agent or subcontractor of HIE agrees to the same restrictions and conditions as regards PHI that apply to HIE throughout this Agreement when such agents or subcontractors are performing any of the tasks, duties, or obligations required of HIE by this Agreement.

4.8. Auditing of Records. HIE agrees to make its internal practices, books, and records relating to its access to, Use, and Disclosure of PHI received from or on behalf of Participant or created by HIE on behalf of Participant available to Participant or, at the request of Participant, to the U.S. Secretary of the Department of Health and Human Services ("Secretary") in a time and manner designated by Participant or the Secretary for purposes of determining compliance with Information Privacy and Protection Laws.

4.9. Compliance with Law and Agreement. Each party to this Agreement shall comply with, and as applicable shall require its directors, officers and employees to comply with, all applicable Information Privacy and Protection Laws and with each party's duties and obligations pursuant to this Agreement.

4.10. Incorporation of Additional Requirements; Construction. The requirements of applicable law pertaining to PHI are, to the extent not adequately provided for in this Agreement, hereby incorporated by this reference and shall become a part of this Agreement. This Agreement shall be construed as broadly as necessary to implement and comply with Information Privacy and Protection Laws.

5. Termination.

5.1. Unilateral Termination. This Agreement may be terminated by HIE or Participant with or without cause on at least sixty (60) days' prior written notice to the other party.

5.2. Participant's Right to Termination.

5.2.1. Participant may terminate this Agreement upon thirty (30) days' prior written notice to HIE should HIE's Standards change regarding Use of the Clinical Messaging System in a manner that Participant reasonably believes lessens the safeguards on accessing the data that is available through Use of the Clinical Messaging System.

5.2.2. Participant may terminate this Agreement upon thirty (30) days' prior written notice to HIE should HIE change the fees referenced on attached Exhibit___. Notice of termination under this subparagraph must be given by Participant within thirty (30) days of HIE changing the fees.

5.3. Termination for Material Breach. Notwithstanding anything to the contrary in this Agreement, upon gaining knowledge of a material breach of the terms of this Agreement by a party to this Agreement, the non-breaching party may, but need not, at its sole discretion:(1) if

the breach cannot be cured, terminate this Agreement upon thirty (30) days written notice to the breaching party without any judicial intervention being required and without liability for such termination; or (2) if the breach can be cured, provide at least ten (10) business days written notice of the breach to the breaching party and the opportunity to cure the same within the ten (10) day period or be subject to termination of this Agreement within thirty (30)days.

5.4. HIE's Right to Termination/Suspension.

5.4.1. HIE may terminate this Agreement upon written notice to Participant should HIE determine or become aware that: (1) Participant or Participant Users have not complied with HIE's Standards, Information Privacy and Protection Laws or requirements of applicable law with regard to Use of the Clinical Messaging System and fail to cure such noncompliance within ten (10) business days after receiving notice of such noncompliance from HIE; (2)Participant's license to provide healthcare services is terminated or suspended; or (3) Participant has engaged in any pattern or practice that would constitute a violation of this Agreement and Participant fails to discontinue such conduct within ten (10) business days after receiving notice of such noncompliance from HIE.

5.4.2. HIE may terminate this Agreement upon written notice to Participant if Participant fails to pay amounts owed to HIE when due, and such failure to pay continues for thirty (30) days after written notice from HIE.

5.4.3. HIE may also immediately suspend a Participant or Participant User's access to the Clinical Messaging System, without terminating this Agreement, pursuant to terms of HIE's Standards.

5.5. Participant Rights Upon Termination. Upon termination of this Agreement, Participant shall have the right to have HIE remove any and all of Participant's data residing within the System, excepting only demographic data and such other data rightfully transferred to and residing in one or more discrete work group database(s) assigned to some other HIE Participant, or in the virtual health record, prior to the date of Participant's request for removal. The provisions of paragraph 4 of this Agreement shall survive termination of this Agreement and continue to apply to Participant's data not removed from the Clinical Messaging System. Upon notice of termination for reasons other than termination by HIE under paragraph 5.3 or paragraph 5.4.1 of this Agreement, HIE and Participant shall agree upon a reasonable time (not to exceed one hundred eighty (180) days from the effective date of termination), terms and conditions within which Participant may continue Use of the Clinical Messaging System. During this time period, Participant may continue Use of the Clinical Messaging System in accordance with this Agreement, and the parties shall be subject to all terms of this Agreement and any agreement between the parties regarding the termination, including payment of all amounts that may be owed to HIE.

6. General Provisions.

6.1. Compliance with Law. HIE, Participant and each Participant User shall comply with applicable Federal and State laws regarding Use of the Clinical Messaging System. This Agreement shall be interpreted to the maximum extent possible as being consistent with such laws.

6.2. Independent Contractor. This Agreement is intended to create the relationship of independent contractor between Participant and HIE. Nothing contained herein shall be interpreted to create any relationship of agency, employment, partnership or joint venture

between HIE and Participant. Neither party shall represent or hold themselves out to any person or entity other than is consistent with the relationship of independent contractor.

6.3. Entire Agreement. This Agreement, and the Exhibit___ attached to this Agreement, constitute the entire understanding and agreement of the parties, and shall supersede all prior understandings and agreements of the parties on the subject matter of this Agreement.

6.4. Amendment. Except as otherwise set forth in this Agreement, this Agreement shall not be changed, modified or altered except by amendment, which, to be valid and enforceable, shall be in writing and signed by the parties. Notwithstanding the foregoing, HIE may unilaterally amend this Agreement in order to comply with any applicable federal or state laws or regulations, including but not limited to Information Privacy and Protection Laws, effective immediately upon written notice to the Participant, and may otherwise amend the terms of this Agreement effective upon ninety(90) days prior written notice to the Participant. Participant's Use of the Clinical Messaging System after the effective date specified in such notice shall constitute acceptance of the amendment. Notwithstanding the foregoing, HIE's Standards may by modified as provided in this Agreement.

6.5. Notices. Either party may send any notices required pursuant to this Agreement, except notices of termination and notices regarding indemnity obligations, by first class mail, electronic transmission, certified mail or a recognized overnight delivery service, to the last known physical or electronic address for Participant in HIE's records. All termination notices under this Agreement by either party, and all notices regarding indemnity obligations, shall be made in writing and sent via certified mail, return receipt requested, or a recognized overnight delivery service, to the addresses of the parties set forth above.

6.6. Assignment. Neither party's rights, duties and responsibilities pursuant to this Agreement may be assigned or delegated without the prior written consent of the other party, except for a transfer or assignment to apparent, subsidiary or affiliate or an entity with which it is merged or consolidated, or the purchaser of all or substantially all of its assets provided that the transferee assumes all of its obligations under this Agreement.

6.7. Severability. If any provision of this Agreement is held to be invalid or unenforceable, the remaining provisions shall continue in full force and effect, unless the invalid or unenforceable provision is material to this Agreement and its invalidity or unenforceability results in substantial economic detriment to either party to this Agreement.

6.8. Governing Law. This Agreement shall be governed by the laws of the participating state.

6.9. Benefit. The terms and provisions of this Agreement shall bind and benefit Participant and permitted assigns, and shall bind and benefit HIE and its permitted assigns. There shall be no third party beneficiaries of this Agreement.

6.10. Interpretation. Any ambiguity or inconsistency in this Agreement shall be resolved in favor of a meaning that permits both parties to comply with applicable laws.

