Privacy Impact Assessment for the VA IT System called:

AudioCARE Enterprise Production – Legacy (AEP-L)

Enterprise Program Management Office (EPMO)

Veterans Health Administration/Clinical Ancillary

Date PIA submitted for review:

March 28, 2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Phillip Cauthers	Phillip.Cauthers@VA.GOV	503-721-1037
Information System Security Officer (ISSO)	Bobbi Begay	Bobbi.Begay@VA.GOV	720-788-4518
Information System Owner	Christopher Brown	Christopher.Brown1@VA.GOV	202-270-1432

Abstract

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

AudioCARE Enterprise Production – Legacy (AEP-L) is a Commercial Off the Shelf (COTS) application operational at approximately 140 VA Healthcare facilities in 22 VISNs; allowing Veterans to provide and receive medical information via toll-free telephone and internet sites. AEP-L is software and hardware, performing prescription inquiry; refill order processing; prescription medication information; prescription renewal requests and pick-up reminders; appointment scheduling and reminders; preventive health messages; customized patient surveys; secure physician / patient communications; pre-examination questionnaires, immunization information and screening reminders; staff emergency notifications; and patient-initiated balance inquires. AEP-L increases efficiency in handling routine patient requests and providing self-help tools accessible 24x7. Outgoing notifications can be triggered at user-defined options for each application, to allow direct control of the time notifications are made and the nature of information provided.

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:

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *Indicate the ownership or control of the IT system or project.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *A general description of the information in the IT system and the purpose for collecting this information.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *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.*
- *A citation of the legal authority to operate the IT system.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*
- *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?*

AudioCARE Enterprise Production - Legacy (AEP-L) is a COTS system owned and controlled by the EPMO Health Portfolio, comprised of telephony, text, email, and web applications enhancing patient communications for VA Health facilities. AEP-L is an "on premise" system integrated

with VistA and VA facilities' phone switch. AEP-L increases the efficient handling of routine patient requests for information on prescription refills, renewals, status, educational materials, miscellaneous communications, and surveys. AEP-L is located at approximately 140 VA facilities in 22 VISNs. The number of end-users is dependent on the number of patients serviced by each individual VA Medical Center. **An estimated 30,000 Veterans utilize AEP-L**. AEP-L is standardize on Windows 2019 servers and parallel security controls/security plans. AEP-L performs specific patient communication tasks.

The VA System of Record Notice (VA SORN) is 79VA10 (Amended Dec 23, 2020). The legal authority to operate is through VistA and Executive Order 9397 and the completion of this PIA does not require any changes to business processes.

AEP-L has unique application components for specific patient communication tasks:

Pharmacy Suite – AudioREFILL-Cerner, AudioRENEWAL, and AudioRxINFO

- Automates prescription refill / renewal
- Request a prescription refill, renewal, or status
- Provide educational materials for prescriptions
- "Prescription ready" notifications
- Refills through VA Consolidated Mail Order Pharmacy Service or local pharmacies

Pharmacy Suite requires: Name, Social Security Number (SSN), Prescription Number, Refills, Expiration Date, Last Fill Date, Rx Status, Drug National Drug Code (NDC), Drug Name, Site Name, and other data.

Miscellaneous Communications and Surveys – AudioCOMMUNICATOR

Informs patients; reduces anxiety; improves patient experience; provides facility communications:

- Custom announcements,
- Health & wellness reminders / surveys,
- Vaccination reminders
- Drug recalls

AudioCOMMUNICATOR requires: Name, SSN, Phone Number, and Date of Birth (DoB).

MTalkC and AudioCTalk – End users cannot access MTalkC or AudioCTalk

- Required for AEP operations
- De-identified PII and PHI pass through MTalkC & AudioCTalk
- MTalkC - processes phone calls through facility telephone switch.
- AudioCTALK - system processing and core call queue for all applications.

A new AEP-L configuration Baseline Standard uses system security levels established for VA workstations and servers. Standards include two-factor authentication, hard disk encryption, group policy management, monitoring features such as NESSUS and ePolicy scans, and vulnerability remediation using enterprise patch management solutions.

The Appointment Suite – AudioREMINDER, AudioINQUIRY, AudioCANCEL, AudioVERIFY/AudioCONTACT - call or text reminders for scheduled appointments, Multiple appointments for one or more individuals in a single household made in one call.

Patients can: retrieve appointment information, verify and update contact information, and confirm, cancel, or request appointment rescheduling

VA facilities can: inform patients of cancellations; give instructions or messages, customized by department with reminders such as ‘arrive 30 minutes early’ or ‘bring insurance cards and referral forms’.

