Drug Enforcement Administration

Privacy Impact Assessment
for the
Prescription Drug Monitoring Program Analytics System (PDMPAS)

Issued by:

David J. Mudd
Associate Chief Counsel,
DEA Senior Component Official for Privacy

Approved by: Katherine Harman-Stokes
Director (Acting)
Office of Privacy and Civil Liberties U.S. Department of Justice

Date approved: August 29, 2022

(May 2019 DOJ PIA Template)

Section 1: Executive Summary

Provide a high-level overview of the information technology (e.g., application, tool, automated process) in non-technical terms that describes the information technology, its purpose, how the information technology operates to achieve that purpose, the general types of information involved, how information may be used and shared, and why a Privacy Impact Assessment was conducted. (Note: this section is an overview; the questions below elicit more detail.)

The Prescription Drug Monitoring Program Analytics System (PDMPAS) is a set of analytic tools, data sources, and processes that are used to support the DEA's Diversion Control Division's (DC) mission by leveraging Prescription Drug Monitoring Program (PDMP) data to support cases and investigations across the country. In practice, PDMP data is provided by the field and includes pharmaceutical transaction data in support of the case work being driven by the field. To support these cases, PDMPAS will analyze the data provided and identify the patterns, metrics, risk factors, and red flags pertinent to the case and provide an overview of the entire dataset to the field.

The PDMPAS environment does collect and maintain some forms of personally identifiable information (PII) and therefore DEA is required to complete a Privacy Impact Assessment (PIA) for its use, pursuant to the E-Government Act of 2002 and the Office of Management and Budget's (OMB) implementing guidance (OMB M-03-22).

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the information technology, why the information is being collected, maintained, or disseminated, and how the information will help achieve the Component's purpose, for example, for criminal or civil law enforcement purposes, intelligence activities, and administrative matters, to conduct analyses to identify previously unknown areas of concern or patterns.

The purpose of this environment is to provide a protected sandbox environment to research and conduct in-depth and actionable analytical support to DEA's DC for case support, civil litigation, and special projects. The analytical process ingests PDMP data, enhances it with commercially available data (e.g. Thompson-Reuters, Lexus-Nexus), and analyzes the enhanced data in support of special projects and cases. This process is based on over 150 risk factors developed by investigators, attorneys, and subject matter experts that are coded into a data analytics process.

When a request is submitted for a PDMPAS package, the applicable data may come in as Microsoft Excel, text or similar data file through Concorde for analysis. The data analysis requested from the field can be provided in standard form, custom or by commercial inquiries. A variety of analytic tools, namely Structured Query Language and Python, are used to process the data and provide responses to the field for all of their needs and questions. A comprehensive report is also created and provided to the field for them to review and analyze.

PDMP is also used to identify early prescription refills, doctor shopping (i.e. a person obtaining prescriptions from multiple doctors at once), distance traveled, dangerous drug combinations, prescription fraud, patient cells/crews (conspiracies of 3 or more patents), and payment schemes. DEA utilizes the PDMP in two ways: first it provides assistance in determining pharmaceutical drug diversion, and second it establishes production quotas of controlled substances.

The PDMPAS team consists of DEA employees and contractors who will collectively use this environment to support daily operations as users. PDMPAS team members may include the following positions: Section Chiefs, Program Analysts, Investigators, and Contractor analysts and/or Consultants with user approved privileges being assigned individually for each role.

2.2 Indicate the legal authorities, policies, or agreements that authorize collection of the information. (Check all that apply and include citations/references.)

Authority		Citation/Reference
X	Statute	21 U.S.C. § 878, Controlled Substances Act
	Executive Order	
	Federal Regulation	
	Agreement, memorandum of understanding, or other documented arrangement	
	Other (summarize and provide copy of relevant portion)	

Section 3: Information in the Information Technology

3.1 Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in Column (2), and indicate to whom the information relates in Column (3). Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	X	A, B, C and D	*Names could be collected of employees, contractors, other federal government personnel, members of the public (US or non-USPERs).*
Date of birth or age	X	A, B, C and D	*Other personal information e.g. date of birth, age etc. could be collected of employees, contractors, other federal government personnel, members of the public (US or non-USPERs).*
Place of birth	X	A, B, C and D	*Other personal information e.g. date of birth, age etc. could be collected of employees, contractors, other federal government personnel, members of the public (US or non-USPERs).*
Gender	X	A,B,C and D	*Gender information could be collected of employees, contractors, other federal government personnel, members of the public (US or non-USPERs).*
Race, ethnicity or citizenship	X	A, B, C and D	*Race, ethnicity and/ or citizenship could be collected of employees, contractors, other federal government personnel, members of the public (US or non-USPERs).*

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Religion	X	A,B,C and D	*Religion could be collected of employees, contractors, other federal government personnel, members of the public (US or non-USPERs).*
Social Security Number (full, last 4 digits or otherwise truncated)	X	A,B,C and D	*Social Security Number (SSN) could be collected of employees, contractors, other federal government personnel, members of the public (US or non-USPERs).*
Tax Identification Number (TIN)	X	A,B,C and D	*Government assigned identifiers etc. could be collected of employees, contractors, other federal government personnel, members of the public (US or non-USPERs).*
Driver's license	X	A,B,C and D	*Government assigned identifiers etc. could be collected of employees, contractors, other federal government personnel, members of the public (US or non-USPERs).*
Alien registration number	X	A,B,C and D	*Government assigned identifiers etc. could be collected of employees, contractors, other federal government personnel, members of the public (US or non-USPERs).*

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Passport number	X	A,B,C and D	*Government assigned identifiers etc. could be collected of employees, contractors, other federal government personnel, members of the public (US or non-USPERs).*
Mother's maiden name			
Vehicle identifiers	X	A,B,C and D	*Vehicle Identification Numbers could be collected of employees, contractors, other federal government personnel, members of the public (US or non-USPERs).*
Personal mailing address	X	A,B,C and D	*Email addresses, phone numbers etc. could be collected of employees, contractors, other federal government personnel, members of the public (US or non-USPERs) to include for prescribers, pharmacies, and/or patients.*
Personal e-mail address	X	A,B,C and D	*Email addresses, etc. could be collected of employees, contractors, other federal government personnel, members of the public (US or non-USPERs) to include for prescribers, pharmacies, and/or patients.*

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Personal phone number	X	A,B,C and D	*Phone numbers etc. could be collected of employees, contractors, other federal government personnel, members of the public (US or non-USPERs) to include for prescribers, pharmacies, and/or patients.*
Medical records number	X	A,B,C and D	*Health information could be collected of employees, contractors, other federal government personnel, members of the public (US or non-USPERs)*
Medical notes or other medical or health information	X	A,B,C and D	*Health information could be collected of employees, contractors, other federal government personnel, members of the public (US or non-USPERs)*
Financial account information	X	A,B,C and D	*Financial information could be collected of employees, contractors, other federal government personnel, members of the public (US or non-USPERs).*
Applicant information			
Education records			
Military status or other information			
Employment status, history, or similar information			
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents			
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			
Foreign activities			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Criminal records information, e.g., criminal history, arrests, criminal charges	X	A,B,C and D	*Criminal history could be collected of employees, contractors, other federal government personnel, members of the public (US or non-USPERs).*
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations	X	A,B,C and D	*Civil law violation information could be collected of employees, contractors, other federal government personnel, members of the public (US or non-USPERs).*
Whistleblower, e.g., tip, complaint or referral			
Grand jury information	X	A,B,C and D	*Information related to grand jury, criminal prosecution, or civil litigation could be collected of employees, contractors, other federal government personnel, members of the public (US or non-USPERs).*
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			
Procurement/contracting records			
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities			
Biometric data:			
- **Photographs or photographic identifiers**			
- **Video containing biometric data**			
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
- **Scars, marks, tattoos**			
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	A and B	*System admin/audit related information etc. could be collected of employees, contractors, and/or other federal government personnel*
- **User passwords/codes**	X	A and B	*System admin/audit related information etc. could be collected of employees, contractors, and/or other federal government personnel*
- **IP address**	X	A and B	*System admin/audit related information etc. could be collected of employees, contractors, and/or other federal government personnel*
- **Date/time of access**	X	A and B	*System admin/audit related information etc. could be collected of employees, contractors, and/or other federal government personnel*
- **Queries run**			
- **Content of files accessed/reviewed**			
- **Contents of files**			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Other (please list the type of info and describe as completely as possible):	X	A,B,C and D	*Possible instances of unknown PII related information could be collected and additionally Patient ID of employees, contractors, other federal government personnel, members of the public (US or non-USPERs); and/or Prescriber ID's of members of the public (US or non-USPERs); could also be collected.*

3.2 Indicate below the Department's source(s) of the information. (Check all that apply.)

Directly from the individual to whom the information pertains:					
In person		Hard copy: mail/fax	X	Online	X
Phone		Email	X		
Other (specify):					

Government sources:					
Within the Component	X	Other DOJ Components	X	Online	
State, local, tribal		Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)			
Other (specify):					

Non-government sources:					
Members of the public		Public media, Internet		Private sector	
Commercial data brokers	X				
Other (specify):					

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information and how the information will be shared or accessed, such as on a case-by-case basis by manual secure electronic transmission, external user authorized accounts (i.e., direct log-in access), interconnected systems, or electronic bulk transfer.

