Bureau of Justice Assistance
U.S. Department of Justice

PDMP TTAC
Prescription Drug Monitoring Program Training and Technical Assistance Center

Prescription Drug
Monitoring Program

Prescription Drug Monitoring Program Research Requests

February 2023

This project was supported by Grant No. 2019-PM-BX-K003 awarded by the Bureau of Justice Assistance (BJA). BJA is a component of the U.S. Department of Justice's Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the Office for Victims of Crime, and the Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking (SMART). Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice.

Table of Contents

A Guide for Prescription Drug Monitoring Program Research Requests and Outreach

Introduction

The misuse of prescription drugs, especially opioids, has become a national crisis. The opioid epidemic creates a public health and safety concern that requires innovative solutions. One potential solution is the use of prescription drug monitoring programs (PDMPs). Research on the use of PDMPs provides evidence-based outcomes that can help inform decisions around public policy and provide insight into potential strategies to address the opioid crisis. PDMPs help detect fraud and provide valuable data that can be used to better understand the scope of the epidemic and the impact of various interventions. Research can also inform strategies for use of PDMPs to decrease opioid misuse and improve public health and safety. Despite the potential benefits of using PDMPs for research purposes, researchers have had trouble in obtaining access to the data stored within these programs. As the opioid crisis continues to worsen, PDMPs expect requests for access from researchers to increase, as more data is needed to inform public policy decisions and interventions.

Most PDMPs have the legal authority to provide PDMP data to researchers, though the requirements for getting access vary from state to state. In some cases, researchers must receive approval from a state government agency or the PDMP itself, while in others, researchers may only need to submit a formal request for the data. For example, in California, researchers must submit a written request to the PDMP that includes a detailed description of the research project and its expected outcomes. In addition, researchers may be required to provide proof of institutional review board (IRB) approval if the research includes human subjects. Once approved, researchers can use the data for various research purposes, such as analyzing prescribing patterns or understanding the impact of interventions.

Using PDMP Data

When conducting research on PDMP data, researchers may choose to use identified, de-identified, or aggregated data. Identified data includes personal identifying information (PII) or protected health information (PHI) and is subject to state and federal privacy requirements. De-identified data does not include any personal identifying information or protected health information and is not subject to the same privacy requirements. Aggregated data is a combination of data points that are averaged or summarized and is also not subject to the same privacy requirements. Using identified data in research can provide the most accurate results but carries the highest risk of a privacy breach. Using de-identified or aggregated data can provide a reasonable balance between accuracy and privacy but may not provide the same level of accuracy as identified data.

Legal Requirements and Privacy Protections

In the United States, the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act are two federal laws that provide privacy protections for individuals. In addition, each state has its own privacy laws that must be followed when conducting research on PDMP data.

The IRB process is used to review research protocols and ensure the safety of research participants. The IRB is responsible for reviewing research protocols and ensuring that the research is conducted in an ethical manner and in accordance with applicable laws and regulations. The review process includes an assessment of the risk and benefits of the research, the research design, the methods of data collection, the data security measures, and the informed consent requirements. The goal of the IRB process is to ensure that research participants are not exposed to undue risk and that their rights and privacy are respected. The IRB also evaluates the research protocol to ensure that it is scientifically valid and that the research will produce meaningful and useful results.

Getting Started—Steps for Researchers

For access to PDMPs in most states, researchers will need to comply with the following requirements:

- Prepare a research request that includes a detailed description of the research project, its expected outcomes, and related literature reviews; the type of data being requested (identified, de-identified, aggregated, etc.); the completed IRB certification; and researcher contact information.
- Indemnify adherence to all required privacy and security requirements, including access to and retention of the data.
- Submit the research request to the PDMP for review.
- Obtain approval from the PDMP, if required.
- Provide proof of IRB approval, if the research includes human subjects.
- Receive the data from the PDMP.
- Analyze the data and share the results.

Researchers should note that this list may not be all-inclusive, as a state may have additional requirements. For example, data use agreements (DUAs) between the state and the researcher or research institution are customary practice.

PDMPs Reaching Out to Researchers

PDMPs can reach out to researchers at both the federal and state levels. At the federal level, the National Institutes of Health has a program that provides funding for research related to prescription drug use and misuse. In addition, the Centers for Disease Control and Prevention has a program that provides funding to states for research on PDMP data. At the state level,

PDMPs can contact state health departments, universities, and other research institutions to collaborate on research projects. PDMPs can also reach out directly to researchers via professional organizations, conferences, and online groups. Finally, PDMPs can use social media to advertise research opportunities and connect with potential researchers.

Getting Started—Steps for PDMPs

When providing PDMP data to researchers, PDMPs should ensure that the data is secure and uses best practices for the release of PHI. For example, the use of strong data encryption and secure transmission protocols are critical. Data breaches carry significant penalties, both civilly and criminally. Not all researchers work with highly sensitive information, and it is important that everyone involved understands how the data will be used and protected.

