Privacy Impact Assessment for the VA IT System called:

PMP Government Gateway

Veterans Health Administration

Clinical Services

Date PIA submitted for review:

February 24,2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Margaret (Peggy) Pugh	Margaret.Pugh@va.gov	202-731-6843
Information System Security Officer (ISSO)	Andrew Vilailack	Andrew.Vilailack@va.gov	813-970-7568
Information System Owner	Joseph Still	Joseph.Still@va.gov	(717) 272-6621 ext 4904

Abstract

The abstract provides the simplest explanation for "what does the system do?" and will be published online to accompany the PIA link.

The VA PMP Gateway Software as a Service (SaaS) will be used by the Veterans Health Administration to query and retrieve Prescription Drug Monitoring Program (PDMP) data in conjunction with the VA's electronic health record (EHR) system to supply the facility information about the patient's prescription history. The gateway allows a single point of entry to integrate prescription information among multiple state databases and multiple protocols to obtain prescription usage history for the Veteran.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

1 General Description

A. The IT system name and the name of the program office that owns the IT system.

The PMP Government Gateway is owned by Bamboo Health and the VA office that provides guidance for the PDMP implementation with the VistA EHR integration is Clinical Services.

B. The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.

Prescription Drug Monitoring Program is an initiative driven by the Mission Act, Section 134 for the VA to participate in the national network of state-based prescription drug monitoring programs to support the safe and effective prescribing of controlled substances to covered patients. Another primary driver includes *VHA Directive 1306(1) "Querying State Prescription Drug Monitoring Programs (PDMP)," October 2016 (Amended October 21, 2019)*. Efforts in support of these drivers further the PDMP aspect of PMOP's mission to be the premier source of pain management, opioid safety, and Prescription Drug Monitoring Program (PDMP) expertise for ensuring VA provides high-quality, timely access to person-centered care for Veterans nationwide.

C. Indicate the ownership or control of the IT system or project.

Patient and provider demographics are controlled within the VistA EHR as the authoritative source system. Using the CPRS GUI and VDIF as the middleware, VA licensed healthcare providers and their delegates can perform a national query of all states that are connected to the Bamboo Health PDMP Gateway to view an aggregate report of the Patient's PDMP prescription history.

2. Information Collection and Sharing

D. The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.

All Veterans who receive healthcare at a VA medical facility.

E. A general description of the information in the IT system and the purpose for collecting this information.

Patient and Provider demographics are used by the PMP Gateway in order to initiate PDMP query requests to the state PDMP databases.

F. Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.

The PMP Gateway uses patient and provider demographics for patient matching and retrieval of PDMP data from state databases for the PDMP report.

G. Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.

The system is cloud-based and hosted on AWS.

3. Legal Authority and SORN

H. A citation of the legal authority to operate the IT system.

VHA Directive 1306(1):
This Veterans Health Administration (VHA) Directive establishes policy requiring VHA health care providers to query State Prescription Drug Monitoring Programs (PDMPs) to support safe and effective prescribing of controlled substances. This Directive does not establish policy regarding the disclosure of information to state PDMPs except to the extent required to query. AUTHORITY: 38 U.S.C. §§ 7301(b), 5701(l), 7332(b)(2)(G); 38 CFR §§ 1.483, 1.515.

S.2372 - VA MISSION Act of 2018:
Section 134 - The VA must enter into an agreement with a national network of prescription drug-monitoring programs or any state or regional drug prescription monitoring programs to allow licensed VA health care providers to question controlled substance prescriptions written in participating states or regions.

I. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?

The SORN will not require amendment and the SORN does include supplementary information for cloud usage.

D. System Changes

J. Whether the completion of this PIA will result in circumstances that require changes to business processes

No changes required to business processes.

K. Whether the completion of this PIA could potentially result in technology changes

No technical changes.

Section 1. Characterization of the Information

The following questions are intended to define the scope of the information requested and collected as well as the reasons for its collection as part of the program, IT system, or technology being developed.

1.1 What information is collected, used, disseminated, created, or maintained in the system?

Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy- Protected Information. For additional information on these information types and definitions, please see VA Directives and Handbooks in the 6500 series (https://vaww.va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.
This question is related to privacy control AP-1, Authority To Collect, and AP-2, Purpose Specification.