F.4 Public Entity to Private Entity Business Agreement (marked version)

Master Agreement/Contract

("Agreement")

"PARTICIPANT"

This agreement is designed specifically for use between private and public entities, and should be supplemented with BAAs to provide additional leverage. There is a great deal in this agreement to explicitly protect each party. As written, this agreement is akin to that needed by a "mail service". It may also be necessary to adjust terms to reflect the "pure switch" vs. "hybrid switch option".

_____

_____

Address of Participant

_____

_____

Tax I.D. No.:

"HIE" Health Information Exchange

Address of HIE:

RECITALS

A. HIE provides a Clinical Messaging System, as hereinafter defined, to improve the quality of health care in the community and to enhance health care providers' ability to exchange electronic data. HIE may also provide other products or services from time to time.

Pure switch vs. hybrid issue here

B. Participant is a PMP [or interstate data Hub] which HIE has agreed to accept for enrollment. Participant desires to Use the Clinical Messaging System provided by HIE for purposes of promoting the improvement of health care treatment, payment and operations.

This was added to account for PMPi or similar – and it may be necessary to insert the definition of an alternate entity. The role of that entity may be very important to terms (i.e., blind pipe vs. hybrid)

C. In order to send or receive data through the HIE Clinical Messaging System, Participant must first make various covenants, warranties and representations to HIE, as hereinafter set forth, concerning the Use of the Clinical Messaging System and related tools and services. In providing the Clinical Messaging System and related tools and services to Participant, HIE must first make various covenants, warranties, and representations to Participant as hereinafter set forth.

D. The relationship between HIE and Participant created under the terms of this Agreement results in HIE's classification as a "Business Associate" under HIPAA. The HIPAA regulations

require Participant to enter agreements that include certain mandated provisions, which are included as part of this Agreement, with all vendors and contractors that are classified as "Business Associates."

NOW, THEREFORE, in consideration of the recitals set forth above and the mutual promises set forth below, the parties agree as follows:

A. Services. HIE will manage and administer the Clinical Messaging System and its Use. So long as this Agreement is in effect and Participant and Participant Users comply with all terms of this Agreement, HIE will provide Participant and Participant Users access to Use the Clinical Messaging System. HIE and Participant agree to all Terms and Conditions, attached.

B. Fees. Participant agrees to pay HIE the amounts referenced on attached Exhibit___, along with applicable taxes, associated with various Uses of the Clinical Messaging System as required by the Order and Invoice. Any amounts not paid when due shall bear interest at the rate of eighteen percent (18%) per annum. Participant agrees that payment amounts and the interest rate are subject to change upon sixty (60) days written notice to Participant from HIE, subject to Participant's right to terminate the Agreement as provided herein. HIE may refuse Participant and Participant Users access to Uses of the Clinical Messaging System if payment is not timely made by Participant.

C. Addendums

Any addendums, such as BAAs, would be here

This Agreement is dated and shall be effective on the date set forth below by HIE as the effective date.

SIGNATURE PAGE BETWEEN PARTICIPANT AND HIE

Effective Date _____

TERMS AND CONDITIONS:

1. Definitions. Terms used but not otherwise defined in this Agreement shall have the same meaning as those terms in 45 C.F.R. 160.103 and 164.501. All terms defined in this Agreement shall have a meaning consistent with terms defined in 45 C.F.R. 160.103 and 164.501. Capitalized terms in this Agreement are defined as follows:

1.1 "Board of Directors" shall mean the Board of Directors of HIE.

In some cases, it will not have such a body, and then this shall be removed

1.2. "Breach" shall mean the unauthorized acquisition, access, use, or disclosure of PHI as defined in Section 13400 of HITECH and 45 C.F.R. 164.402.

1.3. "Business Associate" shall mean a person or entity who performs a function for or assists a Covered Entity or organized health care arrangement with the performance of a function or activity involving the use or disclosure of PHI. Examples of functions include, but are not limited to: data analysis, consulting, data aggregation, management, administrative or financial services. The provision of the service involves the disclosure of PHI from the Covered Entity or organized health care arrangement, or from another Business Associate of the Covered Entity or organized health care arrangement, to the person or entity.

1.4. “Clinical Messaging System” or “System” shall mean the technology tools, services and systems HIE provides and/ or maintains.

1.5. “Covered Entity” shall mean a Participant in the Clinical Messaging System that meets the definition of a Covered Entity under HIPAA.

1.6. “De-identification” shall mean to remove, encode, encrypt, or otherwise eliminate or conceal data which identifies an Individual, or modifies information so that there is no reasonable basis to believe that the information can be used to identify an Individual. De-identification includes, without limitation, any process meeting the requirements for De-identification set forth in 45 C.F.R. § 164.514, as such provision is currently drafted and as it may be subsequently updated, amended, or revised.

1.7. “Designated Record Set” means Protected Health Information maintained by or for Participant that is: (1) the medical records and billing records about Individuals maintained by or for a covered health care provider; (2) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (3) used, in whole or in part, by or for Participant to make decisions about Individuals.

Note that this definition is broader than a limited data set, and intentionally so

1.8. “Disclose,” “Disclosing,” or “Disclosure” means the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information.

1.09. “HITECH” means the Health Information Technology for Economic and Clinical Health Act in the American Recovery and Reinvestment Act of 2009, including any implementing regulations.

1.10. “Individual” means a natural person who is the subject of PHI.

1.11. “Information Privacy and Protection Laws” mean (i) the Health Insurance Portability and Accountability Act of 1996, as amended and including any implementing regulations (“HIPAA”); (ii) HITECH; (iii) the Gramm-Leach-Bliley Act, as amended and including any implementing regulations; (iv) any statute, regulation, administrative or judicial ruling requiring a party to protect the privacy or security of information pertaining to the health or medical status or condition of an Individual, and/or the payment for health or medical care for an Individual; (v) any statute, regulation, administrative or judicial ruling requiring a party to protect the privacy of information pertaining to the financial or credit status or condition of an individual; (vi) any statute, regulation, administrative or judicial ruling requiring a party to protect information pertaining to individuals based upon the individuals’ status as consumers; and (vii) any other statute, regulation, administrative or judicial ruling requiring a party to protect the confidentiality, privacy and/or security of information pertaining to individuals; all to the extent that such Information Privacy and Protection Laws have been enacted, promulgated, issued or published by any federal or state governmental authority with jurisdiction over an individual, a Participant or HIE.

Note that this might be supplemented by more commentary regarding relevant state privacy laws

1.12. “Message Content” shall mean that information which is requested or sent by a Participant to another user of the Clinical Messaging System through the HIE, including but not limited to, PHI, individually identifiable information, de-identified data, pseudonymized data, metadata, digital certificates issued by HIE to any Participant, and schema.

1.13. “Network Account” shall mean the right given to Participant to access and Use the Clinical Messaging System by Participant and Participant Users.

1.14. “Participant User” shall mean any person accepted by HIE and who is authorized to use the Clinical Messaging System through Participant’s right of Use set forth in this Agreement. Participant shall designate Participant Users.

1.15. “Protected Health Information,” or “PHI,” means any information that identifies or could reasonably be used to identify an Individual, which in any way concerns that Individual’s health status, health care, or payments for his or her health care, or which a party is otherwise legally required to protect under an Information Privacy and Protection Law applicable to that party, and includes as well any information derived by the processing of such information that is not De-Identified with respect to any Individual who is the subject of the information.

1.16. “HIE’s Standards” shall mean those standards, policies and procedures adopted by the Board of Directors and subject to revision, modification or change by the Board of Directors, which address requirements and standards with regard to Use of the Clinical Messaging System. HIE’s Standards may include, but are not limited to: activity on the System, operating rules, definitions and specifications of format, content, and transmission of electronic data, support descriptions and details of connecting to the System.