In addition, researchers need accurate, consistent, and standardized data. Missing data fields, geographical errors, and/or changes in data elements can negatively impact research outcomes. Issues are compounded if PII is included. In most cases, PDMPs will work closely with their health information technology and/or other experienced government data professionals in providing information for researchers. The following list, while not all-inclusive, serves as a guide for PDMPs:

- Acknowledge receipt of the research request.
- Verify the identity and qualifications of the researcher(s).
- Verify the validity of the IRB certification, if required.
- If the research request is accepted, prepare the requested PDMP data for release.
- Be prepared to answer questions, or provide the resource who can, about the data.
- Establish a process to monitor access to the data.
- Provide the policies, legislations, and/or rules governing security and use of the data.
- Ensure that the researcher(s) provides updates on their progress and any outcomes.
- Define a process for authorizing new access to the data, as needed.
- Define a process/response to any data breaches, including unauthorized access.
- Ensure that use of the data does not exceed the scope or intent of the original agreement without prior authorization.
- Ensure that an agreement is in place, including verification, that the data will be destroyed once the project is completed.

Research provides valuable insights into PDMP data, much of which can be turned into actionable policy, strategy, and future program innovations. Partnering with a research institution, like a university, can add extensive value and utility for PDMPs well into the future.

Final Thoughts

Research using PDMP data has had a positive impact on policy, public health, and public safety. Research has provided evidence-based outcomes used to inform public policy decisions and inform strategies for addressing the opioid crisis. Research also has helped identify prescribing trends and other misuses of opioids and has supplied valuable insight into the impact of various interventions. By understanding the scope of the opioid crisis and the impact of interventions, policymakers and public health officials can develop strategies to reduce opioid misuse and improve public health and safety.

Appendices

Appendix A. Example of a State PDMP Research Request

Information to Be Obtained	Notes/Explanations
Point of contact information	Includes principal investigator's name, contact information, and institutional affiliation
General description of study	Study's goals, objectives, and aims
General description of how data will be used for the proposed study	Explanation of why PDMP data is needed
Data elements	PDMP should consider providing a list of available data fields
Data time periods requested	Start and end dates of records requested
Plan for data storage/protection	Usually covered also in the DUA and the IRB process
Plan for data confidentiality	Usually covered also in the DUA and the IRB process
Project start and end dates	Study start and end dates
Plan for data destruction	What will be done with the data upon end of study?
List of people who will have access to the data	Typical to include their roles/qualifications
Option for prior publication review	Typical for most state agencies
Study sponsor/funder	Financial source, if any
IRB approval/exemption certification	Does the study require an IRB review?
DUA	Typically obtained after the requestor receives approval

Appendix B. Example of a DUA

Common Terms/Conditions	Notes
Assurance of data integrity, security, and confidentiality	Includes data storage and security plan
Non-transfer of data for other projects/purposes	Statement specifying that the data provided will only be used for the approved study
Protection of potential identification of individuals	Includes specifications of public reporting of potentially identifying information and small cell suppression
Data destruction plan	Specification of what will be done with the provided data file upon completion of the project within a time frame (e.g., 7 years in case of audit)
Option/requirement to review prior to publication	
IRB certification of approval or exemption	
Protocol for data security	
Notification of data security breach	Specifies a privacy officer or a specific staff member(s)
State agency/department retains ownership of data	
Notification of change in key project staff	
Cost for data preparation	Some state agencies charge researchers for the cost of data preparation

Appendix C. Common Information Required by an IRB

Common Information Required by IRBs	Notes
Study goals	Includes the expected benefits
Principal investigator's qualifications	
Other research personnel and qualifications	
Literature review related to study	Includes why the study is needed
Study design	Includes the methodology/analytic plan
Plan for individuals' privacy	Includes how individuals within the data will be kept confidential or anonymous
Plan for data storage	Includes who will have direct access to the data, how long it will be kept, and when and how it will be destroyed
Plan for findings dissemination	
Project timeline	
DUA	Typically required before an IRB provides certification of approval or exemption
Training and certification of human subjects' confidentiality	Academic institutions require certain researchers to obtain certification

Appendix D. Example of a State PDMP Legislative Rule Outlining the Release of De-identified Data

Release of De-Identified INSPECT Data

Policy

The Indiana Board of Pharmacy (Board) may release de-identified data[1] for research or educational purposes in accordance with the requirements set forth herein.

Applicable Laws

IC 35-48-7-11.1 Confidentiality

...

(j) The board may compile statistical reports from the information described in subsection (a). The reports must not include information that identifies any practitioner, ultimate user, or other person administering a controlled substance. Statistical reports compiled public records.

Protocol for Release of De-Identified Data

Researcher must apply for the release of the de-identified data by (a) submitting a protocol and institutional review board (IRB) application and approval for Board review and, if deemed necessary by the Board, (b) making a personal appearance in front of the INSPECT Subcommittee.[2] The Board will place the application on its meeting agenda.

Board will review protocol and grant or deny the application to release the de-identified data based on the following factors:

1. The reason for the study and anticipated outcome (e.g. publication, presentation at scientific meeting, etc.);
2. Data fields and time frame requested;
3. Agreement that use of the data is limited to the protocol terms;
4. Agreement that the data cannot be transferred/shared with anyone outside the specific research project for which it is approved;
5. Agreement that research results will be reported to the INSPECT Subcommittee and approved by the Subcommittee prior to publication;
6. Agreement that the Indiana Board of Pharmacy and INSPECT may use the results for Board related purposes (e.g. reports to legislature); and
7. Any other information the Board deems necessary to render a decision on the application.

---

[1] De-identified data is defined below under the heading "INSPECT De-identified Data Defined".

[2] The institutional review board (IRB) must be registered with the Office for Human Research Protections (OHRP).

For more information please visit www.INspect.in.gov or email: INspect@pla.in.gov