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional SPI is collected, used, disseminated, created, or maintained, please list those in the text box below:

- ☒ Name
- ☐ Social Security Number
- ☒ Date of Birth
- ☐ Mother's Maiden Name
- ☒ Personal Mailing Address
- ☒ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☐ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☐ Financial Information
- ☐ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers*

☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☐ Medications
☐ Medical Records
☐ Race/Ethnicity
☐ Tax Identification Number
☐ Medical Record Number
☒ Gender
☐ Integrated Control Number (ICN)
☐ Military History/Service Connection
☐ Next of Kin
☒ Other Data Elements (list below)

Additional elements include Provider's state location, personal NPI# and/or personal DEA# if licensed, requestor's Person Class Role, as well as Delegate's va.gov email address.

PII Mapping of Components (Servers/Database)

PMP Government Gateway consists of 1 key component (database). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected and the reasons for the collection of the PII are in the table below.

Note: Due to the PIA being a public facing document, please do not include the server names in the table.

Internal Database Connections

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
VDIF/HealthShare	Yes	Yes	Provider Data: • Role • First Name • Last Name • DEA Number • Personal NPI Delegate Data: • Role • First Name • Last Name • System ID (va.gov email) Location Data:	Required Data from VistA sent by VDIF to Bamboo Health for Patient	Enterprise Baseline Security Configuration

			• Name (facility division) • DEA Number • NPI Number • Address (State Code) Patient Data: • First Name • Middle Name • Last Name • DOB • Sex Code • Address (Street, City, State, Zip • Phone		

1.2 What are the sources of the information in the system?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.2a List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

The patient and provider information are retrieved from VistA.

1.2b Describe why information from sources other than the individual is required. For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question indicate why the system is using this source of data.

N/A.

1.2c If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

VistA is the authoritative source for patient and provider data. The PMP Gateway creates a report about the patient's prescription history using the prescription data that is collected and maintained by the individual State PDMPs.

1.3 How is the information collected?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.3a This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technologies used in the storage or transmission of information in identifiable form?

Yes, information is collected through technologies in identifiable form.

1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form's OMB control number and the agency form number.

Information is not collected on a paper form.

1.4 How will the information be checked for accuracy? How often will it be checked?

These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

The information is checked for accuracy by the data owner at the state level.

1.4b If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

Data validation testing on the retrieval side performed by VHA staff. Database integrity checks are done by the Bamboo Health. This is done in different areas as follows:

Replication:
The primary DB instance is synchronously replicated across Availability Zones to Aurora Replicas to provide data redundancy, eliminate I/O freezes, and minimize latency spikes during system backups. Running a DB cluster with high availability can enhance availability during planned system maintenance and help protect your databases against failure and Availability Zone disruption.

AWS Configuration is a continuous monitoring and assessment service that records changes to the configuration of your AWS resources. You can view the current and historic configurations of a resource and use this information to troubleshoot outages, conduct security attack analysis, and much more. You can view the configuration at any point in time and use that information to re-configure your resources and bring them into a steady state during an outage situation.

Connection Security:
Using TLS, we encrypt a connection between applications and the Aurora PostgreSQL DB clusters.

KMS Encryption Context Integrity Check:
When Amazon RDS uses your KMS CMK, or when Amazon EBS uses it on behalf of Amazon RDS, the service specifies an encryption context. The encryption context is additional authenticated data (AAD) that AWS KMS uses to ensure data integrity. When an encryption context is specified for an encryption operation, the service must specify the same encryption context for the decryption operation.

1.5 What specific legal authorities, arrangements, and agreements defined the collection of information?

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders. This question is related to privacy control AP-1, Authority to Collect

VHA Directive 1306(1):
This Veterans Health Administration (VHA) Directive establishes policy requiring VHA health care providers to query State Prescription Drug Monitoring Programs (PDMPs) to support safe and effective prescribing of controlled substances. This Directive does not establish policy regarding the disclosure of information to state PDMPs except to the extent required to query. AUTHORITY: 38 U.S.C. §§ 7301(b), 5701(l), 7332(b)(2)(G); 38 CFR §§ 1.483, 1.515.

S.2372 - VA MISSION Act of 2018:
Section 134 - The VA must enter into an agreement with a national network of prescription drug-monitoring programs or any state or regional drug prescription monitoring programs to allow licensed VA health care providers to question controlled substance prescriptions written in participating states or regions.

