Privacy Impact Assessment for the VA IT System called:

Advanced Medication Platform Pharmacy GUI (AMPL) Assessing

Office of Information and Technology (OIT)
Enterprise Program Management Office Health Data Services

Veteran's Health Administration (VHA)

Date PIA submitted for review:

4/14/2025

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Nancy Katz- Johnson	nancy.katz-johnson@va.gov	203-535-7280
Information System Security Officer (ISSO)	Bradley Rosborough	Bradley.Rosborough@va.gov	(352) 248-0949
Information System Owner	Tony Sines	Tony.Sines@va.gov	(316) 249-8510

Abstract

The abstract provides the simplest explanation for "what does the system do for VA?".

The Advanced Medication Platform (AMPL) provides a comprehensive view of local and remote clinical patient data to enhance clinical decision support, by bringing together multiple domains. These domains include patient demographics, Crisis, Warnings, Allergies and/or Adverse Reactions and Directives (CWAD), allergies and adverse reactions, consults, immunizations, vitals, progress notes, problem lists, labs, and medications into one Graphical User Interface (GUI). With the use of the Veterans Data Integration and Federation (VDIF) service, AMPL aggregates VistA data obtained from all VistA instances across the VA enterprise to provide pharmacists a complete view of patient data. AMPL also offers enhanced functionality to assist Pharmacists with management of pending orders.

Overview

The overview is the most important section of the Privacy Impact Assessment (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. What is the business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?

Advanced Medication Platform (AMPL) Pharmacy Graphic User Interface (GUI) – AMPL-GUI provides enhancements to the functionality of the Veterans Health Information Systems and Technology Architecture (VistA) Pharmacy package. Being deployed in the Amazon Web Services (AWS) Cloud, these enhancements will provide pharmacists with a single point of access to patients' medical data in a clearer and more user-friendly display. The AMPL GUI is intended to advance VA's ongoing efforts to employ robust electronic health records and improve the efficiency and safety of the medication order process. AMPL GUI will support the current workflow, development and incorporation of new technology/functionality and techniques, and allow users to make more informed decisions, using clinical knowledge and patient-specific information, intelligently filtered, organized, and presented as care is being delivered.

- AMPL – Graphical User Interface (GUI) is owned by VHA Pharmacy.
- The business purpose of the system is to aggregate data from the various enterprise VistA sites to provide a complete view of patient clinical data and enhance pharmacy decision support.
- The AMPL system does not store any data and is a read-only system.
- The AMPL system is an enterprise application deployed in the AWS Cloud.
- The AMPL system uses patient and pharmacy data from VistA via the Veterans Data Integration and Federation (VDIF) service. VDIF provides data using the HealthShare Fast Healthcare Interoperability Resources (FHIR) gateway and VDIF custom services.
- The AMPL system does not share any data, as it does not store any data. All patient and pharmacy data are retrieved via the HealthShare VDIF service.

• The AMPL system is an enterprise application deployed in the Cloud. All security controls are maintained at the enterprise level.
• The AMPL systems are operated under the legal authority of VHA Pharmacy.
• Completion of the PIA will not require alterations to the AMPL system technologies.
• The AMPL system does not store any data. All data is obtained from the HealthShare VDIF service.
• The AMPL system is deployed on AWS FedRAMP Cloud in accordance with all applicable regulations. AWS Government Cloud is authorized under FedRAMP.
• The AMPL system does not store any data. Data ownership is not applicable.
• The AMPL system does not store any data. Organizational accountability is not applicable.
• The AMPL system does not store any data. Release of data is not applicable.

B. Who is the owner or has control of the IT system or project? If the system has an eMASS entry, ensure this information matches with the eMASS entry.

VA owned and operated

2. Information Collection and Sharing

C. Indicate the expected number of individuals whose information is stored in the system and include a brief description of the typical client or affected individual?

AMPL does not store information.

Check if Applicable	Demographic of individuals
☒	Veterans or Dependents
☐	VA Employees
☐	Clinical Trainees
☐	VA Contractors
☐	Members of the Public/Individuals
☐	Volunteers

D. What is a general description of the information in the IT system and the purpose for collecting this information?

The Advanced Medication Platform (AMPL) provides a comprehensive view of local and remote clinical patient data to enhance clinical decision support, by bringing together multiple domains. These domains include patient demographics, Crisis, Warnings, Allergies and/or Adverse Reactions and Directives (CWAD), allergies and adverse reactions, consults, immunizations, vitals, progress notes, problem lists, labs, and medications into one Graphical User Interface (GUI). With the use of the Veterans Data Integration and Federation (VDIF) service, AMPL aggregates VistA data obtained from all VistA instances across the VA enterprise to provide pharmacists a complete view of patient data. AMPL also offers enhanced functionality to assist Pharmacists with management of pending orders.