1.17. “Receive,” “Receiving,” and “Receipt” means (i) to take physical delivery of media containing information, or (ii) in the case of electronic delivery, for information to come into existence in a party’s information processing system in a form capable of being processed by or perceived from a system of that type by the Receiving party if the Receiving party has designated that system or address as a place for Receipt of information to a Disclosing party and the Disclosing party does not know that the information cannot be accessed from the particular system.

1.18. “Security Rule” means the Security Standards for Protection of Electronic Protected Health Information at 45 C.F.R. Part 164, Subpart C.

1.19. “Third Party” means any individual, person, or organization not a party to this Agreement.

1.20. “Transaction” means the Transmission of information between parties to this Agreement.

1.21. “Transmit,” “Transmitted,” or “Transmission” means the transfer of information by one party to another, regardless of the method or technology used to transfer the information.

1.22. “Use” shall mean the sharing, employment, application, utilization, examination, analysis, De-identification, or commingling with other information, of information by a party that holds that information.

2. Duties and Obligations of HIE.

2.1. Training. HIE will provide training for Participant and Participant Users as regards the Clinical Messaging System in accordance with a reasonable schedule that will be mutually agreed to by the parties.

2.2. Use of Clinical Messaging System. HIE will provide Participant and Participant Users products and services and access to the Uses of the Clinical Messaging System described on Exhibit___ provided such Use is consistent with HIE’s Standards. HIE shall furnish each Participant User a unique identification method (i.e., login, password, PIN, etc.) with which each Participant User will be able to initially access and Use the Clinical Messaging System. Participant User shall change the initial password they receive immediately after initial login to

the System. The Participant User shall not share the Participant User's password or any other security measures issued to the Participant User by HIE with any person. All access to the System shall use full SSL security, message tracing and message acknowledgement. [Participant authorizes HIE to use data within the Clinical Messaging System for quality improvement programs, practice management and research provided that such use is consistent with HIE's Standards and requirements of applicable law, including, but not limited to the Information Privacy and Protection Laws.]

This area may be subject to supplementation by state PMP privacy laws for authorized users and non-operational (research) use. Note that the highlighted section is outside the TPO scope, and as such is optional. Participant numbers may impact security issue. We could also call out specifics here instead of having an exhibit. Will anything done outside PMP operational uses (e.g., research) come back to benefit the PMP?

2.3. Data Storage and Distribution. Data within the Clinical Messaging System will be available to Participant Users pursuant to HIE's Standards and subject to compliance with applicable laws. The Uses of the Clinical Messaging System that are provided to Participant Users are described on Exhibit___.

Sections 2.3 and 2.4 will be impacted by the "blind" vs. "hybrid issue"

2.4. Data Backup. HIE shall make available requisite disk space for the storage of software and data as may be required for HIE, as a Business Associate, to comply with applicable law, but in any event there shall be available sufficient disk space to permit Participants to retain an estimated five (5) years of clinical data, or as required to comply with applicable law. If HIE and Participant dispute whether a Participant's use is "normal use" the parties shall resolve such disputes in accordance with paragraph 5 of this Agreement. Tape backups will be regularly performed and stored in a secured off-site location.

Some believe that this section may be confusing, and might be removed

2.5. Inquiries from Individuals. Should HIE receive from an Individual a request for data specific to such Individual, which data the Individual believes is contained in the Clinical Messaging System, HIE shall redirect the Individual to the health care provider from whom the Individual received the services which the data references. HIE will not provide medical record data or other information stored within the Clinical Messaging System to such Individuals other than as required by law.

2.6. Right to Audit. HIE shall have the right to audit Participant's and Participant Users' Use of the Clinical Messaging System to ascertain compliance with HIE's Standards and applicable law with regard to Use of the Clinical Messaging System. The results of such audits shall be shared with Participant and the HIE Board of Directors.

2.7. Right to Impose Sanctions. HIE shall have the right to impose sanctions as described in HIE's Standards on a Participant User should Participant User's Use of the Clinical Messaging System be in violation of the terms of this Agreement or HIE's Standards.

2.8. Liability Insurance. HIE shall purchase and/or maintain liability insurance or a self-insurance plan which provides coverage to HIE of not less than one million dollars ($1,000,000) per incident per year for any claims arising from or in connection with the provision of services under this Agreement.

It was noted that this section could also fall into the "as applicable and appropriate" (aka, optional depending on circumstances) category, and may additionally be handled in some cases through the posting of a bond instead of purchasing insurance

2.9. Indemnity. HIE agrees to indemnify Participant from any and all claims, demands, actions, and causes of action asserted by a third party against Participant which may result or arise out of any actions or omissions of HIE or any of HIE's agents, employees, or representatives due to HIE's failure to comply with privacy or security obligations under this Agreement or imposed by law or HIE's failure to comply with the terms of this Agreement. This indemnity shall include the payment to Participant for attorney's fees, court costs and expert witness fees Participant incurs in defending itself from any such claims, demands, actions or cause of action. For this indemnity obligation to apply, Participant shall (a) provide HIE notice in writing upon the discovery of the claim, (b) fully cooperate with HIE in the defense of the claim, and (c) not settle the claim without the prior written consent of HIE, which consent shall not be unreasonably withheld. If there is a Breach by HIE and/or HIE's agents or subcontractors in the course of HIE providing services to Participant and Participant is required by law to notify the involved Individual(s) of whom such Breach pertains and/or any governmental entity as may be required by law, HIE shall pay all Participant's reasonable notification costs and, as mutually agreed by the parties, reasonable costs associated with mitigating any harmful effects of such Breach. For purposes of this paragraph, a HIE agent or subcontractor shall mean those persons or entities that have a contract with HIE to provide HIE with products or services. HIE's liability under this paragraph shall not exceed the greater of coverage for such liability as may be provided by insurance held by HIE or the total amount paid by Participant to HIE to obtain services under this Agreement for the twelve (12) month period preceding the date such liability arose.

2.10. DISCLAIMER. HIE MAKES NO WARRANTIES, EXPRESS OR IMPLIED, WITH REGARD TO THE CLINICALMESSAGING SYSTEM, INCLUDING BUTNOT LIMITED TO, ANY WARRANTY OFNONINFRINGEMENT, OR THE IMPLIEDWARRANTY OF MERCHANTABILITYAND FITNESS FOR A PARTICULARPURPOSE REGARDLESS OF THESERVICES OR RESOURCES PROVIDED BYIT. HIE DISCLAIMS ANY LIABILITY FORTHE FAILURE OF PERSON WHO USESTHE CLINCIAL MESSAGING SYSTEM TOCOMPLY WITH HIE'S STANDARDS ORAPPLICABLE LAW OR THE CONTENT ORUSE OF THE CLINICAL MESSAGINGSYSTEM BY ANY SUCH PERSON. HIEDOES NOT WARRANT UNINTERRUPTEDOR ERROR FREE OPERATION OF THECLINICAL MESSAGING SYSTEM OR THECOMPATIBILITY OF THE CLINICALMESSAGING SYSTEM WITH ANYPARTICULAR HARDWARE, SOFTWAREOR INTER-CONNECTIVITY WITH OTHERNETWORKS OR SERVICES.