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks. (*Work with your System ISSO to complete this section)*

Consider the following Fair Information Practice Principles (FIPPs) when assessing the risk to individual privacy:

Principle of Purpose Specification: Explain how the collection ties with the purpose of the underlying mission of the organization and its enabling authority.

Principle of Minimization: Is the information directly relevant and necessary to accomplish the specific purposes of the program?

Principle of Individual Participation: Does the program, to the extent possible and practical, collect information directly from the individual?

Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?
This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

Privacy Risk: There is risk that VA SPI could be disclosed.

Mitigation: Information Security Policy control implementation including access control and secure design ensure only secure transactions are completed and only valid users have access to PII.

Bamboo Health leverages AWS to host its solutions provided as internal and external facing SAAS solutions. The AWS design consists of multiple accounts, virtual private clouds, and security features to ensure the highest level of access control while providing an extremely fault tolerant and highly available strategic architecture.

Leveraging cloud services and NIST design standards, we configure and automate protection of access to specific subnets. We control traffic flow to application subnets and data subnets to ensure only know solutions can route to protected areas. Leveraging Security Groups, we can extend this protection on a host-by-host basis to ensure the highest level of access restrictions. All access to AWS resources is controlled through domain management to ensure only specific access is allowed and all accounts require multi-factor authentication to access.

Section 2. Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

2.1 Describe how the information in the system will be used in support of the program's business purpose.

Identify and list each use (both internal and external to VA) of the information collected or maintained. This question is related to privacy control AP-2, Purpose Specification.

PDMP database checks require an accounting of disclosure note to be placed into the patient record each time a check is performed. Bamboo Health tracks and reports on all database searches to the PMP Interconnect. Data recorded as a result is regulated by state legislation.

The following data elements are used in the PDMP query request for patient matching:
Provider Data:
- Role
- First Name
- Last Name
- DEA Number
- Personal NPI

Delegate Data:
- Role
- First Name
- Last Name
- System ID (va.gov email)

Location Data:
- Name (facility division)
- DEA Number
- NPI Number
- Address (State Code)

Patient Data:
- First Name
- Middle Name
- Last Name
- DOB
- Sex Code
- Address (Street, City, State, Zip
- Phone

2.2 What types of tools are used to analyze data and what type of data may be produced?
These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis.

No analysis of the data is performed, it's a simple return of a query.

2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly

created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

If the PDMP Gateway report identifies prescription(s) filled outside the VA within a particular timeframe, the Provider has the opportunity to indicate on a PDMP Progress Note that observation and whether there are safety concerns, however manual intervention is required for that to occur.

2.3 How is the information in the system secured?

These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

2.3a What measures are in place to protect data in transit and at rest?

Data is encrypted in transit leveraging TLS 1.2 and at rest leveraging AWS' built-in AES 256-bit encryption.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs?

SSN is not used in the PDMP queries initiated from the VA.

2.3c How is PII/PHI safeguarded in accordance with OMB Memorandum M-06-15?

This control is partially inherited from the pre-existing FedRAMP P-ATO for the AWS US East/West IaaS, dated 11/13/2017. AWS restricts access to data centers, hardware, firmware, and transmissions within and between data centers. AWS establishes and manages cryptographic keys employed within the AWS services such as AWS KMS, Amazon S3, and Amazon EBS-volume encryption in accordance with federally approved and validated cryptography requirements for key generation, distribution, storage, access, and destruction.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. ***Example: Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.***

Consider the following FIPPs below to assist in providing a response:

Principle of Transparency: Is the PIA and SORN, if applicable, clear about the uses of the information?

Principle of Use Limitation: *Is the use of information contained in the system relevant to the mission of the project?*
This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

2.4a How is access to the PII determined?

There are multiple layers of approvals that Providers must receive, prior to being granted the permissions to the access the systems that allows them to perform a PDMP query. All VA employees that require a VA network account and the credentials to gain logical and physical VA resources; must go through the Personnel Security Adjudication process. Once granted access to the VA network, additional approvals are required for the Providers to gain access to the appropriate systems/applications to perform their day-to-day clinical workflows. Once all approvals have been obtained, for Prescribers, they must have an individual DEA#, along with a valid DEA expiration date on file in order to query as a non-delegate. For Pharmacists, they must have an individual NPI#, along with an effective date/time stamp on file in order to query as a non-delegate. Otherwise, these requestors would have to select a Supervisor and query as authorized delegates.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented?