Appointment Reminder has opt-in / opt-out capability. Facility staff record patient text and email preferences in specific registration screens. Text or email appointment information includes: Date, time, location, and number for cancellation or rescheduling.

Appointment Suite requires: Clinic Name, Clinic / Division / Location IEN, Appointment Date / Time, Appointment Division / Location, Patient Name, Phone Number, DOB, and Gender.

Clinical Information - AudioNOTES - reduces time consumed in direct provider / patient communication (e.g., tests, lab results, and studies). Each patient has a secured voice “mailbox” for the provider to leave messages; standard or custom messages can be recorded. Patients can retrieve messages by using a pre-assigned pin number. AudioNOTES can alert patients of messages and can report messages and results not accessed by the patient.

AudioNOTES requires: Name, SSN, VistA Patient Number, Phone Number, and DOB.

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.

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.

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 Account Information
☐ Health Insurance Beneficiary Numbers Account numbers
☐ Certificate/License numbers
☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☒ Current Medications
☐ Previous Medical Records
☐ Race/Ethnicity
☐ Tax Identification Number
☐ Medical Record Number
☒ Gender
☐ Integration Control Number (ICN)
☐ Military History/Service Connection
☐ Next of Kin
☒ Other Unique Identifying Information (list below)

Other Unique Identifiers:

Prescription Number; Rx Status; Expiration Date; Last Refill Date; Refill Remaining; Medication National Drug Code; Drug Name; Site Name; Appointment Date/Time; Appointment Location; Division/Location (Internal Entry Number (VistA) (IEN)); Clinic Name, VistA Patient Number.

PII Mapping of Components

AEP-L consists of 3 key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **AEP-L** and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

Note: Due to the PIA being a public facing document, please do not include the server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

PII Mapped to Components

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
Pharmacy Suite	Yes	Yes	Name, SSN, Prescription Number, Refills Remaining, Expiration Date, Last Fill Date,	Prescription refill and renewal process	Role Based Access control

			Rx Status, Drug NDC, Drug Name, Site Name		
Appointment Suite	Yes	Yes	Name, VistA Patient Number, Phone Number, DOB, Gender	call or text patients reminding of upcoming appointments	Role-based access;
Clinical Information/ Miscellaneous Communications and Surveys	Yes	Yes	Name, SSN, VistA Patient Number, Phone Number, and DOB	Improve overall patient experience. Call patients to alert them of messages in the system	Role-based access; pre-assigned PIN

1.2 What are the sources of the information in the system?

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?

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 1.3 indicate why the system is using this source of data.

If the system creates information (for example, a score, analysis, or report), list the system as a source of information.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

PII / PHI is received from the Patient or from VA VistA.

1.3 How is the information collected?

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 technology used in the storage or transmission of information in identifiable form?

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.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

PII / PHI is received directly from the user by telephone or from VA VistA through internal System-to-System information sharing.

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

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.

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.
This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

AEP-L validates accuracy of Information from VistA (e.g., Appointment Date/Time) by manually running the update from host utility within the application. Patients can verify home phone number, cell phone number, and email address by phone call. Information discrepancies are reported to VistA staff for update and is not updated by AEP-L.

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

Title 38, United States Code, Chapter 5, Sections 501(b), 304; and Chapter 73, Section 7301(a).

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.

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: AEP-L contains sensitive personal information (SPI) including Name, SSN, and Date of Birth. Due to highly sensitive nature of this data, there is a risk that unauthorized data access or other data breached; serious harm or identity theft may result.

Mitigation: VHA security measures, access controls and employee / contractor training protect PII / PHI from inappropriate use and/or disclosure. Security measures at each VA facility include access control, configuration management, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system protection, awareness and training, risk assessment, and identification authentication. Privacy measures include authority and purpose, accountability, audit and risk management, data quality and integrity, data minimization and retention, individual participation and redress, transparency, and use limitation. The patients authenticate using 2 factor authentication.

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.