E. What information sharing is conducted by the IT system? A general description of the modules and components, where relevant, and their functions.

With the use of the Veterans Data Integration and Federation (VDIF) service, AMPL aggregates VistA data obtained from all VistA instances across the VA enterprise to provide pharmacists a complete view of patient data. AMPL also offers enhanced functionality to assist Pharmacists with management of pending orders.

F. Are the modules/subsystems only applicable if information is shared?

AMPL does not share any information

G. Is the system operated in more than one site to include primary and secondary 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?

. AMPL is within the VAEC AWS Cloud.

3. Legal Authority and System of Record Notices (SORN)

H. What is the citation of the legal authority?

In accordance with 24VA10A7_Patient Medical Records Nov022020 AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 38, United States Code, Sections 501(b) and 304.

I. What is the SORN?

SYSTEM NAME AND NUMBER: Patient Medical Records–VA (24VA10A7)
https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

J. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval.

AMPL is not in the process of being modified.

4. System Changes

K. Will the business processes change due to the information collection and sharing?

☐ Yes
☒ No
if yes, <<ADD ANSWER HERE>>

I. Will the technology changes impact information collection and sharing?

☐ Yes
☒ No
if yes, <<ADD ANSWER HERE>>

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 Information 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.

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1. It must also match the information provided in question 3.4 of the PTA.

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
- ☒ **Full** Social Security Number
- ☐ **Partial** 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[1]
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☒ Medications
- ☒ Medical Records
- ☒ Race/Ethnicity
- ☐ Tax Identification Number
- ☐ Medical Record Number
- ☒ Sex
- ☒ Integrated Control Number (ICN)
- ☒ Military History/Service Connection
- ☒ Next of Kin
- ☐ Date of Death
- ☐ Business Email Address
- ☐ Electronic Data

[1] *Specify type of Certificate or License Number (e.g., Occupational, Education, Medical)

Interchange Personal Identifier (EDIPI)

☐ Other Data Elements (List Below)

Other PII/PHI data elements:

1.2 List the sources of the information in the system

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.2 a 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 AMPL-GUI systems displays patient and pharmacy data to clinical users. The sole source of this data is the FHIR and custom Rest services provided by the Veterans Data Integration & Federation (VDIF) service program. The patient and pharmacy data is strictly read-only.

1.2 b 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.

AMPL displays data pulled from VDIF.

1.2 c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?

AMPL does not create information.

1.3 Methods of information collection

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.3 a 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?

The AMPL GUI system does not collect or store any data. AMPL displays data pulled from VDIF.

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

AMPLis not subject to the paperwork reduction act.

1.4 Information checks for accuracy, and 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.

1.4 a 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 AMPL GUI system does not collect or store any data. The AMPL-GUI system obtains all its data from the VDIF FHIR/Custom Services server. VDIF is ultimately responsible for the accuracy of the data.

1.4 b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?

The AMPL GUI system does not collect or store any data. The AMPL-GUI system obtains all its data from the VDIF FHIR/Custom Services server. VDIF is ultimately responsible for the accuracy of the data.

1.5 Identify the specific legal authorities, arrangements, and agreements that 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

•Presidential Review Directive 5, A National Obligation – Planning for Health Preparedness for and Readjustment of the Military, Veterans, and Their Families after Future Deployments, August 1998.

•Per SORN 24VA10A7 – Patient Medical Records Title 38, United States Code, Section 501(b) and 304.

1.6 <u>PRIVACY IMPACT ASSESSMENT: Characterization of the information</u>

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.

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

<u>Principle of Purpose Specification:</u> The collection ties with the purpose of the underlying mission of the organization and its enabling authority.

<u>Principle of Minimization:</u> The information is directly relevant and necessary to accomplish the specific purposes of the program.

Principle of Individual Participation: *The program, to the extent possible and practical, collects information directly from the individual.*

Principle of Data Quality and Integrity: *VA policies and procedures must ensure that personally identifiable information is accurate, complete, and current.*
This 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: AMPL disseminates a visual display of PII and other highly delicate PHI. If this information was breached or accidentally released to inappropriate parties or the public, it could result in financial, personal, and/or emotional harm to the individuals whose information is contained in the system.