2.11. LIMITATION OF LIABILITY.EXCEPT FOR HIE'S LIABILITYOBLIGATIONS AS EXPRESSLY SETFORTH IN THE INDEMNITY PARAGRAPHOF THIS AGREEMENT, REGARDLESS OFWHETHER ANY REMEDY FAILS OF ITSESSENTIAL PURPOSE, THE MAXIMUMLIABILITY OF HIE UNDER THISAGREEMENT SHALL NOT EXCEED THETOTAL AMOUNT PAID BY PARTICIPANTTO HIE TO OBTAIN SERVICES UNDERTHIS AGREEMENT FOR THE TWELVE (12) MONTH PERIOD PRECEDING THEDATE THE LIABILITY AROSE. IN NOEVENT SHALL HIE BE LIABLE FORSPECIAL, INCIDENTAL, CONSEQUENTIAL, OR EXEMPLARYDAMAGES INCLUDING WITHOUTLIMITATION, LOST DATA OR LOSTPROFITS.

3. Duties and Obligations of Participant.

3.1. Assistance and Cooperation with HIE in Providing Products and Services. Participant, at its sole cost and expense, shall cooperate and work in good faith with HIE to assist HIE in working with Participant to provide the products and services described in Exhibit___.

Could also call out specifics here

3.2. Complying with HIE's Standards In Use of Clinical Messaging System. In Using the Clinical Messaging System, Participant shall Use the System in a manner consistent with and shall comply with HIE's Standards and applicable law. Participant specifically agrees to comply with and to be subject to HIE's Standards. HIE's Standards are subject to amendment, revision and modification by the Board of Directors solely in its discretion. Changes to HIE's Standards may reflect changes in applicable law or the need to adopt new technologies, systems, or desired functionality or changes in HIE's operational policies. Participant is encouraged to provide input to HIE's Standards and to propose changes. Copies of all HIE's Standards may be reviewed upon request.

This makes it easier to unilaterally change the terms to ensure continuing compliance with shifting standards without experiencing the large overhead cost of renegotiating multiple agreements

3.3 Participant Responsibility for Data. HIE provides tools for Participant Users to use the Clinical Messaging System but does not act in any other way for Participant or any other person or entity that Uses the Clinical Messaging System. HIE is not responsible for and does not inspect the contents of data that any Participant or any other persons or entity places in or obtains from the Clinical Messaging System. Participant's decision to place certain data in and Use the Clinical Messaging System is based on Participant's sole discretion. By placing an Individual's PHI in the Clinical Messaging System, Participant is certifying to HIE that such PHI can be Disclosed to Covered Entities for purposes of health care treatment. To the maximum extent permitted by applicable law, as between Participant and HIE, Participant is solely responsible for establishing the connection to the Clinical Messaging System, the proper transmission and receipt of data, for implementing sufficient safeguards and procedures to satisfy particular requirements for security, privacy and accuracy of data placed in or transmitted by Participant in Using the Clinical Messaging System. Backup of data located on Participant's own computer components is Participant's responsibility; HIE will backup data on the Clinical Messaging System as described in paragraph 2.4 of this Agreement.

3.4. Contact Information. Participant agrees to notify HIE in writing as soon as possible as to any change in status of a Participant User. Participant is responsible to provide HIE with the most current name and contact information for Participant and all Participant Users.

3.5. Training of Staff. Compliance with applicable federal and state laws, rules and regulations concerning adequate training of staff is the sole responsibility of the Participant.

3.6. Resources. Except as otherwise provided by Exhibit__, Participant, at Participant's own expense, shall provide and maintain necessary hardware, software, equipment and services necessary to Use the Clinical Messaging System. In addition to the services described in Exhibit__, HIE may provide services as ancillary services, but such services would be performed under the terms of a separate addendum or agreement (an "Order "as defined in Exhibit___) between HIE and Participant. Support services which may be available under the terms of a separate addendum or agreement include: (a) help desk services during business hours and limited holiday and weekend hours, and (b) onsite support services at Participant's location.

3.7. Responsibility for Network Account. Participant shall be solely responsible for all Use of its Network Account, for payment of charges incurred for such Use, and for violations of the terms of this Agreement by anyone using the Network Account.

3.8. Warranties with Use. By its Use of the Clinical Messaging System, Participant warrants (1) that Participant's and Participant Users' Use is in compliance with the terms of this Agreement, and (2) that Participant's and Participant Users' Use is in compliance with applicable law.

3.9. Indemnity. Participant agrees to indemnify HIE and hold HIE harmless from any and all claims, demands, actions, and causes of action asserted by a third party against HIE which may result or arise out of any actions of Participant or any Participant User who becomes an authorized user through this Agreement or any Use through Participant's Network Account. This indemnity shall include the payment to HIE for attorney's fees, court costs and expert witness fees HIE incurs in defending itself from any such claims, demands, actions or cause of action. For this indemnity obligation to apply, HIE shall (a) provide Participant notice in writing upon the discovery of the claim, (b) fully cooperate with Participant in the defense of the claim, and (c) not settle the claim without the prior written consent of Participant, which consent shall not be unreasonably withheld. If there is a Breach by Participant and/or Participant's agents or subcontractors in the course of HIE providing services to Participant and HIE is required by law to notify the involved Individual(s) of whom such Breach pertains and/or any governmental entity as may be required by law, Participant shall pay all HIE's reasonable notification costs and, as mutually agreed by the parties, reasonable costs associated with mitigating any harmful effects of such Breach. For purposes of this paragraph, a Participant agent or subcontractor shall mean those persons or entities that have a contract with Participant to provide Participant with products or services. [If Participant has insurance coverage for its obligations under this paragraph and such insurance coverage provides at least one million dollars ($1,000,000) of coverage for such obligations, then the Participant's liability under this paragraph shall not exceed the total of such insurance coverage provided for its obligations.]

This was addressed earlier as well, and in any case is an optional call-out

3.10. Rights in Products. Participant shall not assert and shall not have any ownership rights or other property rights in any of HIE's Standards, the Clinical Messaging System or any information or materials furnished by HIE to Participant. Participant agrees that the parties from whom HIE licenses the software products and related documentation ("Products") which may be used in the Clinical Messaging System, own all right, title and interest in such Products. Participant will not delete or in any manner alter the copyright, trademark or other proprietary rights or notices of the parties from whom HIE licenses the Products or from HIE appearing on the Products as delivered to Participant. Participant will reproduce such notices on all copies it makes of the Products. Participant will treat this Agreement, source codes and other business and technical information relating to the Products and relating to HIE's Standards or the Clinical Messaging System as confidential information and will not disclose the same except as may be required under applicable law or as may be necessary to perform its duties and obligations under this Agreement.

3.11. HIE Right to Access. Participant shall give HIE access at all reasonable times to its computer hardware and software used in the operation of the Clinical Messaging System for purposes of HIE ensuring that the System is operating properly, and for performance of needed maintenance and upgrades.

4. Confidentiality and Privacy.

4.1. Permitted Uses and Disclosures of PHI by HIE. The scope of PHI that may be Used, Disclosed, or accessed and/or the functions performed by HIE includes PHI necessary to perform functions required by this Agreement. HIE will not Use, Disclose, or access PHI in violation of any applicable Information Privacy and Protection Laws. HIE further agrees to not Use or further Disclose PHI other than as permitted or required by this Agreement or by law. HIE shall comply with the requirements of HITECH applicable to HIE as a Business Associate.

4.2. Access to Records. To the extent HIE has possession of PHI in a Designated Record Set, HIE agrees to provide access, at the request of Participant to PHI in a Designated Record Set to Participant (but not to an Individual) as may be necessary to meet the requirements under 45 CFR 164.524.