- **Patient Name:** Optional data element that can customize patient communications. Also used in transaction reports.
- **Social Security Number:** Identifies the patient and retrieves prescription information from VistA.
- **Date of Birth:** Optional data element verifying patients when calling with VA-provided information such as surveys, Referral reminders, Flu shot reminders, etc.
- **Phone Number:** Used for specialty messages from VA Medical Centers to a specific group of patients.
- **Email Address:** Used for communications rather than via a telephone call.
- **Prescription Number:** Used in conjunction with the SSN to retrieve prescription information from VistA, and process prescription refill or renewal requests to the pharmacy.
- **Refills Remaining:** Number of refills remaining on a prescription. Spoken to the patient and not updateable.
- **Expiration Date:** Prescription expiration date. Spoken to the patient and not updateable.
- **Last Refill Date:** Most recent prescription refill by a pharmacy. Spoken to the patient and not updateable.
- **Prescription Status:** Retrieved from VistA and conveyed to the patient
- **Medication National Drug Code:** Nationally standardized code for medication. Used to provide information over the phone, such as potential side effects, overdose information, common uses, etc.
- **Drug Name:** Retrieved from VistA; name of the patient's medication based on the prescription number
- **Site Name:** Used for requesting refills and renewals of prescriptions to process at correct pharmacy.
- **VistA Patient Number:** Used by Appointment Suite, Clinical Information, and Miscellaneous Communications and Surveys modules to provide reference of correct treatment office, medication, or educational material
- **Gender:** Provides reference to correct treatment office / facility
- **Scheduling**: Appointment Date/Time; Appointment Location; Division/Location (Internal Entry Number (VistA) (IEN)); Clinic Name

2.2 What types of tools are used to analyze data and what type of data may be produced?

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.

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.
This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

AudioCARE has the capability to analyze the data used in operation. Data is retrieved from the VistA Host and conveyed to the patient. AEP-L creates statistical and transaction reports for system and application administrators to monitor system effectiveness.

2.3 How is the information in the system secured?
The AudioCARE systems utilize Whole Disk Encryption to secure the data at rest on the system. Secure protocols such as SFTP and TLS are used to secure the data in transit to and from the system. In addition, no time is PHI/PII information permitted to be retrieved from the AudioCARE system to the AudioCARE corporate network.

2.3a What measures are in place to protect data in transit and at rest?
Secure protocols such as SFTP and TLS are used to secure the data in transit to and from the system.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs? The AudioCARE systems utilize Whole Disk Encryption to secure the SSNs that are collected, processed or retained.

2.3c How is PII/PHI safeguarded in accordance with OMB Memorandum M-06-15?
AudioCARE contractors and VA personnel that manages this system are required to complete annual security trainings relating to safeguarding PII/PHI. They are:

- VA Privacy and Information Security Awareness, and Rules of Behavior - Must be less than 1 year
- VA Privacy and HIPAA Training - Must be less than 1 year
- Training for Elevated Privileges for System Access - Must be less than 1 year
- Information Security Role-Based Training for System Administrators - Must be less than 1 year
- Information Security and Privacy Role-Based - Must be less than 1 year
- Elevated Privileges for System Access TMS - Must be less than 1 year
- Information Security and Privacy Role-Based Training for System Administrators TMS - Must be less than 1 year

This question is related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information. How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

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.

System Administrators are monitored by the Enterprise Applications Service Line and comply with VA IT policies after receiving approval using the elevated privileges access system (ePAS). AEP-L administrators are screened prior to receiving elevated privileges to access AEP-L. AEP-L is reviewed annually to ensure VA ATO compliance with Security and Privacy requirements. PII / PHI is not downloaded or stored on mobile computing devices or removable electronic media. All AEP-L staff complete annual IA and Privacy training.

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

Patient Name
SSN
Date of Birth
Phone Number
Email Address
Prescription Number
Refills Remaining
Expiration Date

Last Refill Date
Prescription Status
Medication National Drug Code
Site Name
Address
Clinic Name
Gender
Appointment Date/Time
Appointment Location
Division/Location (Internal Entry Number (IEN)(VistA))
VistA Patient 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. If the system is using cloud technology, will it be following the NARA approved retention length and schedule?

The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.
This question is related to privacy control DM-2, Data Retention and Disposal.

Duration of retention for individual transaction data and statistical data in AEP-L is flexible. Individual transaction data is usually retained for 90 days; statistical data for 1 year. System parameters are customizable to meet individual sites' needs and requirements for data retention.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so, please indicate the name of the records retention schedule.

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.
This question is related to privacy control DM-2, Data Retention and Disposal.

When managing and maintaining VA data and records, healthcare facilities follow the guidelines established in the NARA-approved Veterans Health Administration Record Control Schedule (RCS) 10-1, RCS 10-1 link for VHA: http://www.va.gov/vhapublications/rcs10/rcs10-1. National Archives and Record Administration: www.nara.gov.

3.4 What are the procedures for the elimination of SPI?

Explain how records are destroyed or eliminated at the end of the 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

Electronic data and files containing any Sensitive Personal Information (SPI) (which includes PII / PHI) are destroyed per **VA Directive 6500, VA Cybersecurity Program.**, at this link: https://www.va.gov/digitalstrategy/docs/VA_Directive_6500_24_Jan_2019.pdf.