Mitigation: The AMPL-GUI application is careful to only display the information necessary to accomplish the VA mission. AMPL is only available to users who have been granted access to view patient data as deemed necessary by their position in the VA. AMPL access is authorized by PIV credentials and proper Active Directory membership. The system logs are securely maintained in the event management system under EO management. The only information shared internally is audit log information recording which users accessed patient information using AMPL. Access to the audit logs is limited to only personnel with a security related job function and auditors. Additionally, to identify the parties involved in an incident, identify potential issues and concerns, and aid the affected parties so that they may find the help they need to get through their crisis. By only displaying the minimum necessary information, AMPL-GUI can better protect the individual's information.

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 that 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.

The AMPL-GUI system does not collect or maintain any data. The system retrieves and display data from the VDIF services. This data is used by authenticated pharmacy clinicians to view relevant patient and pharmacy data to process and fulfill medication orders.

2.2 Describe the types of tools 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.

2.2 a 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?

The AMPL-GUI system does not collect nor does it store data.

2.2 b 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.

AMPL does not create or make available new or previously unutilized information.

2.3 How the information in the system is secured.

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

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

Secure Socket Layer (SSL)

2.3 b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs? (refer to PTA question 3.8).

Yes. Only last 4 digits of SSN is displayed.

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

AMPL displaying only last four is a safeguard. First 5 numbers are masked.

2.4 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u>

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:

<u>Principle of Transparency:</u> 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.

2.4 a How is access to the PII determined?

The AMPL-GUI system utilizes two-factor authentication using PIV credentials. Access to the AMPL-GUI system is restricted to authorized VHA Pharmacy personnel.

2.4 b Are criteria, procedures, controls, and responsibilities regarding access documented? How are the documented, i.e. Policy, SOP, other. And where is this documentation located?

Criteria, procedures, controls and responsibilities regarding access is documented in the Access Control SOP located in eMASS.

2.4 c Does access require manager approval?

Yes

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

AMPL does not track when PII is accessed.

2.4e Who is responsible for assuring safeguards for the PII as identified in eMASS?

To gain access to eMASS you must request access and be approved by the ISO. The ISO ensures there are safeguards in place.

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

The AMPL-GUI system does not collect nor does it retain data.

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. If the system is using cloud technology, will it be following the NARA approved retention length and schedule https://www.archives.gov/records-mgmt/grs? This question is related to privacy control DM-2, Data Retention and Disposal.

The AMPL-GUI system does not collect nor does it retain data.

3.3 The retention schedule 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. Please work with the system 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?

The AMPL-GUI system does not collect nor does it retain data.

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

The AMPL-GUI system does not collect nor does it retain data.

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 AMPL-GUI system does not collect or retain data.

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.

The AMPL-GUI system does not collect nor does it retain data.

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 Privacy Officer (PO) to complete all Privacy Risk questions inside the document in 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: The project retains only the information necessary for its purpose, additionally, the PII is retained only for as long as necessary and relevant to fulfill the specified purposes.

Principle of Data Quality and Integrity: The PIA should describe 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: The AMPL-GUI system does not collect nor does it retain data.

Mitigation: The AMPL-GUI system does not collect nor does it retain data.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

PII Mapping of Components

4.1a Advanced Medication Platform Pharmacy GUI (AMPL) consists of 2 key components (servers/databases/instances/applications/software/application programming interfaces (API)). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Advanced Medication Platform Pharmacy GUI (AMPL) 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 server names in the table. The first table of 3.9a in the PTA should be used to answer this question.

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	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
N/A					
N/A					

4.1 b List internal organizations information is shared/received/transmitted, the information shared/received/transmitted, and the purpose, and how the information is transmitted.

NOTE: Question 3.9b (second table) on Privacy Threshold Analysis should be used to answer this question.

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

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
Veterans Data Integration & Federation (VDIF)	To facilitate the process of completing pharmacy orders by displaying patient and pharmacy data.	• Name • Social Security Number • Date of Birth • Personal Mailing Address • Personal Phone Number(s) • Personal Email Address • Emergency Contact Information (Name, Phone Number, etc. of a different individual) • Health Insurance Beneficiary Numbers Account Numbers • Current Medications • Previous Medical Records • Race/Ethnicity • Sex • Certificate/License Numbers • Integration Control Number (ICN) • Military History/Service Connection • Next of Kin	HTTPS

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the VA network 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 in this section.).