4.3. Accounting for Disclosure of Records. HIE shall maintain an accounting or record of all Disclosures of PHI it makes only as required by and in accordance with 45 C.F.R164.528. Records of Disclosures shall be retained by HIE for a period of time that complies with HIPAA and other applicable federal or state law requirements pertaining to record retention. The record of the Disclosure shall include the following information: (a) the date of the Disclosure, (b) the name and address of the organization and/or individual receiving the information; (c) a brief description of the information Disclosed; and (d) a copy of all requests for Disclosures. HIE agrees to provide to Participant (but not an Individual), in the time and manner designated by Participant, information collected in accordance with this section, to permit Participant to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR164.528.

4.4. Mitigation. HIE agrees to mitigate, to the extent practicable, any harmful effect that is known to HIE of a Use or Disclosure of PHI by HIE in violation of the requirements of this Agreement.

Generic security breach language

4.5. Safeguards and Security Incidents. At all times following the Receipt of PHI, until such time as the PHI is no longer in HIE's possession or subject to its control:

4.5.1. HIE shall implement administrative, physical, and technical safeguards, as required by the Security Rule, that reasonably and appropriately protect the confidentiality, integrity and availability of PHI that it Receives, maintains, or Transmits on behalf of Participant. Such administrative, physical, and technical safeguards shall be implemented in order to prevent any Use or Disclosure of PHI other than those permitted under this Agreement;

4.5.2. HIE shall notify Participant of any Use or Disclosure of PHI not permitted by or contrary to the terms of this Agreement of which HIE becomes aware;

4.5.3. HIE shall notify Participant of any security incident of which it becomes aware;

4.5.4. HIE shall comply with the requirements of the Information Privacy and Protection Laws in order to notify Participant of any Breach of unsecured PHI following the discovery of such Breach. In any event, such notice will be provided without unreasonable delay and in no case later than the time required by Information Privacy and Protection Laws for providing such notice. Such notice shall include the identification of each Individual whose unsecured protected health information has been, or is reasonably believed by HIE to have been, accessed, acquired or disclosed during such Breach. HIE and Participant will cooperate with each other with regard to reporting of such a Breach if such reporting is required by law.

4.6. Disclosure of PHI to Third Parties. HIE may not Disclose PHI to third parties except under the following conditions:

4.6.1. The Disclosure is of the "minimum necessary" (as that term is defined in HIPAA) information for the purposes of the Disclosure, if such standard is required by applicable law; and

4.6.2. The Disclosure is necessary to accomplish a purpose for which the PHI was Disclosed to the Receiving party and is permitted under applicable Information Privacy and Protection Laws and this Agreement. For purposes of this Agreement, a Participant or Participant User's access and Use of the Clinical Messaging System shall not be considered a Disclosure of PHI by HIE under this Agreement.

4.7. Subcontractors. HIE agrees to ensure that any agent or subcontractor of HIE agrees to the same restrictions and conditions as regards PHI that apply to HIE throughout this Agreement when such agents or subcontractors are performing any of the tasks, duties, or obligations required of HIE by this Agreement.

4.8. Auditing of Records. HIE agrees to make its internal practices, books, and records relating to its access to, Use, and Disclosure of PHI received from or on behalf of Participant or created by HIE on behalf of Participant available to Participant or, at the request of Participant, to the U.S. Secretary of the Department of Health and Human Services ("Secretary") in a time and manner designated by Participant or the Secretary for purposes of determining compliance with Information Privacy and Protection Laws.

4.9. Compliance with Law and Agreement. Each party to this Agreement shall comply with, and as applicable shall require its directors, officers and employees to comply with, all applicable Information Privacy and Protection Laws and with each party's duties and obligations pursuant to this Agreement.

4.10. Incorporation of Additional Requirements; Construction. The requirements of applicable law pertaining to PHI are, to the extent not adequately provided for in this Agreement, hereby incorporated by this reference and shall become a part of this Agreement. This Agreement shall be construed as broadly as necessary to implement and comply with Information Privacy and Protection Laws.

5. Termination.

5.1. Unilateral Termination. This Agreement may be terminated by HIE or Participant with or without cause on at least sixty (60) days' prior written notice to the other party.

It was noted that 60 days was comparatively generous

5.2. Participant's Right to Termination.

5.2.1. Participant may terminate this Agreement upon thirty (30) days' prior written notice to HIE should HIE's Standards change regarding Use of the Clinical Messaging System in a manner that Participant reasonably believes lessens the safeguards on accessing the data that is available through Use of the Clinical Messaging System.

5.2.2. Participant may terminate this Agreement upon thirty (30) days' prior written notice to HIE should HIE change the fees referenced on attached Exhibit___. Notice of termination under this subparagraph must be given by Participant within thirty (30) days of HIE changing the fees.

5.3. Termination for Material Breach. Notwithstanding anything to the contrary in this Agreement, upon gaining knowledge of a material breach of the terms of this Agreement by a party to this Agreement, the non-breaching party may, but need not, at its sole discretion:(1) if the breach cannot be cured, terminate this Agreement upon thirty (30) days written notice to the breaching party without any judicial intervention being required and without liability for such termination; or (2) if the breach can be cured, provide at least ten (10) business days written notice of the breach to the breaching party and the opportunity to cure the same within the ten (10) day period or be subject to termination of this Agreement within thirty (30)days.

5.4. HIE's Right to Termination/Suspension.

5.4.1. HIE may terminate this Agreement upon written notice to Participant should HIE determine or become aware that: (1) Participant or Participant Users have not complied with HIE's Standards, Information Privacy and Protection Laws or requirements of applicable law with regard to Use of the Clinical Messaging System and fail to cure such noncompliance within ten (10) business days after receiving notice of such noncompliance from HIE; (2)Participant's license to provide healthcare services is terminated or suspended; or (3) Participant has engaged in any pattern or practice that would constitute a violation of this Agreement and Participant fails to discontinue such conduct within ten (10) business days after receiving notice of such noncompliance from HIE.

5.4.2. HIE may terminate this Agreement upon written notice to Participant if Participant fails to pay amounts owed to HIE when due, and such failure to pay continues for thirty (30) days after written notice from HIE.

5.4.3. HIE may also immediately suspend a Participant or Participant User's access to the Clinical Messaging System, without terminating this Agreement, pursuant to terms of HIE's Standards.

The standards are likely to have to be addressed in detail in another agreement, or supplemented here

5.5. Participant Rights Upon Termination. Upon termination of this Agreement, Participant shall have the right to have HIE remove any and all of Participant's data residing within the System, excepting only demographic data and such other data rightfully transferred to and residing in one or more discrete work group database(s) assigned to some other HIE Participant, or in the virtual health record, prior to the date of Participant's request for removal. The provisions of paragraph 4 of this Agreement shall survive termination of this Agreement and continue to apply to Participant's data not removed from the Clinical Messaging System. Upon notice of termination for reasons other than termination by HIE under paragraph 5.3 or paragraph 5.4.1 of this Agreement, HIE and Participant shall agree upon a reasonable time (not to exceed one hundred eighty (180) days from the effective date of termination), terms and conditions within which Participant may continue Use of the Clinical Messaging System. During this time period, Participant may continue Use of the Clinical Messaging System in accordance with this Agreement, and the parties shall be subject to all terms of this Agreement and any agreement between the parties regarding the termination, including payment of all amounts that may be owed to HIE.

6. General Provisions.

6.1. Compliance with Law. HIE, Participant and each Participant User shall comply with applicable Federal and State laws regarding Use of the Clinical Messaging System. This

Agreement shall be interpreted to the maximum extent possible as being consistent with such laws.