Yes, Access Control policy and procedures are documented in eMASS as part of the ATO process.

2.4c Does access require manager approval?

Yes

2.4d Is access to the PII being monitored, tracked, or recorded?

Yes

2.4e Who is responsible for assuring safeguards for the PII?

The system ISO and ISSO.

Section 3. Retention of Information

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

*Identify and list all information collected from question 1.1 that is **retained** by the system. This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal*

No PII is retained by the result of a query as it is sent as a HTML page. Manual intervention is needed to add any returned data into a patient progress note. Copying any data is strictly controlled by state legislation (must be allowed by the state). However, data that was sent to query from VA will be retained and stored for auditing purposes and used by the state to determine who has accessed their PDMPs. The patient data used in the PDMP query includes the patient's name, gender, date of birth, personal mailing address, and phone number.

3.2 How long is information retained?

*In some cases VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. **For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods**. The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented. If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

If allowed by state law, and written into a progress note, retention is controlled by VHA policy for retention of healthcare data.

Data sent to Bamboo Health is retained for seven years and disposed of following Federal Policy NIST 800- 88. The NIST 800-88 document's objective is to assist with decision making when media require disposal, reuse, or will be leaving the effective control of an organization. Organizations should develop and use local policies and procedures in conjunction with this guide to make effective, risk-based decisions on the ultimate sanitization and/or disposition of media and information. More on the means used to dispose of the data is listed in sections below.
Bamboo Health disposes of audit logs in accordance with Federal and State requirements utilizing NIST 800- 88 guidelines for cryptographic erasure.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)?

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner. Please work with the system Privacy Officer and VA Records Officer to answer these questions.
This question is related to privacy control DM-2, Data Retention and Disposal.

3.3a Are all records stored within the system of record indicated on an approved disposition authority?

Yes

3.3b Please indicate each records retention schedule, series, and disposition authority.

Bamboo Health retains audit records that is in accordance with NARA requirements and the VHA Records Control Schedule (RCS) 10-1. In addition, Bamboo Health follows the Federal Requirements for Non-government systems and used the retention and disposal methods approved of in NIST 800-88. The NIST 800-88 document's objective is to assist with decision making when media require disposal, reuse, or will be leaving the effective control of an organization. Organizations should develop and use local policies and procedures in conjunction with this guide to make effective, risk-based decisions on the ultimate sanitization and/or disposition of media and information. More on the means used to dispose of the data is listed in sections below. Information related to patient queries and Veteran data sent to create query will be retained for seven years and disposed of according to NIST 800-88.

3.4 What are the procedures for the elimination or transfer of SPI?

Explain how records are destroyed, eliminated or transferred to NARA at the end of their mandatory retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc.? This question is related to privacy control DM-2, Data Retention and Disposal.

The records retained by Bamboo Health are electronically purged according to the requirements in NIST 800- 88.

Bamboo Health leverages Cryptographic Erase via AWS KMS along with AWS physical controls to comply with NIST 800-88.

Bamboo Health leverages AWS controls for disposal of physical media. The AWS Risk and Compliance white paper confirms compliance. Per the document, when a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in DoD 5220.22-or NIST 800-88 to destroy data as part of the decommissioning process. If a hardware device is unable to be decommissioned using these procedures, the device will be degaussed or physically destroyed in accordance with industry-standard practices. Amazon EBS volumes are presented as raw unformatted block devices that have been wiped prior to being made available for use. Wiping occurs immediately before reuse.

3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

Hypothetical data (false/dummy patient records) are used for testing, no actual PII is passed during testing and training.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

Consider the following FIPPs below to assist in providing a response:

Principle of Minimization: Does the project retain only the information necessary for its purpose? Is the PII retained only for as long as necessary and relevant to fulfill the specified purposes?

Principle of Data Quality and Integrity: Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?
This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:

Privacy Risk: There is a risk of information disclosure if there is a breach of Bamboo Health computer systems.

Mitigation: All data is encrypted at rest using FIPS 140-2 encryption with keys maintained by the AWS KMS service. KMS utilizes customer master keys protected by hardware security modules (HSMs). The FIPS certificate leveraged for the system can be found below:

- AWS Key Management Service (KMS) FIPS Certificate #4177
- AWS Application Load Balancer (ALB) FIPS Certificate #3553

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA.