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

Follow the format below:

Privacy Risk: The privacy risk associated with displaying data within the Department of Veterans Affairs is that the data may be disclosed to individuals who do not require access or have a need to know. Inappropriate/unauthorized disclosure heightens the threat of the information being misused.

Mitigation: AMPL user access is restricted to VA personnel who have the need-to-know patient clinical data to perform their job functions and provide patient care. The system logs are

securely maintained in the event management system under EO management. The only information shared internally is audit log information recording which users accessed patient information using AMPL. Access to the audit logs is limited to only personnel with a security related job function and auditors. 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.

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 List the external organizations (outside VA) that information shared/received. and information shared/received, and the purpose, and how the information transmitted and what measures are taken to ensure it is secure.

The sharing of information outside the agency must be compatible with the original collection. The sharing must be covered by an appropriate routine use in a SORN. If not covered, 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.

NOTE: Question 3.10 on Privacy Threshold Analysis should be used to answer this question.

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 IT System or External Program Office information is shared/received with	***List the purpose of information being shared / received / transmitted***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)***	***List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
None				

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.

If no External Sharing listed on the table above, ***(State there is no external sharing in both the risk and mitigation fields).***

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: AMPL GUI does not share/receive data from external systems.

Mitigation: AMPL GUI does not share/receive data from external systems.

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 The notice provided to the individual before collection of the information. Please provide a copy and/or screen shot of a web notice of the notice as an Appendix-A 6.1 on the last page of the document. (A notice may include a posted privacy policy, a Privacy Act notice on forms,

notice given to individuals by the sources system, or a system of records notice published in the Federal Register.) If notice was not provided, explain why.

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 Provide the Privacy Notice provided to the public by this system or any source systems. Include a copy of the notice in Appendix A of the PIA, the Federal Register citation, or Privacy Statement from collection of information such as forms or surveys.

The VHA Notice of Privacy Practice (NOPP)
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946
explains the collection and use of protected health information to individuals receiving health care from VA. The NOPP is mailed every three years or when there is a major change to all enrolled Veterans. Non Veterans receiving care are provided the notice at the time of their encounter.

This Privacy Impact Assessment (PIA) also serves as notice As required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means."

A Privacy Act Statement is provided on all forms that collect information that will be maintained in a privacy act system of records. The statement provides the purpose, authority and the conditions under which the information can be disclosed.

Notice is provided in the SORN

6.1b If notice was not provided, explain why.

Notice was provided.

6.1c Provide how the notice provided at the time of collection meets the purpose of use for this system.

The VHA Notice of Privacy Practice (NOPP)
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946
explains the collection and use of protected health information to individuals receiving health care from VA. The NOPP is mailed every three years or when there is a major change to all enrolled Veterans. Non Veterans receiving care are provided the notice at the time of their encounter.

This Privacy Impact Assessment (PIA) also serves as notice As required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after

completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means."

A Privacy Act Statement is provided on all forms that collect information that will be maintained in a privacy act system of records. The statement provides the purpose, authority and the conditions under which the information can be disclosed.

Notice is provided in the SORN

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.

Ample does not collect nor retain data. Source Information is requested when it is necessary to administer benefits to veterans and other potential beneficiaries. While an individual may choose not to provide information, this may prevent them from obtaining the benefits necessary to them.

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.

Information is used, accessed and disclosed in accordance with the Privacy Act, 5 USC 552a, Title 38 USC 5701, Confidential Nature of Claims, Title USC 7332 and the HIPAA Privacy Rule 45 CFR.
Individuals are provided with a copy of the Notice of Privacy Practices that indicates when information will be used without their consent and when they will be asked to provide consent. Information is used, accessed and disclosed in accordance with the Privacy Act, 5 USC 552a, Title 38 USC 5701, Confidential Nature of Claims, Title USC 7332 and the HIPAA Privacy Rule 45 CFR.

Individuals or their legal representative may consent to the use or disclosure of information via a written request submitted to their facility Privacy Officer. Individuals also have the right to request a restriction to the use of their information. The written request must state what information and/or to whom the information is restricted and must include their signature and date of the request. The request is then forwarded to facility Privacy Officer for review and processing. Individuals may also request to Opt-Out of the facility directory during an inpatient admission. If the individual chooses to opt-out, information is not disclosed from the facility directory unless otherwise required

by law.

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 Privacy Officer (PO) 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: This is referring to sufficient notice provided to the individual.