6.2. Independent Contractor. This Agreement is intended to create the relationship of independent contractor between Participant and HIE. Nothing contained herein shall be interpreted to create any relationship of agency, employment, partnership or joint venture between HIE and Participant. Neither party shall represent or hold themselves out to any person or entity other than is consistent with the relationship of independent contractor.

6.3. Entire Agreement. This Agreement, and the Exhibit___ attached to this Agreement, constitute the entire understanding and agreement of the parties, and shall supersede all prior understandings and agreements of the parties on the subject matter of this Agreement.

This was noted as very important

6.4. Amendment. Except as otherwise set forth in this Agreement, this Agreement shall not be changed, modified or altered except by amendment, which, to be valid and enforceable, shall be in writing and signed by the parties. Notwithstanding the foregoing, HIE may unilaterally amend this Agreement in order to comply with any applicable federal or state laws or regulations, including but not limited to Information Privacy and Protection Laws, effective immediately upon written notice to the Participant, and may otherwise amend the terms of this Agreement effective upon ninety(90) days prior written notice to the Participant. Participant's Use of the Clinical Messaging System after the effective date specified in such notice shall constitute acceptance of the amendment. Notwithstanding the foregoing, HIE's Standards may by modified as provided in this Agreement.

6.5. Notices. Either party may send any notices required pursuant to this Agreement, except notices of termination and notices regarding indemnity obligations, by first class mail, electronic transmission, certified mail or a recognized overnight delivery service, to the last known physical or electronic address for Participant in HIE's records. All termination notices under this Agreement by either party, and all notices regarding indemnity obligations, shall be made in writing and sent via certified mail, return receipt requested, or a recognized overnight delivery service, to the addresses of the parties set forth above.

6.6. Assignment. Neither party's rights, duties and responsibilities pursuant to this Agreement may be assigned or delegated without the prior written consent of the other party, except for a transfer or assignment to apparent, subsidiary or affiliate or an entity with which it is merged or consolidated, or the purchaser of all or substantially all of its assets provided that the transferee assumes all of its obligations under this Agreement.

6.7. Severability. If any provision of this Agreement is held to be invalid or unenforceable, the remaining provisions shall continue in full force and effect, unless the invalid or unenforceable provision is material to this Agreement and its invalidity or unenforceability results in substantial economic detriment to either party to this Agreement.

6.8. Governing Law. This Agreement shall be governed by the laws of the participating state.

May wish to clarify

6.9. Benefit. The terms and provisions of this Agreement shall bind and benefit Participant and permitted assigns, and shall bind and benefit HIE and its permitted assigns. There shall be no third party beneficiaries of this Agreement.

6.10. Interpretation. Any ambiguity or inconsistency in this Agreement shall be resolved in favor of a meaning that permits both parties to comply with applicable laws.

Considered a public entity callout, but was not agreed on

Discussed arbitration/mediation, but noted that states typically have a hard time accepting that option (vs. having greater leverage)

F.5 Mapping of Business Agreement Terms

Table 27. Mapping of Business Agreement Terms

Requirement	Public Entity to Public Entity Business Agreement	Public Entity to Private Entity Business Agreement
Scope of work, Transaction standards (as needed)	Sections 3 and 4 (generally)	Sections 2.3, 2.4, 3.3
Downstream pass-through requirements	Section 3 (b, c, g)	Section 2.2
Liabilities*	Section 4 (e, i)	Sections 2.10, 2.11
Indemnifications*	Section 4 (i)	Sections 2.9, 3.9
Payments (if any)	Silent, by intent	Section 3.6
Sanctions/terms*	Section 4 (generally)	Section 5 (generally)
Authorized users	Section 3 (generally and (a) specifically)	Section 4 (generally)
Secondary data uses	Section 3 (b, c, g) – none allowed	Section 4

F.6 West Virginia Business Associate Agreement Addendum

WV STATE GOVERNMENT

HIPAA BUSINESS ASSOCIATE ADDENDUM

This Health Insurance Portability and Accountability Act of 1996 (hereafter, HIPAA) Business Associate Addendum ("Addendum") is made a part of the Agreement ("Agreement") by and between the State of West Virginia ("Agency"), and Business Associate ("Associate"), and is effective on the date of execution of a binding Agreement with the Agency.

The Associate performs certain services on behalf of or for the Agency pursuant to the underlying Agreement that requires the exchange of information including protected health information protected by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as amended by the American Recovery and Reinvestment Act of 2009 (Pub. L. No.111-5) (the "HITECH Act"), any associated regulations and the federal regulations published at45 CFR parts 160 and 164 (sometimes collectively referred to as "HIPAA"). The Agency is a "Covered Entity" as that term is defined in HIPAA, and the parties to the underlying Agreement are entering into this Addendum to establish the responsibilities of both parties regarding HIPAA-covered information and to bring the underlying Agreement into compliance with HIPAA.

Whereas it is desirable, in order to further the continued efficient operations of Agency to disclose to its Associate certain information which may contain confidential individually identifiable health information (hereafter, Protected Health Information or PHI); and

Whereas, it is the desire of both parties that the confidentiality of the PHI disclosed hereunder be maintained and treated in accordance with all applicable laws relating to confidentiality, including the Privacy and Security Rules, the HITECH Act and its associated regulations, and the parties do agree to at all times treat the PHI and interpret this Addendum consistent with that desire.

NOW THEREFORE: the parties agree that in consideration of the mutual promises herein, in the Agreement, and of the exchange of PHI hereunder that:

1. Definitions. Terms used, but not otherwise defined, in this Addendum shall have the same meaning as those terms in the Privacy and Security Rules, including the HITECH Act.

a. Breach shall mean the acquisition, access, use or disclosure of protected health information which compromises the security or privacy of such information, except as excluded in the definition of Breach in 45 CFR § 164.402.160.103.

b. Business Associate shall have the meaning given to such term in 45 CFR §

c. Electronic Health Record shall mean an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.

d. Electronic Protected Health Information means Protected Health Information that is transmitted by Electronic Media (as defined in the Security and Privacy Rule) or maintained in Electronic Media.

e. Privacy Rule means the Standards for Privacy of Individually Identifiable Health Information found at 45 CFR Parts 160 and Part 164, Subparts A and E, as amended.

f. Personal Health Record shall mean an electronic record of identifiable health information on an individual that can be drawn from multiple sources and that is managed, shared and controlled by or primarily for the individual.

g. Protected Health Information or PHI shall have the meaning given to such term in 45 CFR § 164.501, limited to the information created or received by Associate from or on behalf of Agency.

h. Security Incident means any known successful or unsuccessful attempt by an authorized or unauthorized individual to inappropriately use, disclose, modify, access, or destroy any information.

i. Security Rule means the Standards for the security of Electronic Protected Health Information found at 45 CFR Parts 160 and 162, and Part 164, Subparts A and C. The application of Security provisions Sections 164.308; 164.310, 164.312, and 164.316 of title 45, Code of Federal Regulations shall apply to Associate of Agency in the same manner that such sections apply to the Agency.

j. Unsecured PHR Identifiable Health Information is information that is not protected through the use of a technology or methodology specified by the Secretary in the guidance issued under Section 13402(h)(2) of the HITECH Act.

k. Vendor of Personal Health Records shall mean an entity, other than a covered entity, that offers or maintains a personal health record.

2. PHI Disclosures; Permitted Uses.

a. PHI Described. PHI disclosed by the Agency to the Associate, PHI created by the Associate on behalf of the Agency, and PHI received by the Associate from a third party on behalf of the Agency are disclosable under this Addendum. The disclosable PHI is limited to the minimum necessary to complete the tasks, or to provide the services, associated with the terms of the original Agreement.

b. Purposes. Except as otherwise limited in this Addendum, Associate may use or disclose the PHI on behalf of, or to provide services to, Agency for the purposes necessary to complete the tasks, or provide the services, associated with, and required by the terms of the original Agreement, if such use or disclosure of the PHI would not violate the Privacy or Security Rules or applicable state law if done by Agency or violate the minimum necessary and related Privacy and Security policies and procedures of the Agency.

3. Obligations of Associate.

a. Stated Purposes Only. The PHI may not be used by the Associate for any purpose other than stated in this Addendum or as required or permitted by law.

b. Limited Disclosure. The PHI is confidential and will not be disclosed by the Associate other than as stated in this Addendum or as required or permitted by law. Associate will refrain from receiving any remuneration in exchange for any individual's PHI, unless Agency gives written approval, and the exchange is pursuant to a valid authorization (that includes a specification of whether the PHI can be further exchanged for remuneration by the entity receiving PHI of that Individual), or satisfies one of the exceptions enumerated in Section

13405(e)(2) of the HITECH Act. Associate will refrain from marketing activities that would violate HIPAA, specifically Section 13406 of the HITECH Act. Associate will report to Agency

any use or disclosure of the PHI, including any Security Incident not provided for by this Agreement of which it becomes aware.

c. Safeguards. The Associate will use appropriate safeguards to prevent use or disclosure of the PHI, except as provided for in this Addendum. This shall include, but not be limited to:

(i) Limitation of the groups of its employees or agents, otherwise known as workforce members, to whom the PHI is disclosed to those reasonably required to accomplish the purposes stated in this Addendum, and the use and disclosure of the minimum PHI necessary;

(ii) Appropriate notification and training of its employees or agents to whom the PHI will be disclosed in order to protect the PHI from unauthorized disclosure;

(iii) Maintenance of a comprehensive written PHI privacy and security program that includes administrative, technical and physical safeguards appropriate to the size, nature, scope and complexity of the Associate's operations.

d. Compliance With Law. The Associate will not use or disclose the PHI in a manner in violation of existing law and specifically not in violation of laws relating to confidentiality of PHI, including but not limited to, the Privacy and Security Rules.

e. Mitigation. Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Associate of a use or disclosure of the PHI by Associate in violation of the requirements of this Addendum, and report its mitigation activity back to the Agency.

f. Support of Individual Rights.

(i) Access to PHI. Associate shall make the PHI maintained by Associate or its agents or subcontractors in Designated Record Sets available to Agency for inspection and copying within ten (10) days of a request by Agency to enable Agency to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 CFR § 164.524 and consistent with Section 13405 of the HITECH Act.

(ii) Amendment of PHI. Within ten (10) days of receipt of a request from Agency for an amendment of the PHI or a record about an individual contained in a Designated Record Set, Associate or its agents or subcontractors shall make such PHI available to Agency for amendment and incorporate any such amendment to enable Agency to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 CFR § 164.526.

(iii) Accounting Rights. Within ten (10) days of notice of a request for an accounting of disclosures of the PHI, Associate and its agents or subcontractors shall make available to Agency the documentation required to provide an accounting of disclosures to enable Agency to fulfill its obligations under the Privacy Rule, including, but not limited to, 45CFR §164.528 and consistent with Section 13405 of the HITECH Act. Associate agrees to document disclosures of the PHI and information related to such disclosures as would be required for Agency to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 CFR §§ 164.528 and 164.316. This should include a process that allows for an accounting to be collected and maintained by Associate and its agents or subcontractors for at least six (6) years from the date of disclosure, or longer if required by state law. At a minimum, such documentation shall include:

- the date of disclosure;
- the name of the entity or person who received the PHI, and if known, the address of the entity or person;

- a brief description of the PHI disclosed; and
- a brief statement of purposes of the disclosure that reasonably informs the Individual of the basis for the disclosure, or a copy of the Individual's authorization, or a copy of the written request for disclosure.

(iv) Request for Restriction. Under the direction of the Agency, abide by any Individual's request to restrict the disclosure of PHI consistent with the requirements of Section 13405 of the HITECH Act and 45 CFR § 164.522.

g. Retention of PHI. Notwithstanding section 4.a. of this Addendum, Associate and its subcontractors or agents shall retain all PHI pursuant to state and federal law and shall continue to maintain the PHI required under Section 3.f. of this Addendum for a period of six (6) years after termination of the Agreement, or longer if required under state law.

h. Agents, Subcontractors Compliance. The Associate will ensure that any of its agents, including any subcontractors, to whom it provides any of the PHI it receives hereunder, or to whom it provides any PHI which the Associate creates or receives on behalf of the Agency, agree to the restrictions and conditions which apply to the Associate hereunder.

i. Amendments. The Associate shall make available to the specific Individual to whom it applies any PHI; make such PHI available for amendment; and make available the PHI required to provide an accounting of disclosures, all to the extent required by 45 CFR §§164.524, 164.526, and 164.528 respectively.

j. Federal Access. The Associate shall make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by the Associate on behalf of the Agency available to the U.S. Secretary of Health and Human Services consistent with 45 CFR § 164.504.

k. Security. The Associate shall take all steps necessary to ensure the continuous security of all PHI and data systems containing PHI. In addition, compliance with 74 FR 19006 Guidance Specifying the Technologies and Methodologies That Render PHI Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements under Section 13402 of Title XIII is required. Except with respect to Associate owned devices or equipment, if Associate chooses not to adopt such methodologies as defined in 74 FR 19006 based on its Security Risk Analysis, Associate shall document such rationale and submit it to the Agency.

I. Notification of Breach. During the term of this Agreement, the Associate shall notify the Agency and, unless otherwise directed by the Agency in writing, the Office of Technology immediately by telephone call plus e-mail, web form or fax upon the discovery of Breach of security of PHI, where the use or disclosure is not provided for by this Addendum of which it becomes aware, if the PHI was, or is reasonably believed to have been, acquired by an unauthorized person; or within 24 hours by e-mail or fax of any suspected Security Incident, intrusion or unauthorized use or disclosure of PHI in violation of this Agreement and this Addendum, or potential loss of confidential data affecting this Agreement. Notification shall be provided to the Agency contract manager at www.state.wv.us/admin/purchase/vrc/agencyli.htm and, unless otherwise directed by the Agency in writing, the Office of Technology at mailto:incident@wv.gov.

The Associate shall immediately investigate such Security Incident, Breach, or unauthorized use or disclosure of PHI or confidential data. Within 72 hours of the discovery, the Associate shall

notify the Agency contract manager, and, unless otherwise directed by the Agency in writing, the Office of Technology of: (a) What data elements were involved and the extent of the data involved in the Breach; (b) A description of the unauthorized persons known or reasonably believed to have improperly used or disclosed PHI or confidential data; (c) A description of where the PHI or confidential data is believed to have been improperly transmitted, sent, or utilized; (d) A description of the probable causes of the improper use or disclosure; and (e) Whether any federal or state laws requiring individual notifications of Breaches are triggered.

Agency will coordinate with Associate to determine additional specific actions that will be required of the Associate for mitigation of the Breach, which may include notification to the individual or other authorities.