4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system within VA with which information is shared.

State the purpose for the internal sharing. If you have specific authority to share the information, provide a citation to the authority.

For each interface with a system outside your program office, state what specific data elements (PII/PHI) are shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?
This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	List the purpose of the information being shared /received with the specified program office or IT system	List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system	Describe the method of transmittal
VistA/CPRS	Required VistA Data sent to VDIF to process PDMP Query	• First Name (required) • Last Name (required) • Birthdate (required) • Zip code (required if phone is unavailable) • Phone (required if zip code is unavailable) • Full Address (if available for Temporary and Permanent) • Gender (if available) • Middle Name/Initial (if available) • DFN/Station (if available) Requestor Data: • DEA Number (required if licensed) • Personal NPI • Person Class Role - (required if available) • First Name (required) • Last Name (required) • VA.Gov Email (required if Requestor is a Delegate) • Location (required) Delegate Supervisor Data (only required if Requestor is a Delegate): •	HTTPS/TLS1.2 via Port 443
VDIF/HealthShare	Required Data from VistA sent by VDIF to Bamboo Health for Patient	**PATIENT REQUEST** Provider Data: • Role • First Name • Last Name • DEA Number • Personal NPI Delegate Data: • Role • First Name • Last Name	HTTPS/TLS1.2 via Port 44

List the Program Office or IT System information is shared/received with	List the purpose of the information being shared /received with the specified program office or IT system	List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system	Describe the method of transmittal
		• System ID (va.gov email) Location Data: • Name (facility division) • DEA Number • NPI Number • Address (State Code) Patient Data: • First Name • Middle Name • Last Name • DOB • Sex Code • Address (Street, City, State, Zip • Phone •	

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

This question is related to privacy control UL-1, Internal Use.

Follow the format below:

Privacy Risk: Sharing patient information with unauthorized internal VA personnel could result in exposure of patient data.

Mitigation: VA IT systems undergo a Security Control Assessment by the VA Certification Program Office in support of Federal Information Security Management Act compliance and received an Authority to Operate (ATO), issued by the VA's Authorizing Official for Office of Information and Technology. Privacy and access control criteria are implemented and documented as part of the ATO process. The VA does continuous monitoring of security controls as identified in VA Directive 6500 and VA Handbook 6500.

Section 5. External Sharing/Receiving and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to VA, which includes Federal, State, and local governments, and the private sector.

5.1 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

Is the sharing of information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.

Identify and list the names of any Federal, State, or local government agency or private sector organization with which information is shared.

For each interface with a system outside VA, state what specific data elements (PII/PHI) are shared with each specific partner.

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.
This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	List the purpose of information being shared / received / transmitted with the specified program office or IT system	List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program or IT system	List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)	List the method of transmission and the measures in place to secure data
PMP Gateway (connects to State PDMPs via	The information used to generate and	Provider Data: • Role • First Name • Last Name	MOU/ISA	Encrypted transmission of data to VA via

PMP Interconnect)	send query and the patient details.	• DEA Number • Personal National Provider Identifier (NPI) Number Delegate Data: • Role • First Name • Last Name • SystemID (va.gov email) Location Data: • Name (facility division) • DEA Number • NPI Number • Address (State Code) Patient Data: • First Name • Middle Name • Last Name • DOB • Sex Code • Address (Street, City, State, Zip) • Phone		Bamboo Health using VDIF middleware via VA TIC and utilizing FIP 140- 2 or equivalent.

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

Discuss the privacy risks associated with the sharing of information outside the Department and what steps, if any, are currently being taken to mitigate those identified risks.

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum Of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.
Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.
This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

Privacy Risk: Sharing patient information with unauthorized external VA personnel could result in exposure of patient data.

Mitigation: If Bamboo Health employee, contractor, or agent becomes aware of the theft, loss or compromise of any device used to transport, access, or store VA data, Bamboo Health shall notify VA POCs by telephone or email within one hour upon discovery of a security incident.

Bamboo Health will provide details of the security incident, the potential risk to VA data, and all actions taken to remediate the issue. Reportable items include event type, date and time of event, user identification, workstation identification, success or failure of access attempts, and security actions taken by system administrators or security officers. VA Information System Security Officers (ISSO) or Privacy Officers (PO) will contact VA-CSOC within one hour of notification.