Principle of Use Limitation: The information used only for the purpose for which notice was provided either directly to the individual or through a public notice. The procedures in place must 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: There is a risk that an individual may not receive notice that their information is being collected, maintained, processed, or disseminated by the Veterans' Health Administration and the local facilities prior to providing the information to the VHA.

Mitigation: This risk is mitigated by the common practice of providing the NOPP when Veterans apply for benefits. Additionally, new NOPPs are mailed to beneficiaries at least every 3 years and periodic monitoring is performed to check that all employees are aware of the requirement to provide guidance to Veterans and that the signed acknowledgment form, when applicable, is scanned into electronic records, The NOPP is also available at all VHA medical centers from the facility Privacy Officer.
The System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) are also available for review online, as discussed above.

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 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 VA Public Access Link-Home (efoia-host.com) to obtain information about FOIA points of contact and information about agency FOIA processes.***

AMPL GUI does not collect nor retain data. Access to the information displayed on the AMPL GUI is the responsibility of the VDIF and HealthShare system. Source information may be accessed thru MyHealthEVet or thru the medical facility's Release of Information (ROI) office.
VHA Directive 1605.01, Privacy and Release of Information, Paragraph 7 outlines policy and procedures for VHA and its staff to provide individuals with access to and copies of their PII in compliance with the Privacy Act and HIPAA Privacy Rule requirements. VHA also created VA form 10-5345a for use by individuals in requesting copies of their health information under right of access.VA Form 10-5345a is voluntary but does provide an easy way for individual to request their records.

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)?

AMPL GUI does not collect nor retain data. Access to the information displayed on the AMPL GUI is the responsibility of the VDIF and HealthShare system.

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?

Information in this system is covered by SORN 24VA10A7.

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.

AMPL GUI does not collect or retain data as explained in section 7.1. however source data falls under SORN 24VA10A7 which outlines procedures for accessing and correcting information. This is also identified in the Notice of Privacy Practices which is provided to all patients.

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.

AMPL GUI does not collect or retain data as explained in section 7.1.however Veterans are informed of the amendment process for the source data by many resources to include the VHA Notice of Privacy Practice (NOPP) which states:

Right to Request Amendment of Health Information.
You have the right to request an amendment (correction) to your health information in our records if you believe it is incomplete, inaccurate, untimely, or unrelated to your care. You must submit your request in writing, specify the information that you want corrected, and provide a reason to support your request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains your information.

If your request for amendment is denied, you will be notified of this decision in writing and provided appeal rights. In response, you may do any of the following:

- File an appeal
- File a "Statement of Disagreement"
- Ask that your initial request for amendment accompany all future disclosures of the disputed health information

Individuals seeking information regarding access to and contesting of VA benefits records may write, call or visit the nearest VA regional office.

Additional notice is provided through the SORS listed in 6.1 of this PIA and through the Release of Information Office where care is received.

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.

Redress is provided in accordance with 7.3.

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 Privacy Officer (PO) to complete all Privacy Risk questions in this section).*

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: The individual must be provided with the ability to find out whether a project maintains a record relating to them.

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

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

Follow the format below:

Privacy Risk: There is a risk that members of the public will not know the relevant procedures for gaining access to, correcting, or contesting their information.

Mitigation: the risk of incorrect information in an individual's records is mitigated by authenticating information when possible, Additionally, staff verifies information in medical records and corrects information identified as incorrect during each patient's medical appointments.
The NOPP discusses the process for requesting an amendment to one's records.

The*/* Release of Information (ROI) office is available to assist Veterans with obtaining access to their health records and other records containing personal information.
The Veterans' Health Administration (VHA) established MyHealtheVet program to provide Veterans remote access to their medical records. The Veteran must enroll and have access to the premium account to obtain access to all the available features. In addition, VHA Directive 1605.01 Privacy and Release of Information establishes procedures for Veterans to have their records amended where appropriate.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures. (Work with your ISSO to complete this section).

8.1 The procedures in place to determine which users may access the system, must be documented.

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

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

Pharmacy Benefits Management (PBM) has established policies and procedures for the identification and authorization of Pharmacy System users. AMPL-GUI follows these previously established

mechanisms. AMPL-GUI only has one defined role which is read-only access to all patient data relevant to proper execution of medication orders. Access to AMPL is authorized by the user's PIV credentials and verification that the user is within the proper Active Directory group membership.

8.1 b 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?

No users from other agencies access AMPL.

8.1 c 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.

AMPL GUI has users who must request access to a specific AD group. These users have Read-Only access.