Also refer to the updated reference to VA Handbook 6500.1:
VA Handbook 6500: Handbook_6500_24_Feb_2021.pdf
And NIST SP 800-88: Guidelines for Media Sanitization (nist.gov)

If required, data is deleted from the file location and permanently deleted from the deleted item's location or recycle bin. Magnetic media is wiped, and digital media is shredded; both are destroyed per VA Directive 6500.

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. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?
This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research

AEP-L does not perform Research or Testing; data used for Training does not include identifiable SPI.

3.6 <u>PRIVACY IMPACT ASSESSMENT: Retention of information</u>

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.

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 that information maintained by AEP-L will be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached.

Mitigation: Collecting and retaining only the information necessary for fulfilling the VA mission, the disposition of data follows National Archives Records Administration (NARA) standards, ensuring data is not held longer than necessary.

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?

NOTE: Question 3.9 (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

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	AEP-L provides information to patients regarding appointments, prescription refills, and other types of communications previously identified.	Patient Name: SSN: Date of Birth: Phone Number: Email Address: Prescription Number: Refills Remaining: Expiration Date: Last Refill Date: Prescription Status: Medication National Drug Code: Site Name: Appointment Date/Time: Appointment Location: Division/Location (Internal: Entry Number (IEN): VistA Patient Number:	InterSystems ECP protocol over TCP

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

Follow the format below:
Privacy Risk: Data sharing is necessary for eligible individuals to receive medical care at VA facilities. There is a risk that data could be shared inappropriately, potentially causing catastrophic impact on privacy.

Mitigation: Potential harm and/or disclosure due to internal sharing is mitigated with standard information security measures for ATO compliance. Measures include access control, configuration management, media protection, system and service acquisition, audit and accountability, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system integrity, security assessment and authorization, incident response, risk assessment, program management, planning and maintenance. Privacy measures include authority and purpose, accountability, audit and risk management, data quality and integrity, data minimization and retention, individual participation and redress, transparency, and use limitation.

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.

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 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***
MessageMedia (3rd party SMS aggregator)	Used to send Text Messages when this is the patient's preference.	Cell phone number, appointment date/time and location.	Patient agrees / prefers to communicate via text messaging. Short Message Service (SMS) Service Agreement between AudioCARESystems and MessageMedia	TCP/IP over a TLS secured connection. There is a Business Associates Agreement (BAA) on file with MessageMedia

AEP-L security features are based on Veterans Affairs (VA) standards conforming with VA ATO requirements. AEP-L has current VA RMF authorization. AEP-L incorporates VA security elements, for example Full Disk Encryption, Multi-factor Authentication, and roll-based security. AudioCARE Customer Support Representatives can only access deployed AEP-L via the VA Citrix Access Gateway (CAG) after completing annual Privacy and Information Security Awareness training, signing VA Rules of Behavior, and obtaining a PIV card. Even then, there are data retrieval restrictions. At NO TIME is PHI or PII retrieval permitted. The systems used for remote / CAG access are encrypted and secured; only those requiring VA access can logon to them.

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: Data sharing is necessary for eligible individuals to receive medical care at VA facilities. There is a risk that data could be shared inappropriately, potentially causing catastrophic impact on privacy.

Mitigation: Potential harm and/or disclosure due to external sharing is mitigated with standard information security measures for ATO compliance. Measures include access control, configuration management, media protection, system and service acquisition, audit and accountability, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system integrity, security assessment and authorization, incident response, risk assessment, program management, planning and maintenance. Privacy measures include authority and purpose, accountability, audit and risk management, data quality and integrity, data minimization and retention, individual participation and redress, transparency, and use limitation.

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 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?

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. If notice was provided in the Federal Register, provide the citation.

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

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.
This question is 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.

Patients are not asked to provide data directly to AEP-L. Data is captured by the host system during patient registration or pharmacy prescription process. Data is passed to AudioCARE for appropriate communication. AEP-L uses the information to verify the patient's name and prescription information and to create call lists for other communications.

The VA SORN "Veterans Health Information System and Technology Architecture (VistA) – VA", SORN 79VA10 (Amended Dec 23, 2020). in the Federal Register and online at:
https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf

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

Patients provide information directly to AEP-L through 2 factor authentication. During any direct interaction with AEP-L, patients may choose not to provide / use their PII. They can call and specify types of interaction / calls they wish to receive. AEP-L can block outbound calls by patient ID or phone number. These controls are maintained by AEP-L System Administrators. On inbound calls patients can choose not to participate in specific programs.