All associated costs shall be borne by the Associate. This may include, but not be limited to costs associated with notifying affected individuals.

m. Assistance in Litigation or Administrative Proceedings. The Associate shall make itself and any subcontractors, employees or agents assisting Associate in the performance of its obligations under this Agreement, available to the Agency at no cost to the Agency to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against the Agency, its officers or employees based upon claimed violations of HIPAA, the HIPAA regulations or other laws relating to security and privacy, which involves inaction or actions by the Associate, except where Associate or its subcontractor, employee or agent is a named as an adverse party.

4. Addendum Administration.

a. Duties at Termination. Upon any termination of the underlying Agreement, if feasible, the Associate shall return or destroy all PHI received from, or created or received by the Associate on behalf of the Agency that the Associate still maintains in any form and retain no copies of such PHI or, if such return or destruction is not feasible, the Associate shall extend the protections of this Addendum to the PHI and limit further uses and disclosures to the purposes that make the return or destruction of the PHI infeasible. This shall also apply to all agents and subcontractors of Associate. The duty of the Associate and its agents and subcontractors to assist the Agency with any HIPAA required accounting of disclosures survives the termination of the underlying Agreement.

b. Termination for Cause. Agency may terminate the underlying Agreement if at any time it determines that the Associate has violated a material term of the Agreement or this Addendum. Agency may, at its sole discretion, allow Associate a reasonable period of time to cure the material Breach before termination.

c. Judicial or Administrative Proceedings. The Agency may terminate this Agreement if the Associate is found guilty of a criminal violation of HIPAA. The Agency may terminate this Agreement if a finding or stipulation that the Associate has violated any standard or requirement of HIPAA/HITECH, or other security or privacy laws is made in any administrative or civil proceeding in which the Associate is a party or has been joined. Associate shall be subject to prosecution by the Department of Justice for violations of HIPAA/HITECH and shall be responsible for any and all costs associated with prosecution.

d. Survival. The respective rights and obligations of Associate under this

Addendum shall survive the termination of the underlying Agreement.

5. General Provisions/Ownership of PHI.

a. Retention of Ownership. Ownership of the PHI resides with the Agency and is to be returned on demand or destroyed at the Agency's option.

b. Secondary PHI. Any data or PHI generated from the PHI disclosed hereunder which would permit identification of an Individual must be held confidential and is also the property of Agency.

c. Electronic Transmission. Except as permitted by law or this Addendum, the PHI or any data generated from the PHI which would permit identification of an Individual must not be transmitted to another party by electronic or other means for additional uses not authorized by this Addendum or to another contractor, or allied agency, or affiliate without prior written approval of Agency.

d. No Sales. Reports or data containing the PHI may not be sold without Agency's or the affected Individual's written consent.

e. No Third-Party Beneficiaries. Nothing express or implied in this Addendum is intended to confer, nor shall anything herein confer, upon any person other than Agency, Associate and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.

f. Interpretation. The provisions of this Addendum shall prevail over any provisions in the Agreement that may conflict or appear inconsistent with any provisions in this Addendum. The interpretation of this Addendum shall be made under the laws of the state of West Virginia.

g. Amendment. The parties agree that to the extent necessary to comply with applicable law they will agree to further amend this Addendum.

h. Additional Terms and Conditions. Additional discretionary terms may be included in the release order or change order process.

Form-WVBAA-012004

Amended 07-2010

F.7 West Virginia – State Boilerplate Example

GENERAL TERMS & CONDITIONS

PURCHASE ORDER/CONTRACT

1. ACCEPTANCE: Seller shall be bound by this order and its terms and conditions upon receipt of this order.

2. APPLICABLE LAW: The laws of the State of West Virginia and the Legislative Rules of the Purchasing Division shall govern all rights and duties under the Contract, including without limitation the validity of this Purchase Order/Contract.

3. NON-FUNDING: All services performed or goods delivered under State Purchase Orders/Contracts are to be continued for the terms of the Purchase Order/Contract, contingent upon funds being appropriated by the Legislature or otherwise being made available. In the event funds are not appropriated or otherwise available for these services or goods, this Purchase Order/Contract becomes void and of no effect after June 30.

4. COMPLIANCE: Seller shall comply with all federal, state and local laws, regulations and ordinances including, but not limited to, the prevailing wage rates of the WV Division of Labor.

5. MODIFICATIONS: This writing is the parties' final expression of intent. No modification of this order shall be binding unless agreed to in writing by the Buyer.

6. ASSIGNMENT: Neither this Order nor any monies due, or to become due hereunder may be assigned by the Seller without the Buyer's consent.

7. WARRANTY: The Seller expressly warrants that the goods and/or services covered by this order will: {a} conform to the specifications, drawings, samples or other description furnished or specified by the Buyer; {b} be merchantable and fit for the purpose intended; and/or {c} be free from defect in material and workmanship.

8. CANCELLATION: The Director of Purchasing may cancel any Purchase Order/Contract upon 30 days written notice to the seller.

9. SHIPPING, BILLING & PRICES: Prices are those stated in this order. No price increase will be accepted without written authority from the Buyer. All goods or services shall be shipped on or before the date specified in this Order.

10. LATE PAYMENTS: Payments may only be made after the delivery of goods or services. Interest may be paid on late payments in accordance with the West Virginia Code.

11. TAXES: The State of West Virginia is exempt from federal and state taxes and will not pay or reimburse such taxes.

12. RENEWAL: Any reference to automatic renewal is hereby deleted. The Contract may be renewed only upon mutual written agreement of the parties.

13. BANKRUPTCY: In the event the vendor/contractor files for bankruptcy protection, the State may deem this contract null and void, and terminate such contract without further order.

14. HIPAA BUSINESS ASSOCIATE ADDENDUM: The West Virginia State Government HIPAA Business Associate Addendum (BAA), approved by the Attorney General, is available online at www.state.wv.us/admin/purchase/vrc/hipaa.html and is hereby made part of the agreement provided that the Agency meets the definition of a Covered Entity (45 CFR §160.103) and will be disclosing Protected Health Information (45 CFR §160.103) to the vendor.

15. CONFIDENTIALITY: The vendor agrees that he or she will not disclose to anyone, directly or indirectly, any such personally identifiable information or other confidential information gained from the agency, unless the individual who is the subject of the information consents to the disclosure in writing or the disclosure is made pursuant to the agency's policies, procedures, and rules. Vendor further agrees to comply with the Confidentiality Policies and Information Security Accountability Requirements, set forth in http://www.state.wv.us/admin/purchase/privacy/noticeConfidentiality.pdf.

16. LICENSING: Vendors must be licensed and in good standing in accordance with any and all state and local laws and requirements by any state or local agency of West Virginia, including,but not limited to, the West Virginia Secretary of State's Office, the West Virginia Tax Department, West Virginia Insurance Commission, or any other state agency or political subdivision. Furthermore, the vendor must provide all necessary releases to obtain information to enable the Director or spending unit to verify that the vendor is licensed and in good standing with the above entities.

17. ANTITRUST: In accepting this purchase order or signing this contract with any agency for the State of West Virginia, the vendor agrees to convey, sell, assign, or transfer to the State of West Virginia all rights, title, and interest in and to all causes of action it may now or hereafter acquire under the antitrust laws of the United States and the State of West Virginia for price fixing and/or unreasonable restraints of trade relating to the particular commodities or services purchased or acquired by the State of West Virginia. Such assignment shall be made and become effective at the time the purchasing agency tenders the initial payment to vendor. Vendor certifies that this purchase order or contract is accepted or entered into without any prior understanding, agreement, or connection to any other entity that could be considered a violation of law. Vendor further certifies that this purchase order or contract is in all respects fair and without collusion or fraud.

Rev. 11/09/11