8.2. Contractor signed Non-Disclosure Agreement (NDA), Business Associate Agreement (BAA) etc. in place.

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.

8.2 a Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

VA contractors that have access to the computer system are only delegated keys and menu functions needed to complete their duty task. They are required to complete annual Privacy, Security, and Rules of Behavior training. Contractors having access to PHI/PII are required to have a Business Associate Agreement (BAA) (nationally with the Veterans Health Administration (VHA) or locally with facility). Contracts are reviewed on an annual basis by the Contracting Officer Representative (COR). The Privacy Officer and Information Security Officer monitor that the annual Privacy, Security, and Rules of Behavior (ROB) training is completed by contractors and business associates. Any local BAAs are monitored by Privacy Officer to ensure compliance with the Health Insurance Portability and Accountability Act (HIPAA).

VA contractors under contract to perform system development and test system activities shall use redacted test patient data. No PII/PHI data is used in development or test systems.

8.2 a. Will VA contractors have access to the system and the PII?

VA contractors that have access to the computer system are only delegated keys and menu functions needed to complete their duty task. They are required to complete annual Privacy, Security, and Rules of Behavior training. Contractors having access to PHI/PII are required to have a Business

Associate Agreement (BAA) (nationally with the Veterans Health Administration (VHA) or locally with facility). Contracts are reviewed on an annual basis by the Contracting Officer Representative (COR). The Privacy Officer and Information Security Officer monitor that the annual Privacy, Security, and Rules of Behavior (ROB) training is completed by contractors and business associates. Any local BAAs are monitored by Privacy Officer to ensure compliance with the Health Insurance Portability and Accountability Act (HIPAA).

VA contractors under contract to perform system development and test system activities shall use redacted test patient data. No PII/PHI data is used in development or test systems.

8.2 b. What involvement will contractors have with the design and maintenance of the system?
VA contractors under contract to perform system development and test system activities shall use redacted test patient data. No PII/PHI data is used in development or test 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.

Personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA National ROB or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training which all personnel must complete via the VA's Talent Management System (TMS). After the user's initial acceptance of the ROB, the user must re-affirm their acceptance annually as part of the security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system. System administrators are required to complete additional role-based training. Users with access to PHI are required to complete HIPAA privacy training annually.

• PRIVACY AND HIPPA TRAINING
• VA PRIVACY & VA INFORMATION SECURITY

8.4 The Authorization and Accreditation (A&A) completed for the system.

8.4a If completed, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 06/03/2022
3. *The Authorization Status:* Authorized
4. *The Authorization Date:* 08/29/2022
5. *The Authorization Termination Date:* 08/28/2025
6. *The Risk Review Completion Date:* 01/11/2024
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 not completed or In Process, provide your ***Initial Operating Capability (IOC) date.***

No – IOC Target date is 04/29/2022

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. ***(Refer to question 1.8 of the PTA)***

AMPL GUI utilizes the VAEC FedRAMP AWS Cloud.

9.2 Does the contract with the Hosting 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 3.3.1 of the PTA)* *This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

AMPL does not store nor maintain any data.

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.

System logs are securely maintained in the AWS Cloud Watch under EO management. Access to the logs is limited to only personnel with a security related job function and auditors.

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.

AMPL does not store or maintain data.

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).

AMPL does not use any AI bots.

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
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.

NANCY KATZ-JOHNSON

Digitally signed by NANCY KATZ-JOHNSON
Date: 2025.05.21 11:20:08 -04'00'

Privacy Officer, Nancy Katz- Johnson

BRADLEY ROSBOROUGH

Digitally signed by BRADLEY ROSBOROUGH
Date: 2025.05.21 14:40:55 -04'00'

Information System Security Officer, Bradley Rosborough

TONY SINES

Digitally signed by TONY SINES
Date: 2025.05.21 15:55:06 -05'00'

Information System Owner, Tony Sines

APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy; a Privacy Act notice on forms; screen shot of a website collection privacy notice).

The VHA Notice of Privacy Practice (NOPP)
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

HELPFUL LINKS:

Records Control Schedule 10-1 (va.gov)

General Records Schedule
https://www.archives.gov/records-mgmt/grs.html

National Archives (Federal Records Management):
https://www.archives.gov/records-mgmt/grs

VA Publications:
https://www.va.gov/vapubs/

VA Privacy Service Privacy Hub:
https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):
VHA Directive 1605.04
IB 10-163p (va.gov)