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

Patients have the opportunity to consent to use of their PII in AEP-L by calling in and specifying the type of interaction / calls they wish to receive. AEP-L can block outbound calls by patient ID or phone number. These controls are maintained by AEP-L System Administrators. On inbound calls patients can choose not to participate in specific programs.

6.4 <u>PRIVACY IMPACT ASSESSMENT: Notice</u>

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks.

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: There is risk an individual may not receive notice that information is being collected, maintained, processed, or disseminated by VHA prior to providing the information to AEP-L. AEP-L receives PII / PHI from VistA, and not from individuals.

Mitigation: Risk mitigation is accomplished when VHA / VistA provides a Notice of Privacy Practice (NOPP). Additional mitigation is provided by making the System of Record Notices (SORNs) and PIA available for review online. AEP-L receives PII / PHI from VistA, and not from individuals.

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?

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.

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).

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.
This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

Individuals access their information by telephone, text message or email. Patients can call AEP-L, identify themselves, and receive any Prescription, Appointment, or Clinical information available to

them. During outbound communications patients are contacted through their preferred method (phone, email, text message), and appropriate information is provided. All information is sourced from the local site VistA host.

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.

AEP-L system does not directly update the VistA host. Inaccurate information is updated by site personnel with access to the appropriate VistA module. Patients must contact a Pharmacy Representative or call center staff to correct information pertaining to prescriptions, or a Central Appointments representative for incorrect appointment information.

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.

AEP-L system does not directly update the VistA host. The host site provides appropriate contacts to update patient information.

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.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.

AEP-L system does not directly collect patient PII / PHI and cannot provide formal redress to individuals. Inaccurate information is updated by site personnel with access to the appropriate VistA module. If the incorrect information pertains to prescriptions, the patient needs to contact a Pharmacy

Representative. If the information pertains to appointments, the patient needs to contact a representative in Central Appointments.

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.

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: AEP-L presents information as it is received from a VistA host. Any access, redress, or corrections are addressed by VistA. AEP-L can potentially forward incorrect data collected by VistA and provided to AEP-L, resulting in the patient receiving incorrect data originating with VistA.

Mitigation: A formal VA procedure exists for individuals to determine whether a system contains information about them. Patients should contact the VA location where they were seen. Inquiries should include the person's full name, social security number and contact information. VA Release of Information (ROI) offices assist Veterans accessing their records containing PII / PHI.

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?

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

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?

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.

This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.

AEP-L is available to all patients who wish to use it. Patients call a phone number provided by the local site, or through the site's automated attendant menu on their phone system. No special access permissions are granted by a site System Administrator. Site administrators can exclude specific clinics and divisions from using AEP-L to ensure patient privacy and confidentiality.

Clinic administrators can access the system remotely to add/remove clinics and do so after receiving approval through the ServiceNow ticketing system and being added to a security group.

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.

AudioCARE Systems employees are considered VA contractors, and complete VA background investigations to receive appropriate security clearance before performing tasks, per VA policies and procedures. Contractors must annually complete Privacy and Information Security Awareness (TMS 10176) and HIPAA training, and sign VA Rules of Behavior. The AudioCARE contract is reviewed annually. AudioCare must notify the VA of any effected employee change.

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.

All AudioCARE employees performing tasks for the VA must annually complete Privacy and Information Security Awareness (TMS 10176) and HIPAA training.

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

If Yes, provide:

1. *The Security Plan Status,*
2. *The Security Plan Status Date,*
3. *The Authorization Status,*
4. *The Authorization Date,*
5. *The Authorization Termination Date,*
6. *The Risk Review Completion Date,*
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH).*

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

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

Yes:

1. The Security Plan Status – **Approved**
2. The Security Plan Status Date – **21 Jul 2021**
3. The Authorization Status – **ATO**
4. The Authorization Date – **6 Aug 2021**
5. The Authorization Termination Date – **4 Nov 2022**
6. The Risk Review Completion Date – **30 July 2021**
7. The FIPS 199 classification of the system – **MODERATE**

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).

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.

No

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)

This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

N/A

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.

N/A

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.

N/A

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).

N/A

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 provided in this Privacy Impact Assessment is true and accurate.

Phillip Cauthers 255139

Digitally signed by Phillip Cauthers 255139
Date: 2022.04.07 12:06:18 -07'00'

Privacy Officer, Phillip Cauthers

BOBBI DEE BEGAY

Digitally signed by BOBBI DEE BEGAY
Date: 2022.04.20 06:37:26 -06'00'

Information Systems Security Officer, Bobbi Begay

Christopher Brown 101386

Digitally signed by Christopher Brown 101386
Date: 2022.05.03 14:50:28 -05'00'

Information System Owner, Christopher Brown

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).