Privacy Impact Assessment for the VA IT System called:

AudioCARE Enterprise Production (AEP-C)

Enterprise Program Management Office (EPMO)

Date PIA submitted for review:

26 August 2021

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Shonta Wright	Shonta.Wright@VA.GOV	352-372-0906
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 (AEP-C) is a Commercial Off The Shelf (COTS) system comprised of telephony, text, email, and web applications that enhance patient communications for VA Health facilities. The system is integrated with the Department of Defense (DoD) Healthcare Management System Modernization (DHMSM) Electronic Health Record (EHR) System and the VA facility's phone switch. AEP-C's system increase the efficiency in handling routine patient requests and providing self-help tools accessible 24x7 for pharmacy refills, status checks, renewal requests, and medication education.

AEP-C can automatically deliver important notifications to engage with patients and provide important healthcare information while obtaining important patient's feedback during the notification. VA-initiated communications include preventive care notifications and surveys; prescription ready for pickup; etc. Outgoing notifications can be triggered at user-defined parameter options for each application to allow for direct control over the time the notifications are made and the nature of the 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 (AEP-C), managed by EPMO, is a COTS system comprised of telephony, text, email, and web applications enhancing patient communications for VA Health facilities. AEP-C is an "on premise" system integrated with the DHMSM EHR System and VA facilities' phone switch. AEP-C increases the efficient handling of routine patient requests for information on prescription refills, renewals, status, educational materials, miscellaneous communications, and surveys. AEP-C is in Area Puget Sound; OEHRM has initiated plans to transfer their AEP iterations to the AEP-C security boundary, at which time the PTA and PIA will be reviewed and re-submitted if necessary. The number of AEP-C end-users is entirely dependent on the number of patients serviced by each individual VA Medical Center. An estimated 30,000 Veterans utilize the AudioCARE system at Area Puget Sound.

The OEHRM iterations and AEP-C are standardized at all sites, on Windows 2016 servers and parallel security controls / security plans, maintaining mirrored security postures and practices for both organizations. AEP-C has application components designed to accomplish specific patient communication tasks. The VA System of Record Notice (VA SORN) for AEP-C is 79VA10P2 (Amended Oct. 31, 2012). Neither the SORN nor AEP-C technology will be affected by incorporation of OEHRM iterations. Information for each AEP suite:

Pharmacy Suite – AudioREFILL-Cerner, AudioRENEWAL, and AudioRxINFO AEP's Pharmacy Suite automates patients' prescription refill / Renewal process. Patients can request a refill, renewal, or status of a prescription during a single phone call. Educational materials for specific prescriptions are provided by AEP. "Prescription ready" notifications can be sent. AEP's interface to the DHMSM EHR pharmacy system limits patient access to only their prescription information. Prescription refills requested through the automated telephone process are mailed to the patient through DHMSM EHR integration with the VA Consolidated Mail Order Pharmacy Service (CMOPS) or processed for pick-up by the local pharmacies. The data required from DHMSM EHR for Pharmacy Suite includes: Patient Social Security Number (SSN), Prescription Number, Refills Remaining, Expiration Date, Last Fill Date, Rx Status, Drug National Drug Code (NDC), Drug Name, Site Name, and Patient Name, among other data.

Miscellaneous Communications and Surveys – AudioCOMMUNICATOR Communicating information to patients is a critical healthcare facility operation. AEP communicates with AudioCOMMUNICATOR. Custom announcements, health and wellness reminders and surveys, flu vaccination reminders, or drug recalls, are communicated to keep patients informed; reduce anxiety; and improve overall patient experience. The data required for AudioCOMMUNICATOR includes: Patient Name, Social Security or Patient Health Record Number (optional), Patient Phone Number, and Date of Birth (optional).

MTalkC and AudioCTalk – AEP-C foundations required for the applications to operate. De-identified PII and PHI pass through these components. MTalkc interfaces with facility telephone switch to process phone calls. AudioCTALK handles all core call queue and system processing of AudioRefill-Cerner, AudioRxINFO, and AudioCOMMUNICATOR. End users cannot access these components.

Section 1. Characterization of the Information

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

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

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

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

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

- ☒ Name
- ☒ SSN
- ☒ Date of Birth
- ☐ Mother's Maiden Name
- ☐ Personal Mailing Address
- ☒ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☒ Personal Email
- ☐ 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
- ☐ Other Unique Identifying Information (list below)

DHMSM EHR and AEP pharmacy suite include Patient SSN, Prescription Number, Refills, Expiration Date, Late Fill Date, Rx Status, Drug NDC, Drug Name, Site Name, and Patient Name

Data required for AudioCOMMUNICATOR include Patient Name, SSN, Phone Number, and Date of Birth

PII Mapping of Components

AEP-C consists of 2 key components. Each has been analyzed to determine if any component elements collect PII. The type of PII collected by AEP-C and the reasons for PII collection are in the table below.

PII Mapped to Components

Do not include the server names in the table.

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
The Pharmacy Suite	Yes	Yes	Patient Social Security Number, Prescription Number, Refills Remaining, Expiration Date, Last Fill Date, Rx Status, Drug NDC, Drug Name, Site Name, and Patient Name	For patient's prescription refill and renewal process	Role Based Access control
Miscellaneous Communications and Surveys	Yes	Yes	Patient Name, Social Security or Patient Health Record Number, Patient Phone Number, and Date of Birth	Healthcare facility operation used to improve the overall patient experience	Role Based Access Control

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.

All PII / PHI used by the AEP-C is obtained through the integration with the existing DHMSM EHR. There is no direct entry of PII / PHI required by the AudioCARE system.

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.

The PHI / PII used by AEP-C is either received directly from the user via telephone, or from the DHMSM EHR via 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.

DHMSM EHR provides most of the information and some is collected directly from the patient by AEP-C. Examples of DHMSM EHR-generated data include prescription refill statuses, quantities, etc.; DHMSM EHR data is not checked for accuracy as AEP-C cannot validate it. AEP-C can verify phone number and email address with the patient. If there are any discrepancies, the information is reported to the administrative staff for updating DHMSM EHR; AEP-C contractors do not directly update that information.

If data such as SSN or prescription numbers are provided to AEP-C by the patient, it can be validated against DHMSM EHR data.

Frequency of DHMSM EHR accuracy checks are not reported to AEP-C. VA clinicians and AEP-C contractors in direct contact with patients manage / monitor the information included in the patient's profile. The Veterans'

identifying information is checked for accuracy by the VA clinicians and is cross-referenced with VA information.

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

Veterans' Health Administration – Organization and Functions, Title 38, United States Code (U.S.C.), Chapter 73, Section 7301(a)

Veterans Benefits - Title 38, United States Code, Chapter 5, Sections 501(b) and 304

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-C contains SPI including, but not limited to: Date of Birth, SSNs and Veterans' names. Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or if otherwise breached, serious harm or even identity theft may result.

Mitigation: Potential harm is mitigated by various levels of security in place on AEP-C. The system uses Full Disk Encryption to protect Data at Rest. Transport Layer Security (TLS) encryption between AEP-C and DHMSM EHR protects Data in Transit Secure File Transfer Protocol (SFTP) is used when transferring call lists. The process, and all encryption, complies with Federal Information Processing Standards (FIPS) 140-2. Access to AEP-C is restricted to personnel with VA Privacy and Information Security Awareness and Rules of Behavior; Privacy; and HIPAA training, certified annually. User access the AEP-C desktop with VA Citrix Access Gateway (CAG), providing Multi-Factor Authentication by requiring PIV card authentication. AEP-C access requires elevated privileges authenticated by an eToken. The VA restricts data retrieval from AEP-C with CAG; PHI / PII cannot be retrieved by AudioCARE Support Representatives. Finally, AEP-C only contains, accesses, and/or processes the minimum necessary data to complete required processing, minimizing PHI / PII at any given time.

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.

Information is used for direct communication with patients through telephone, and web utilities. The information identifies patients and verifies patient information. Communication is prescription refill requests and general announcements / surveys. The minimum required information needed to accomplish communication is retrieved from DHMSM EHR and used by AEP-C. For further details on the information used, please refer to section 1.1.

Patient Name: Optional data element that can customize patient communications. Also used in transaction reports.
SSN: Identifies the patient and retrieves prescription information from DHMSM EHR.
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 DHMSM EHR, 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 DHMSM EHR 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 DHMSM EHR; 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.

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

AEP-C does not perform any analysis of data utilized in operation. Information is retrieved from DHMSM EHR and conveyed to the patient. AEP-C cannot confirm phone numbers and / or email address on file. Incorrect information reported by the patient is reported to VA Administrative Staff for correction and update in DHMSM EHR. AEP-C creates statistical and transaction reports so system and application administrators can monitor system effectiveness.

2.3 How is the information in the system secured?

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

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

Full Disk Encryption protects Data at Rest. Transport Layer Security (TLS) encryption between AEP-C and DHMSM EHR protects Data in Transit Secure File Transfer Protocol (SFTP) is used when transferring call lists.

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

Access to AEP-C is restricted to personnel with VA Privacy and Information Security Awareness and Rules of Behavior; Privacy; and HIPAA training, re-certified annually. User access the AEP-C desktop with VA Citrix Access Gateway (CAG), providing Multi-Factor Authentication by requiring PIV card authentication. AEP-C access requires elevated privileges authenticated by an eToken. The VA restricts data retrieval from AEP-C with CAG; PHI / PII cannot be retrieved by AudioCARE Support Representatives. Finally, AEP-C only contains, accesses, and/or processes the minimum necessary data to complete required processing, minimizing PHI / PII at any given time

2.4 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u> 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 subject to VA IT policies are assigned by the facility where AEP-C resides. AEP-C administrators are screened before receiving administrator passwords, because they can access AEP-C at its lowest levels. AEP-C is classified Mission Assurance Category (MAC) III, Confidentiality Level (CL) Sensitive, per DoD classification criteria. AEP-C is reviewed annually during VA Assessment and Authentication to comply with VA Cyber Security and Privacy. PHI / PII is not downloaded or stored on mobile computing devices or removable electronic media. All staff working with AEAP-C complete annual Information Assurance (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

The information below that may be retained. All information used is either retained on the system, in DHMSM EHR, and/or on the VA Network. No information is retained by the vendor.

- Name
- SSN
- Date of Birth
- Phone Number(s)
- Email Address
- Current Medications

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.

AEP-C is designed to allow flexibility in the duration of retaining individual transaction data and statistical data. Individual transaction data is typically retained for 60 - 90 days; statistical data is retained for 550 days. Parameters are customizable to meet a site's needs and requirements for data retention. At the host site AEP-C currently retains prescription refill transactions for 45 days and statistical data for 550 days. Per the applicable SORN (79VA10P2) the retention period is in accordance with RCS 10-1, Item 2000.2 Information Technology Operations and Maintenance Records will be destroyed 3 years after agreement, control measures, procedures, project, activity, or when transaction is obsolete, completed, terminated or superseded, but longer retention is authorized if required for business use.

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 Department of Veterans' Affairs Record Control Schedule RCS 10-1** which can be found at: http://www.oprm.va.gov/docs/RCS005-1-OIT-8-21-09.pdf

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 of any type, including Protected Health Information (PHI) and Sensitive Personal Information (SPI) are destroyed in accordance with the **Department of Veterans' Affairs VA Directive 6500 and VA Media Sanitization SOP**.

When required, data is deleted from the file location and permanently deleted from the deleted items location or recycle bin. Magnetic media is wiped and digital media are shredded; both are then destroyed per **VA Media Sanitization SOP**.

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-C uses data retrieved from DHMSM EHR. Before use in a Production environment, AEP-C was tested with the DHMSM EHR (B1930). Once in Production, access to the testing environment is removed and the system is only permitted access to the Production Host. Test or training data in the DHMSM EHR is outside of AEP-Cs control.

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.

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.

Privacy Risk: There is a risk that information maintained by AEP-C, DHMSM EHR, and/or the facility may be retained longer than 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 housed in DHMSM EHR is based on standards developed by the National Archives Records Administration (NARA). This ensures data is only kept while 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 3.10 (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 shared/received with the Program Office or IT system***	***Describe the method of transmittal***
Cerner Millenium	Increase efficient handling of patient requests, and provide tools accessible 24x7 for refills, status, renewal requests, and medication education.	If appropriate to VA mission AEP-C collects patient name, SSN, phone number, Date of Birth, email address, prescription numbers and refill information	Electronically pulled from Cerner Millennium through HL7 interface to AEP-C.
DoD Healthcare Management System Modernization	Source of data used by AEP-C to provide information regarding	Prescription information, phone numbers, email address,	HL7 over TCP/IP

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 shared/received with the Program Office or IT system*	*Describe the method of transmittal*
Electronic Health Record	prescription refills, and other types of communications previously identified.	as appropriate to the AEP-C VA mission.	

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.

Privacy Risk: Data sharing is necessary for medical care of persons eligible for care at VHA facilities. There is risk data could be shared with inappropriate organizations of institutions; which has the potential for a catastrophic impact on privacy.

Mitigation: Potential harm is mitigated by various levels of security in place on AEP-C. The system uses Full Disk Encryption to protect Data at Rest. Transport Layer Security (TLS) encryption between AEP-C and DHMSM EHR protects Data in Transit Secure File Transfer Protocol (SFTP) is used when transferring call lists. The process, and all encryption, complies with Federal Information Processing Standards (FIPS) 140-2. Access to AEP-C is restricted to personnel with VA Privacy and Information Security Awareness and Rules of Behavior; Privacy; and HIPAA training, certified annually. User access the AEP-C desktop with VA Citrix Access Gateway (CAG), providing Multi-Factor Authentication by requiring PIV card authentication. AEP-C access requires elevated privileges authenticated by an eToken. The VA restricts data retrieval from AEP-C with CAG; PHI / PII cannot be retrieved by AudioCARE Support Representatives. Finally, AEP-C only contains, accesses, and/or processes the minimum necessary data to complete required processing, minimizing PHI / PII at any given time.

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 3.11 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 shared/received 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)	Sends Text Messages to patients who prefer texts.	Cell phone number	BAA.	TCP/IP over a TLS secured connection.

If specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16, note them here.

AEP-C security features are based on Department of Defense (DoD) standards and requirements. The system is based on the VA Windows 2012 R2 and transitioned to Windows 2016 servers; the VM platform conforms to DoD standards. Full Disk Encryption, Multi-Factor Authentication, and increased roll-based security are some areas implemented on AEP-C systems at VAMCs. AEP Customer Support Representatives only access deployed AudioCARE systems, via the VA CAG after completing annual Security Training, signing Rules of Behavior, and obtaining a PIV card and eToken. Additional restrictions on data retrieval from the system and no PHI / PII retrieval is permitted. Remote / CAG access is encrypted and secured; only personnel requiring access to the VA systems can log on.

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

Privacy Risk: Data sharing is necessary for medical care of persons eligible for care at VHA facilities. There is risk data could be shared with inappropriate organizations of institutions; which has the potential for a catastrophic impact on privacy.

Mitigation: Potential harm is mitigated by various levels of security in place on AEP-C. The system uses Full Disk Encryption to protect Data at Rest. Transport Layer Security (TLS) encryption between AEP-C and DHMSM EHR protects Data in Transit Secure File Transfer Protocol (SFTP) is used when transferring call lists. The process, and all encryption, complies with Federal Information Processing Standards (FIPS) 140-2. Access to AEP-C is restricted to personnel with VA Privacy and Information Security Awareness and Rules of Behavior; Privacy; and HIPAA training, certified annually. User access the AEP-C desktop with VA Citrix Access Gateway (CAG), providing Multi-Factor Authentication by requiring PIV card authentication. AEP-C access requires elevated privileges authenticated by an eToken. The VA restricts data retrieval from AEP-C with CAG; PHI / PII cannot be retrieved by AudioCARE Support Representatives. Finally, AEP-C only contains, accesses, and/or processes the minimum necessary data to complete required processing, minimizing PHI / PII at any given time.

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-C. Data is captured by the host system during patient registration or pharmacy prescription process. Data is passed to AudioCARE for appropriate communication. AEP-C uses the information to verify the patient's name and prescription information and to create call lists for other communications.

The VA System of Record Notice (VA SORN) 79VA10P2 (Amended Oct. 31, 2012), is published in the Federal Register and online at http://www.gpo.gov/fdsys/pkg/FR-2012-10-31/pdf/2012-26804.pdf and https://www.gpo.gov/fdsys/pkg/FR-2013-11-06/pdf/2013-26520.pdf

AEP-C is a system of records collecting PII and receives data only through system-to-system transfers with DHMSM EHR. Because AEP-C does not collect PII directly, a Privacy Act Statement is not required.

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 have an opportunity to consent to specific use of their PII by calling in and specifying the type of interaction / calls they wish to receive. AEP-C can block outbound calls by patient ID or phone number. Control is maintained by the AEP-C System Administrator. For inbound calls patients can elect not to participate in specific programs. Patients can obtain refills through options MyHealthyVet, mailing in a refill card that comes with their prescription(s), or walking up to the pharmacy counter at a VAMC with their refill. AEP-C is a convenient way for patients to request refills and renewals.

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 an opportunity to consent to specific use of their PII by calling in and specifying the type of interaction / calls they wish to receive. AEP-C can block outbound calls by patient ID or phone number. Control is maintained by the AEP-C System Administrator. For inbound calls patients can elect not to participate in specific programs.

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.

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

Privacy Risk: Before providing information to the VA, an individual may not receive appropriate notice that their information is being collected, maintained, processed, or disseminated by the VA

Mitigation: Risk is mitigated by providing a Notice of Privacy Practice (NOPP). Risk is also mitigated by making SORNs and the current Privacy Impact Assessment (PIA) available for online review.

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-C, identify themselves, and be presented with available Prescription information. During outbound communications the system provides appropriate information to the patient through their preferred method (phone, email, text message). All information is from DHMSM EHR.

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.

Inaccurate information is corrected by site personnel with access to the appropriate DHMSM EHR module. For incorrect information about prescriptions, patients contact a Pharmacy Representative. AEP-C does not update patient information directly to DHMSM EHR. Patients can make corrections by calling the appropriate VAMC, or access their information at the MyHealtheVet portal .

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

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures

exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Individuals are provided with contact phone numbers for requesting updates to their information. For example, they are instructed to contact the pharmacy or their provider to renew a prescription that has expired or without refills.

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.

Inaccurate information is corrected by site personnel with access to the appropriate DHMSM EHR module. For incorrect information about prescriptions, patients contact a Pharmacy Representative. AEP-C does not update patient information directly to DHMSM EHR.

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.

Privacy Risk:

AEP-C is dependent on the accuracy of the data provided to it. If patients call into the system, enter their Social Security Number, but do not know their prescription number, the system does not have the ability to look it up for them. In such cases, AEP-C is not able to perform Prescription Refill Requests, Renewals, or status checks. Outbound patient communications may not be conveyed to the intended patients, if the system is not provided accurate phone numbers.

Mitigation:

A formal VA procedure exists for individuals who wish to determine if AEP-C contains information about them. They should contact the VA facility location where they are or were employed or made contact. Inquiries should include the person's full name, social security number, dates of employment, date(s) of contact, and return address. This is the practice used by VHA's Release of Information (ROI) offices to assist Veterans with obtaining access to their medical records and other records containing personal information.

Section 8. Technical Access and Security

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

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

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-C is available to all patients. Patients call a phone number provided by the local site or access the system through the site's automated attendant menu on their phone system. No special access permissions are needed by a System Administrator at the site.

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.

AEP-C is designed and maintained by AudioCARE Systems (vendor) personnel. The Windows platform is controlled by the VA Platforms Group. The VA controls access to the system's Windows level and ensures Confidentiality Agreements and Non-Disclosure Agreements are in place before granting access to the VA network. Contractors complete appropriate background investigations and have received security clearance in accordance with VA Standard Policies and Procedures needed to perform their tasks; and complete VA Privacy and Information Security Awareness and Rules of Behavior, Privacy, and HIPAA training and are re-certified annually. They must also sign the Rules of Behavior and Non-Disclosure Agreements

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 working at the VA complete appropriate background investigations and have received security clearance in accordance with VA Standard Policies and Procedures needed to perform their tasks; and complete VA Privacy and Information Security Awareness and Rules of Behavior, Privacy, and HIPAA training and are re-certified annually. They must also sign the Rules of Behavior and Non-Disclosure Agreements

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

Yes

1. Security Plan Status: **Approved**
2. Security Plan Status Date: **6 Jul 2021**
3. Authorization Status: **ATO**
4. Authorization Date: **30 Jul 2021**
5. Authorization Termination Date: **26 Jan 2022**
6. Risk Review Completion Date: **20 Jul 2021**
7. FIPS 199 classification: **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?

This question is related to privacy control UL-1, Information Sharing with Third Parties.

No

9.2 Identify the cloud model being utilized.

This question is related to privacy control UL-1, Information Sharing with Third Parties.

N/A

9.3 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

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

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

N/A

9.5 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?

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

N/A

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

N/A

Section 9. 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**

ID	Privacy Controls
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.

SHONTA J. WRIGHT 105740

Digitally signed by SHONTA J. WRIGHT 105740
Date: 2021.09.21 12:01:26 -04'00'

Privacy Officer, Shonta Wright

BOBBI DEE BEGAY

Digitally signed by BOBBI DEE BEGAY
Date: 2021.09.22 07:39:13 -06'00'

Information Systems Security Officer, Bobbi Begay

Christopher Brown 101386

Digitally signed by Christopher Brown 101386
Date: 2021.09.20 12:41:13 -05'00'

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).

https://www.oprm.va.gov/docs/Current_SORN_List_10_7_2020.pdf

http://www.gpo.gov/fdsys/pkg/FR-2012-10-31/pdf/2012-26804.pdf

https://www.gpo.gov/fdsys/pkg/FR-2013-11-06/pdf/2013-26520.pdf