Bamboo Health will also provide VA with a written closing action report once the security event or incident has been resolved. VA will follow this same notification process should a security event occur within the VA boundary involving Bamboo Health's provided data. Designated POCs will follow established incident response and reporting procedures, determine whether the incident warrants escalation, and comply with established escalation requirements for responding to security incidents.

Section 6. Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an Appendix-A 6.1 on the last page of the document. Also provide notice given to individuals by the source system (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

6.1a This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

VHA Notice of Privacy Practices, Effective Date: 09/30/2019
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=1090

VHA Handbook 1605.04, VHA Notice of Privacy Practices:
Notice of Privacy Practices IB 10-163 (sharepoint.com)

SOR Number/ Federal Register Citation [79VA10 / 85 FR 84114]:
Veterans Health Information Systems and Technology Architecture (VistA) Records-VA: This system maintains a variety of information on current and former VA employees, contractors, patients, members

of their immediate family, and volunteers. The records include employee productivity information, patient medical information, computer access information, budget and supply information.

6.1b If notice was not provided, explain why. If it was provided, attach a copy of the current notice.

A copy of the current notice can be accessed and viewed below:

VHA Notice of Privacy Practices, Effective Date: 09/30/2019
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=1090

VHA Handbook 1605.04, VHA Notice of Privacy Practices:
Notice of Privacy Practices IB 10-163 (sharepoint.com)

Veterans Health Information Systems and Technology Architecture (VistA) Records-VA:
SOR Number/ Federal Register Citation [79VA10 / 85 FR 84114]

6.1c Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

Bamboo Health has no control over VA request for specific patients therefore has no way of notifying the Veteran of when their information is sent, however every time a query is sent to Bamboo Health an accounting of disclosure is generated and store for the Veteran to access upon request. The VHA Notice of Privacy Practices are distributed and available at the medical clinics where the patient receives healthcare, as well as online as part of the VHA publication series. VA has authority to collect data sent from queries based on agreements with the state and superseding federal policy. This is an excerpt of Directive 1306 which discusses the decision behind making the queries and what the data is used for within the VA: “By law, every prescription of controlled substances (schedule ii-v) must be reported to State PDMP databases. VA Directive 1306 sets policy on reviewing PDMP information when prescribing controlled substances. From Directive 1306: “It is VHA policy that state PDMP databases are queried for VHA patients who are receiving prescriptions for controlled substances as outlined in this policy on a minimum of an annual basis and that the results of queries are documented in the VA medical record. State PDMP databases will be queried prior to initiating therapy with a controlled substance and more often when clinically indicated. The requirements to query set forth in this paragraph are subject to limitations imposed by states on VA’s access to such databases.

Veterans Health Information Systems and Technology Architecture (VistA) Records-VA: This system maintains a variety of information on current and former VA employees, contractors, patients, members of their immediate family, and volunteers. The records include employee productivity information, patient medical information, computer access information, budget and supply information.

NOTE: This policy is the minimum requirement VA-wide. However, if there is variation between state laws for PDMPs (e.g. definition of a controlled substance, PDMP querying frequency, procedures for disclosing PDMP information, delivery format for the PDMP information, etc.), providers and prescribers

must conform to the policies and recommendations of the state of their licensure. For, example, individual VA medical professionals may be required by their state licensing boards to query state PDMPs more frequently than the minimum required by this policy. Additionally, when clinical indications and patient safety concerns warrant more frequent PDMP queries for a particular patient, such queries should be done at the discretion of the prescriber."

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress.

Veterans may decline care of services, but they cannot opt out of the queries as there is Federal law that requires a prescription drug history check prior to any new medications being offered. Bamboo Health has zero control of who or when queries are sent but records each access of record.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

This question is directed at whether an individual may provide consent for specific uses or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent.

Bamboo Health has no control over who is queried and when so they are unable to request consent for this purpose. Bamboo Health has no direct access to the Veteran information or any other information about the Veteran until it is sent in a query from VA.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

Consider the following FIPPs below to assist in providing a response:

Principle of Transparency: Has sufficient notice been provided to the individual?

Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?
This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.

Follow the format below:

Privacy Risk: N/A. Bamboo Health has no prior knowledge or control over whose information is queried therefore cannot provide notice.