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Within the Component			X	Sharing data within Targeting & Special Projects Section, will be done via direct log-in access and managed user accesses.
DOJ Components	X	X		All outside reporting will be shared with our colleagues at the Civil Division's Consumer Protection Branch (CPB) primarily through email within Firebird. There are instances in which data is shared through bulk transfer methods like USA File Exchange, an Executive Office of United States Attorneys designed system that provides a secure electronic data sharing method.
Federal entities				
State, local, tribal gov't entities				
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes				
Private sector				
Foreign governments				
Foreign entities				
Other (specify):				

4.2 If the information will be released to the public for "Open Data" purposes, e.g., on data.gov (a clearinghouse for data from the Executive Branch of the Federal Government), and/or for research or statistical analysis purposes, explain whether—and, if so, how—the

information will be de-identified, aggregated, or otherwise privacy protected.

PDMPAS does not release information to the public for open data purposes.

Section 5: Notice, Consent, Access, and Amendment

5.1 What, if any, kind of notice will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Federal Register System of Records Notice (SORN), providing generalized notice to the public, a Privacy Act § 552a(e)(3) notice for individuals, or both? Will any other notices be provided? If no notice is provided, please explain.

PDMPAS's notice to the public is covered under system of DEA-008, *Investigative Reporting and Filing System*, 77 Fed. Reg. 21808 (Apr. 11, 2012), https://www.gpo.gov/fdsys/pkg/FR-2012-04-11/pdf/2012-8764.pdf.

5.2 What, if any, opportunities will there be for individuals to voluntarily participate in the collection, use or dissemination of information in the system, for example, to consent to collection or specific uses of their information? If no opportunities, please explain why.

All PII collected is in relation to and for cases. There is no means to allow the individual to consent, but due to the nature of the regulatory requirements, individuals do not have the opportunity to decline having the information provided and entered into the PDMPAS system.

5.3 What, if any, procedures exist to allow individuals to gain access to information in the system pertaining to them, request amendment or correction of said information, and receive notification of these procedures (e.g., Freedom of Information Act or Privacy Act procedures)? If no procedures exist, please explain why.

PDMPAS is only available to authorized users with permitted access. This allows for approved users to access the data information as it pertains to appropriate job functions. Individuals may request access to or amendment of their records maintained in PDMPAS through a FOIA and Privacy Act (FOIAPA) request. A FOIAPA request can be made through the DEA FOIA office. However, most information is not available as it is related to case files. DEA has exempted DEA-008, *Investigative Reporting and Filing System* from certain provisions of the Privacy Act. See 28 CFR § 16.98 for a complete list of DEA Privacy Act exemptions.

Section 6: Maintenance of Privacy and Security Controls

6.1 The Department uses administrative, technical, and physical controls to protect information. Indicate the controls below. (Check all that apply).

X	**The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO):** The ATO was approved May 25, 2021. **If an ATO has not been completed, but is underway, provide status or expected completion date: Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:** *N/A, there are no outstanding POAMs for privacy related controls.*
	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** *Assigned controls and assessments are being conducted within DOJs Cyber Security Asset Management, (CSAM) system.*
X	**Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:** *Assigned controls and assessments are being conducted within DOJs Cyber Security Asset Management (CSAM) system. The core controls identified by DOJ will be reviewed annually upon the ATO being granted final approval.*
X	**Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy**. *Yes, as a standard operating procedure, all contracts have the necessary, proper and accurate Privacy Act clauses and language required listed in each contract awarded within DEA.*
X	**Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe:** *The component has a requirement for all employees to include contract employees to complete the mandated Cyber Security Awareness Training annually.*

6.2 Explain key privacy and security administrative, technical, or physical controls that are designed to minimize privacy risks. For example, how are access controls being utilized to reduce the risk of unauthorized access and disclosure, what types of controls will protect PII in transmission, and how will regular auditing of role-based access be used to detect possible unauthorized access?

Only authorized users will be able to access the PDMPAS environment, namely through a Firebird administrative account. Regular patching schedules will be completed by the Information Systems Division (TC), to ensure all vulnerabilities are mitigated. All PII and data transfers will follow strict file transfer protocols.

6.3 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.)

Records in this system will be retained and disposed of in accordance with record retention schedules approved by the National Archives and Records Administration.

Section 7: Privacy Act

7.1 Indicate whether information related to U.S. citizens or aliens lawfully admitted for permanent residence will be retrieved by a personal identifier (i.e., indicate whether information maintained by this information technology will qualify as "records" maintained in a "system of records," as defined in the Privacy Act of 1974, as amended).

_____ No. __X___ Yes.

7.2 Please cite and provide a link (if possible) to existing SORNs that cover the records, and/or explain if a new SORN is being published:

DEA-008, *Investigative Reporting and Filing System*, 77 Fed. Reg. 21808 (Apr. 11, 2012), https://www.gpo.gov/fdsys/pkg/FR-2012-04-11/pdf/2012-8764.pdf.

Section 8: Privacy Risks and Mitigation

When considering the proposed use of the information, its purpose, and the benefit to the Department of the collection and use of this information, what privacy risks are associated with the collection, use, access, dissemination, and maintenance of the information and how are those risks being mitigated?

a. Potential Threats Related to Information Collection

Collecting and maintaining more personal information than necessary to accomplish the DEA's official duties is always a potential threat to privacy. The PDMPAS system collects and maintains only that information about an individual that is relevant and necessary to accomplish DEA's mission to bring to the criminal and civil justice system of the US, or any other competent jurisdiction, those organizations and principal members of organizations, involved in the growing, manufacture, or distribution of controlled substances appearing in or

destined for illicit traffic in the US; and to recommend and support non-enforcement programs aimed at reducing the availability of illicit controlled substances on the domestic and international markets.

In support of the field and Diversion's broader mission, the PDMPAS environment will ingest data from a variety of sources, including by not limited to, state PDMP programs, third party data providers, point of sale collectors, commercial data providers, and partnerships with other branches of the Department of Justice. In some cases, PDMPAS may ingest prescription and identifier data specific to a particular case in support of a broader operation to do further analysis given the identifiers provided by the field or attorneys responsible for the case.

b. Potential Threats Related to Use of the Information

Potential threats to privacy as a result of the DEA's use of the information in the PDMPAS system include the risks of unauthorized access to the information, threats to the integrity of the information resulting from unauthorized access or improper disposal of information and unauthorized disclosure of the information. Only authorized individuals are given access to this information. Each user annually is required to review and acknowledge the DEA IT Rules of Behavior as part of the mandated online IT Security Training. These individuals have read and accepted the IT Rules of Behavior regarding the proper handling of all DEA documents and data. This mitigates the risk of unauthorized use or disclosure of DEA's pertinent information. The limited distribution of the information from the applications, continual monitoring of access to the applications, and the observance of the IT Rules of Behavior, limit privacy risks. Outside of DEA, Federal Government users must also comply with computer security requirements, participate in annual security training, and acknowledge updated rules of behavior.

c. Potential Threats Related to Dissemination

Security measures that are in place to safeguard sharing of information include: IT monitoring tools; firewalls; intrusion detection and data loss prevention mechanisms; and audit logs. Consistent with Federal Information Security Modernization Act of 2014 (FISMA) and NIST security controls, transmissions of DEA non-public data occur only through secure methods, e.g., Virtual Private Networks (VPN), Secure File Transfer Protocol (FTP), or Secure Sockets Layer (SSL). The database is stored on a fully secured server created and administered in compliance with FISMA and Office of Management and Budget (OMB) guidance.

In addition, the method of generating and maintaining User IDs and passwords is one of numerous safeguards DEA uses to protect PII information. To maintain system security, the online functionality of user accounts becomes inactive after a specified number of failed logon attempts or after an extended period of time of no account activity. In addition, the method of generating and maintaining User IDs and passwords is one of numerous safeguards DEA uses to protect PII information.

DEA manages access by utilizing PDMPAS through permission-based role assignments and on a need-to-know basis. PDMPAS runs on a Sensitive But Unclassified Network with Internet Explorer for delivery of services and transporting of data. PDMPAS data may be shared within

the agency to include Division offices and senior management for case support, civil litigation, and special projects. Additionally, data may be shared with the DOJ components with reference to possible criminal, investigative, and enforcement purposes with many safeguarding practices in place.

Immediate notification is relayed to TC for revocation of access when a user or users depart DEA. All DEA personnel and contractors have been cleared to work on the system and agree to comply with the security policies and procedures established by DEA.