Mitigation: N/A. Bamboo Health has no prior knowledge or control over who information is queried therefore cannot provide notice. NOTE: Veterans are advised of State PDMP sharing in the VHA Notice of Privacy Practices dated 9/30/2019. "State PDMP: We may use or disclose your health information without your authorization to an SPDMP in an effort to promote the sharing of prescription information to ensure safe medical care."

Section 7. Access, Redress, and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

7.1 What are the procedures that allow individuals to gain access to their information?

These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. ***For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.***

Individuals that require access to their information will follow the VA procedures or regulations that have been established at the VA facility where they are treated.

7.1b If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR).

Individuals that require access to their information will follow the VA procedures or regulations that have been established at the VA facility where they are treated.

7.1c If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information.

Individuals that require access to their information will follow the VA procedures or regulations that have been established at the VA facility where they are treated.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed. If the correction procedures are the same as those given in question 7.1, state as much. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Individuals that require access to their information to correct inaccurate or erroneous information will follow the VA procedures or regulations that have been established at the VA facility where they are treated.

7.3 How are individuals notified of the procedures for correcting their information?

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Individuals that require access to their information to correct inaccurate or erroneous information will follow the VA procedures or regulations that have been established at the VA facility where they are treated.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Individuals that require access to their information to correct inaccurate or erroneous information will follow the VA procedures or regulations that have been established at the VA facility where they are treated.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department's access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. ***For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals involved might change their behavior.*** *(Work with your System ISSO to complete all Privacy Risk questions inside the document this section).*

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

Principle of Individual Participation: If access and/or correction is denied, then is the individual provided notice as to why the denial was made and how to challenge such a denial?

Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?
This question is related to privacy control IP-3, Redress.

Follow the format below:

Privacy Risk: N/A. Bamboo Health has no control of what is sent by VA. VA is responsible for the accuracy of the data sent to Bamboo Health and must provide Veterans the ability to correct or ensure accuracy of information

Mitigation: N/A. Bamboo Health has no control of what is sent by VA. VA is responsible for the accuracy of the data sent to Bamboo Health and must provide Veterans the ability to correct or ensure accuracy of information.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system, and are they documented?

These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.

8.1a Describe the process by which an individual receives access to the system.

Clinicians accessing patient data undergo training and sign rules of behavior as required by VA policy that states how PII is to be protected on the systems. No user can access CPRS GUI to run a query unless they have a valid DEA# for Prescribers/NPI# for Pharmacists or are a delegate assigned. Furthermore no user can access a CPRS GUI without also have two factor PIV and completed VA onboarding requiring background checks and security policy training.

8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

Bamboo Health allows each state PDMP to access data related to queries conducted against their respective databases. Data is protected at rest and stored within the application for business and auditing purposes.

8.1c Describe the different roles in general terms that have been created to provide access to the system. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

For Providers, they must have an individual DEA#, along with a valid DEA expiration date on file in order to query as a non-delegate. For Pharmacists, they must have an individual NPI#, along with an effective date/time stamp on file in order to query as a non-delegate. Otherwise, these requestors would have to select a Supervisor and query as authorized delegates. All three user types - Providers, Pharmacists, and Licensed Delegates - querying out of the same VA facility will have the same read-only access to PDMP Prescription data provided their VistA information is set up properly and current registrations with the state PDMP are active where required.

8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII. This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

VA Contractors will have no access to PII through the system. The data sent will be stored and controlled by Bamboo Health and Bamboo Health will follow all FEDRAMP requirements related to secure access to the data including third parties, contractors and other authorized users. Only authorized users to VA systems may generate queries. User to VA systems must authenticate using two factor PIV authentication to access CPRS and have valid credentials before sending the query. Contractors are required to follow the same policies and onboarding requirements as employees including training and signing ROB before accessing VA information systems.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately. This question is related to privacy control AR-5, Privacy Awareness and Training.

Users to VA systems are required to take the VA Privacy and Information Security Awareness and Rules of Behavior Training and Bamboo Health users do not have access to VA data that is sent. Only users authorized by the states participating in providing information to the PDMP Gateway have access and can generate audit reports of queries to their states.

8.4 Has Authorization and Accreditation (A&A) been completed for the system?

8.4a If Yes, provide:

1. *The Security Plan Status:* Completed and submitted to VA.
2. *The System Security Plan Status Date:* Latest System Security Plan was submitted to VA on 12/2022.
3. *The Authorization Status:* Provisional ATO granted and FedRAMP ATO is in progress.
4. *The Authorization Date:* Provisional ATO granted 04/15/2022.
5. *The Authorization Termination Date:* Provisional ATO expiration date 04/15/2023.
6. *The Risk Review Completion Date:* SCAAR was completed by VA Cloud Security on 06/22/2022.
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* MODERATE

Please note that all systems containing SPI are categorized at a minimum level of "moderate" under Federal Information Processing Standards Publication 199.

8.4b If No or In Process, provide your ***Initial Operating Capability (IOC) date.***

Bamboo Health is undergoing FedRAMP moderate certification and is hosted in AWS FedRAMP Mod environment. The FedRAMP package was submitted for review to VA Cloud Security Team in March 2021. A One Year ATO was granted on 04/15/2022 and was renewed and expires 04/15/2023. We are continuing to work through the FedRAMP authorization process.

Section 9 – Technology Usage

The following questions are used to identify the technologies being used by the IT system or project.

9.1 Does the system use cloud technology? If so, what cloud model is being utilized?

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1*. (Refer to question 3.3.1 of the PTA)*

Yes, using AWS SaaS model.

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.*

Yes, Bamboo Health has a contract with AWS. The contract permitting the license agreement for the VA to use the PMP Gateway is separate from the contract between Bamboo Health and AWS. The contract number between the VA and Bamboo Health is VA118-16-D-1028. The details of the contract between Bamboo Health and AWS are externally exclusive from VA. Additionally, the mutual agreement for the data usage and flow from the VA to the PMP Gateway is also outlined in the signed and approved MOU/ISA.

9.3 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.

This question is related to privacy control DI-1, Data Quality.

No, the PMP Gateway does not collect any ancillary data from the VA, only the required data from VistA sent by VDIF to Bamboo Health for Patient/Report Requests, as outlined in this PIA.

9.4 NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

Yes, Bamboo Health puts customers on notice to ensure privacy controls are implemented for entities outside of Bamboo Health control.

9.5 If the system is utilizing Robotics Process Automation (RPA), please describe the role of the bots.

Robotic Process Automation is the use of software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. For example, will the automation move or touch PII/PHI information. RPA may also be referred to as "Bots" or Artificial Intelligence (AI).

No, the PMP Gateway does not utilize RPA in the transmission of VA data.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

ID	Privacy Controls
AP	**Authority and Purpose**
AP-1	Authority to Collect
AP-2	Purpose Specification
AR	**Accountability, Audit, and Risk Management**
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-7	Privacy-Enhanced System Design and Development
AR-8	Accounting of Disclosures

ID	Privacy Controls
DI	**Data Quality and Integrity**
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
DM	**Data Minimization and Retention**
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
IP	**Individual Participation and Redress**
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
SE	**Security**
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR	**Transparency**
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

The individuals below attest that the information they provided in this Privacy Impact Assessment is true and accurate.

Margaret L. Pugh 104985

Digitally signed by Margaret L. Pugh 104985
Date: 2023.03.06 17:15:48 -05'00'

Privacy Officer, Margaret Pugh

Digitally signed by ANDREW VILAILACK
Date: 2023.03.06 16:49:30 -05'00'

Information System Security Officer, Andrew Vilailack

Joseph T. Still 242700

Digitally signed by Joseph T. Still 242700
Date: 2023.03.06 16:18:52 -05'00'

Information System Owner, Joseph Still

APPENDIX A-6.1

VHA Notice of Privacy Practices, Effective Date: 09/30/2019
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=1090

VHA Handbook 1605.04, VHA Notice of Privacy Practices:
Notice of Privacy Practices IB 10-163 (sharepoint.com)

Veterans Health Information Systems and Technology Architecture (VistA) Records-VA:
SOR Number/ Federal Register Citation [79VA10 / 85 FR 84114]

HELPFUL LINKS:

Record Control Schedules:

https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

General Records Schedule 1.1: Financial Management and Reporting Records (FSC):

https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

National Archives (Federal Records Management):

https://www.archives.gov/records-mgmt/grs

VHA Publications:

https://www.va.gov/vhapublications/publications.cfm?Pub=2

VA Privacy Service Privacy Hub:

https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices