Privacy Impact Assessment for the VA IT System called:

Adobe Experience Manager for Managed Services -GovCloud - E

Veterans Health Administration

Patient Care Services | Geriatrics and Extended Care

eMASS ID #1419

Date PIA submitted for review:

4/17/2025

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Dennis Lahl	Dennis.Lahl@va.gov	202-461-7330
Information System Security Officer (ISSO)	Scott Miller	Scott.Miller@va.gov	717-413-1940
Information System Owner	David Croall	David.Croall@va.gov	240-586-1680

Abstract

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

Adobe Experience Manager for Managed Services (AEMMS) – GovCloud Software as a Service (SaaS) will allow the State Home Per Diem Program (SHPDP) - to automate the 10-10 State Home (SH) process in the vendor-managed cloud to reduce delays that Veterans experience with the current manual application process; securely provide discrete data needed to conduct detailed analyses of the entire process and identify areas of improvement; and decrease the amount of improper payments made by VA to State Veterans Homes (SVHs) and VA Medical Centers (VAMCs) of jurisdiction. Automation will also enable the SHPDP to comply with the Data Act by providing the information needed to track compliance with the 10-day submission process. The data will be maintained by the vendor and hosted within the Adobe environment on AWS GovCloud and authorized for use at the Federal Risk and Authorization Management Program (FedRAMP) Moderate impact level. The FedRAMP framework includes continuous monitoring of baseline controls for security and encryption. Therefore, when the data is entered on the form, e.g., Date of Birth (DOB), Social Security number (SSN), address, etc., that data is secure in the FedRAMP environment when in process and when at rest. The archive of the10-10SH process data that was processed via workflow, a link will then be sent, and data will be downloaded and uploaded to the 10-10SH VA Share Point site where the VA retains the data for auditing and historical access.

Overview

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

1 General Description

A. What is the business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?
Adobe Experience Manager for Managed Services (AEMMS) – GovCloud - E, Owner is State Home Per Diem Program (SHPDP), under the Veterans Health Administration (VHA) Patient Care Services (PCS), Geriatrics and Extended Care (GEC).

The Adobe Experience Manager for Managed Services (AEMMS) – GovCloud Software as a Service (SaaS) will allow the State Home Per Diem Program (SHPDP) Office to automate the 10-10 State Home (SH) process in the vendor-managed cloud to reduce delays that Veterans experience with the current manual application process; securely provide discrete data needed to conduct detailed analyses of the entire process and identify areas of improvement; and decrease the amount of improper payments made by VA to State Veterans Homes (SVHs) and VA Medical Centers (VAMCs) of jurisdiction.

Automation will also enable the SHPDP to comply with the Data Act by providing the information needed to track compliance with the 10-day submission process.

B. *Who is the owner or has control of the IT system or project? If the system has an eMASS entry, ensure this information matches with the eMASS entry.*
The owners are State Home Per Diem Program (SHPDP), under the Veterans Health Administration (VHA) Patient Care Services (PCS), Geriatrics and Extended Care (GEC).

2. Information Collection and Sharing

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

Veteran applications will be stored for a 45-day period, during the 45-day period the total number of applications may vary. The average number of applications at any time could be approximately 2,000 to 3,000 applications.

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

D. *What is a general description of the information in the IT system and the purpose for collecting this information?*
Veteran information collected to allow the State Home Per Diem Program (SHPDP) Office to automate the 10-10 (SH) process in the vendor-managed cloud to reduce delays that Veterans experience with the current manual application process:

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

No information is shared externally to the VA besides the State Veterans Homes. Information is shared with State Homes Per Diem Program (SHPDP) and VA Medical Centers doing approval through the AEMMS system.

VA State Home Per Diem (SHPD) Documentation Storage SharePoint Site	Name, Social Security Number (SSN), Date of Birth (DOB), Personal Address, Sex, Current Medications, Mother's Maiden Name, Personal Phone Number, Personal Email Address, Emergency Contact Information (Name, Phone), Health Insurance Beneficiary Number, Previous Medical Records, Race/Ethnicity, Financial Information, Military Service and Active-Duty Separation Information, Marital Status	VA SHPD Documentation Storage SharePoint Site
Veterans' Health Administration VA Medical Centers	Name, Social Security Number (SSN), Date of Birth (DOB), Personal Address, Sex, Current Medications, Mother's Maiden Name, Personal Phone Number, Personal Email Address, Emergency Contact Information (Name, Phone), Health Insurance Beneficiary Number, Previous Medical Records, Race/Ethnicity, Financial Information, Military Service and Active-Duty Separation Information, Marital Status	VPN/IPSEC Tunnel as required by the VA administrators to be installed on Linux

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

Yes, the modules/subsystems are applicable because the system receives, stores, or shares data with the modules/subsystems outside of AEMMS.

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

Yes, the system is operated in more than one site. The data will be maintained by the vendor and hosted in the Adobe Experience Manager for Managed Services – GovCloud

environment authorized for use at the Federal Risk and Authorization Management Program (FedRAMP).

The FedRAMP framework includes continuous monitoring of baseline controls for security and encryption. Therefore, when the data is entered on the form, e.g. Date of Birth (DOB), Social Security number (SSN), address, etc., that data is secure in the FedRAMP environment when in process and when at rest.

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

H. What is the citation of the legal authority and SORN to operate the IT system?

SORN 24VA10A7 / 85 FR 62406 "Patient Medical Records-VA", https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf. Authority for maintenance of the system: Title 38, United States Code, Sections 501(b) and 304.

147VA10 / 86 FR 46090 "Enrollment and Eligibility Records-VA", https://www.govinfo.gov/content/pkg/FR-2021-08-17/pdf/2021-17528.pdf. Authority for maintenance of the system: Title 28, United States Code, title 38, U.S.C., sections 501(a), 1705, 1710, 1722, and 5317.

I. What is the SORN?

SORN 24VA10A7 / 85 FR 62406 "Patient Medical Records-VA"

147VA10 / 86 FR 46090 "Enrollment and Eligibility Records-VA"

J. SORN revisions/modification

No SORN revisions and modifications to list for this system.

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

No. There are no effects on connections or sharing. The SORNs applicable to this data collection will not require amendment or revision and approval.

4. System Changes

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

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

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

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

Section 1. Characterization of the Information

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

1.1 Information collected, used, disseminated, created, or maintained in the system.

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

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

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

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

☒ Name
☒ **Full** Social Security Number
☒ **Partial** Social Security Number
☒ Date of Birth
☒ Mother's Maiden Name
☒ Personal Mailing Address
☒ Personal Phone Number(s)
☐ Personal Fax Number
☒ Personal Email Address
☒ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
☒ Financial Information
☒ Health Insurance Beneficiary Numbers Account Numbers
☐ Certificate/License numbers[1]
☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☒ Medications
☒ Medical Records
☒ Race/Ethnicity
☐ Tax Identification Number
☒ Medical Record Number
☒ Sex
☐ Integrated Control Number (ICN)
☒ Military History/Service Connection
☒ Next of Kin

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

☐ Date of Death
☐ Business Email Address
☐ Electronic Data Interchange Personal Identifier (EDIPI)
☒ Other Data Elements (list below)

Other PII/PHI data elements: PIV, Unique Identifying Number, Power of Attorney, Social Work Assessment, Marital Status

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

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

Veteran data is provided from the veteran or representative to State Veterans Home (SVH) staff as an application for benefit. The SVH staff enter the Veteran data on the Web form on the behalf of Veteran.

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

Data can be collected from the individual, State Home in the following ways:

- *From the veteran*
- *Through the Power of Attorney (POA)*

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

SVH completes form for review by VA SHPDP. A record is created through the collection of data to determine if veteran is eligible for the program.

1.3 Methods of information collection
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

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

The information is collected by the State Home and VAMC team via a Web-based form on the VA 10-10SH (OMB Approval No. 2900-0160). The form data resides on the: AEMMS Server. VA personnel will access the AEMMS Server to retrieve any VA 10-10SH forms for review and approval. The AEMMS Server Web Based system will be SSL based.

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

(OMB Approval No. 2900-0160)

1.4 Information checks for accuracy, and how often will it be checked.

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

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

The VA employee physically verifies the submitted data against the data stored in the Veterans Information Systems and Technology Architecture (VISTA - VAEC-AWS), Veterans Information Solution (VIS), and Veterans Benefits Management System (VBMS) to ensure correct eligibility, level of care and per diem payment has been approved.

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

No, this system does not access any other information or systems.

1.5 Identify the specific legal authorities, arrangements, and agreements that defined the collection of information.

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

Legal authorities:

Generally, the Authority to Operate the Veterans Health Administration (VHA) comes from Title 38 U.S. Code Authority: 38 U.S.C. 101, 501, 1710, 1720, 1741-1743, 1745, and as follows.

- Section 51.20 and 51.30 also issued under 38 U.S.C. 511, 1742, 7104 and 7105.
- Section 51.42 also issued under 38 U.S.C. 510 and 1744.
- Section 51.43 also issued under 38 U.S.C. 1712.
- Section 51.310 also issued under 38 U.S.C. 1720(f)
- Function of the SSN is to authorize payment to the State Veterans Home based on the veteran.
- Authority to collect the SSN under Title 38 USC 501 and Executive Order 9397
- Veterans Affairs System of Record Notice (VA SORN)
    - 24VA10P2, Patient Medical Records-VA (8-14-2014)
    - 147VA10NF1, Enrollment and Eligibility Records-VA'' (7-14-2016)
- Collection OMB Number: 2900-0160

- This information is collected under the authority of Title 38 CFR Part 51. The information requested on this form is solicited under the authority of Title 38, U.S.C., Sections 1741, 1742, 1743 and 1745. It is being collected to enable us to determine the eligibility for medical benefits in the State Home Program and will be used for that purpose. The income and eligibility that is supplied may be verified through a computer matching program at any time and information may be disclosed outside the VA as permitted by law; possible disclosures include those described in the "routine uses" identified in the VA system of records 24VA136, Patient Medical Record-VA, published in the Federal Register in accordance with the Privacy Act of 1974. Disclosure is voluntary; however, the information is required in order to determine the eligibility for the medical benefit for which is applied. Disclosure of Social Security number(s) of benefits claimed is requested under the authority of Title 38, U.S.C., and is voluntary. Social Security numbers will be used in the administration of veterans' benefits, in the identification of veterans or persons claiming or receiving VA benefits and their records and may be used for other purposes where authorized by Title 38, U.S.C., and the Privacy Act of 1974 (5 U.S.C. 552a) or where required by other statute.

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: The State Home completes the form with inaccurate information.

Mitigation: Once the VA receives the submitted form the VA employee verifies the veteran data in the Veterans Information Systems and Technology Architecture (VISTA - VAEC-AWS), Veterans Information Solution (VIS), and Veterans Benefits Management System (VBMS).

Section 2. Uses of the Information

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

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

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

PII/PHI Data Element	Internal Use	External Use
Veteran name	Required for identity on the application for benefit	State Home data entry & request for approval
Date of birth (DOB)	Required for identity on the application for benefit	State Home data entry & request for approval
Personal Mailing Address	Required for identity on the application for benefit	State Home data entry & request for approval
Sex	Required for identity on the application for benefit	State Home data entry & request for approval
Mother's Maiden Name	Required for identity on the application for benefit	State Home data entry & request for approval
Personal Phone Number(s)	Required to identify next of kin	State Home data entry & request for approval
Personal Email Address	Required to identify next of kin	State Home data entry & request for approval
Emergency Contact Information (Name, Phone)	Required to identify next of kin	State Home data entry & request for approval
Race/Ethnicity	Required to ensure services provided by State Home meets Veteran's needs or condition of care	State Home data entry & request for approval
Health Data	Required to ensure services provided by State Home meets Veteran's needs or condition of care	Not used
Health Insurance Beneficiary Numbers	Required to ensure services provided by State Home meets Veteran's needs or condition of care	Not used
Medications	Required to ensure services provided by State Home	Not used

	meets Veteran's needs or condition of care	
Medical Records	Required to ensure services provided by State Home meets Veteran's needs or condition of care	Not used
Financial Information	Required to identify Veteran's need in domiciliary level of care	Not used
Social Security Number (SSN)	Required for identity on the application for benefit	Not used
PIV	Required to identify Veteran's need in domiciliary level of care	State Home data entry & request for approval
Unique Identifying Number	Required for identity on the application for benefit	Not used
Power of Attorney	Required to identify Veteran's need in domiciliary level of care	Not used
Social Work Assessment (SWA)	Required for identity on the application for benefit	Not used
Military History/Service Connection	Required for identity on the application for benefit	Not used
Marital Status	Required for identity on the application for benefit	Not used

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

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

There are no reports generated in relationship to data. All forms will be uploaded to a VA Sharepoint site and VA will have the ability to pull the data for VA reporting purposes.

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

the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

The system does not create or make available new or previously unutilized information about an individual.

2.3 How the information in the system is secured.

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

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

Data is sent over HTTPS encryption and the entire server including filesystem and database are encrypted at rest. The security protocol of the data during the transmission is Secure Sockets Layer (SSL). There are certain project-level controls, such as user authentication, that will fall to the customer (VA stakeholders) to implement. New Relic (FedRAMP authorized tool) will be used by the CSP to provide environment metrics for better uptime.

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

Access Controls (ACs) are in-place to make sure only Roles allowed to view the information. The full SSN is not visible to users after initial input. Only the last 4 digits are visible. The system maintains group access to manage access control.

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

The AEMMS System uses access controls to protect PII/PHI data referenced on whitehouse.gov (Link found in Appendix A). The 10-10SH team provides access to the Administration teams for both the VAMC and State Home (SHPDP) teams. Those teams can then grant access to their team members through AWS GovCloud, which is FedRAMP Moderate. Application uses the State Home and VAMC identifiers to limit access. This is a role-based access.

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

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

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

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

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

2.4a How is access to the PII determined?

PII is determined through User Management. VA associates users and groups with roles equivalent to their day-to-day responsibilities. The process for managing and approving user permissions will be up to the VA's policy and processes since VA further delegates access to SVH and VAMC admins at each local facility.

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

VA has the responsibility to document who gets what roles. Whatever Access Controls a local State Home (SHPDP) submits is what they have access to in the User Guide for AEMMS, this link is on the AEMMS website. If these are not submitted to the VAMC, the ACs are not available.

2.4c Does access require manager approval?

Yes. Access can either be set up using defined approvers or line manager approval. The application needs to interface with a system that houses that information. The PII information in the platform will require manager approval on the State Home or VAMC teams. The Local site admin at the SVH or VAMC is responsible for all approvals.

For State Home employees Login.gov and Id.me (SSOe) are utilized to approve and verify individuals looking to access the AEMMS system. Certain contractors and VA personnel are approved via the VA PIV card process (SSOi).

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

AEMMS will track all access to the forms through an auditing feature that will be able to pull data related to user's last login and certain actions related to the Online 10-10SH. Data will be retained following VA retention rules. Data is maintained on AEMMS for a minimum of 45 days and purged after completion. The backup tapes are through 1 week outside of this. New Relic maintains log files for 1 year.

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

AEMMS is responsible for setting up the technical safeguards and for any safeguards that fall under the responsibility of AEMMS per documentation in FedRAMP #F1509037239. Safeguards with the application (i.e. user management) will be VAs responsibility. A workflow is created for State Home (SHPDP) and VAMC that will enforce assignments for respected parties re: the approval process mentioned in 2.4c.

Below are the teams responsible for assuring the safeguards are in place:

Health Information Manager at the State Home
VAMC State Home Per Diem POC
Software as a Service Information Manager/Adobe FedRAMP Managed Services.

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*

- Name
- Social Security Number (SSN)
- Date of birth (DOB)
- Personal Mailing Address
- Sex
- Medications
- Mother's Maiden Name
- Personal Phone Number(s)
- Personal Email Address
- Emergency Contact Information (Name, Phone, etc.)
- Health Insurance Beneficiary Numbers
- Current Medications
- Previous Medical Record
- Race/Ethnicity
- Health/medical information
- Military History/Service Connection

3.2 How long is information retained?

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

Records entered this web-based application will not remain in the application. SHPDP official files/documents are retained at the VAMC of Jurisdiction until they are inactive for six years after final payment or cancellation, but longer retention is authorized if required for business use. (GRS 1.1, Item 010) (DAA-GRS-2013-0003-0001).

3.3 The retention schedule approved by the VA records office and the National Archives and Records Administration (NARA).

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

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

Yes, VHA Record Control Schedule (RCS) 10–1
https://vaww.va.gov/vhapublications/rcs10/rcs10-1.pdf
4000.1b Financial transaction records related to procuring goods and services, paying bills, collecting debts, and accounting. (see section 3.2 above)

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

The records retention schedule, series, and disposition authority can be found in SORN 24VA10A7 / 85 FR 62406 “Patient Medical Records-VA", https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf . Authority for maintenance of the system: Title 38, United States Code, Sections 501(b) and 304.

The records will be Electric Health Record (EHR) via Paper Source Documents and Interim Electronic Source Information.

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

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

Destruction of Records (Paper and Compact Disk)

For the destruction of Records you (business owner) and your Department Records Liaison will complete the VA Form 7468.

Destruction of Stored records: Pull the form from the box, then complete the electronic version of the VA Form 7468.

Department Records Liaison will submit the VA Form 7468 to VHA 12PCS Records Officer for routing, approval, and the authority to destroy. AEMMS has an out-of-box purge operation which is configured to delete all database records and filesystem records

for a given 10-10SH. AEMMS has configured the purge interval to run nightly and purge any completed workflow process more than 45 days old. The participants of the 10-10SH process have 45 days before it is removed from their inbox and placed in the archival queue. The 45-day purge date starts when the 10-10SH is archived.

The VHA Office of Geriatrics and Extended Care has program management responsibility of SHPDP will verify eligibility of the records for destruction and sign the VA Form 7468, on line 18a and 18b. VA Form 7468 will be returned to the Department Records Liaison who will sign line 19a and 19b to verify destruction is completed.

A signed copy of the VA Form 7468 will be returned to the VHA Office of Geriatrics and Extended Care has program management responsibility of SHPDP Records Manager via email or hand delivered.

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

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

This system is not used for testing, training, or research.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

Principle of Minimization: The project retains only the information necessary for its purpose, additionally, the PII is retained only for as long as necessary and relevant to fulfill the specified purposes.

Principle of Data Quality and Integrity: The PIA should describe policies and procedures for how PII that is no longer relevant and necessary is purged.

This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:

Privacy Risk: Retention of data/information is maintained beyond the disposition date poses a risk of exposure, disclosure, access and need to provide to an outside requester.

Mitigation: Information is located on the secure SharePoint behind the VA firewall. A SharePoint is accessed through PIV access by VA employees only. Permissions are granted by the SHPDP Office and monitored monthly or when new employees are added or deleted by 10N Designation Letter.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

PII Mapping of Components

4.1a Adobe Experience Manager for Managed Services (AEMMS) consists of 2 key components (servers/databases/instances/applications/software/application programming interfaces (API)). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Adobe Experience Manager for Managed and the reasons for the collection of the PII are in the table below.

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

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards

State Home Per Diem Program (SHPDP) Office	Yes	Yes	Name, Social Security Number (SSN), Date of birth (DOB), Address, Sex, Age, Physical Information, Health Data, Social Work Assessment, Medications, Marital Status	Complete and track application	Data is secure in the FedRAMP environment when in process and when at rest. The security protocol of the data during the transmission is SSL. There are certain project-level controls, such as user authentication.
Veterans' Health Administration VA Medical Centers (State Home Per Diem Offices)	Yes	Yes	Name, Social Security Number (SSN), Date of birth (DOB), Address, Sex, Age, Physical Information, Health Data, Social Work Assessment, Medications, Marital Status	Complete and track application	Data is secure in the FedRAMP environment when in process and when at rest. The security protocol of the data during the transmission is SSL. There are certain project-level controls, such as user authentication.

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

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

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

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

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

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

Data Shared with Internal Organizations

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
VA State Home Per Diem (SHPD) Documentation Storage SharePoint Site	State Home Per Diem Program (SHPDP) Office needs to share information because this program will serve as AEMMS' storage site.	Name, Social Security Number (SSN), Date of birth (DOB), Mother's Maiden Name, Personal Mailing Address, Personal Email Address, Emergency Contact Information (Name, Phone, etc.), Financial Information, Health Insurance Beneficiary Numbers, Medications, Medical Records, Race/Ethnicity, Sex, Military History/Service, Marital Status	VA SHPD Documentation Storage SharePoint Site
Veterans' Health Administration VA Medical Centers	State Home Per Diem Offices will share information with this Program as the VA is the primary resource to Veterans and staff who will benefit from AEMMS.	Name, Social Security Number (SSN), Date of birth (DOB), Mother's Maiden Name, Personal Mailing Address, Personal Email Address, Emergency Contact Information (Name, Phone, etc.), Financial	VPN/IPSEC Tunnel as required by the VA administrators to be installed on Linux servers

IT system and/or Program office. Information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List PII/PHI data elements shared/received/transmitted.*	*Describe the method of transmittal*
		Information, Health Insurance Beneficiary Numbers, Medications, Medical Records, Race/Ethnicity, Sex, Military History/Service, Marital Status	

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: If persons without a need to know in the performance of their duties have access to Veteran Data.

Mitigation: The FedRAMP framework includes continuous monitoring of baseline controls for security and encryption. Therefore, when the data is entered on the form, e.g. DOB, SSN, address, etc., that data is secure in the FedRAMP environment when in process and when at rest. Permissions or control for access are granted and monitored routinely by VA staff. Information is reviewed by Chief of SHPDP Office. AEMMS is responsible for reporting an unauthorized access, and the system would be shut down until resolved. Detailed information is contained in the AEMMS FedRAMP documentation, which may be requested by the VA. AEMMS does not provide public access.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

Data Shared with External Organizations

List IT System or External Program Office information is shared/received with	***List the purpose of information being shared / received / transmitted***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)***	***List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
State Veteran's Home per Diem	Complete and process State Veteran Home per diem request	Name, Social Security Number (SSN), Date of birth (DOB), Mother's Maiden Name, Personal Mailing Address, Personal Email Address, Emergency Contact Information (Name, Phone, etc.), Financial Information, Health Insurance Beneficiary Numbers, Medications, Medical Records, Race/Ethnicity, Sex, Military History/Service, Marital Status	Contract	SSL or create a VPN/IPSEC Tunnel as required by the State Homes Network security with the VA administrators to be installed on Linux servers

Adobe Experience Manager (AEMMS) Forms Managed Services - Enterprise	Complete and process State Veteran Home per diem request.	Name, Social Security Number (SSN), Date of birth (DOB), Mother's Maiden Name, Personal Mailing Address, Personal Email Address, Emergency Contact Information (Name, Phone, etc.), Financial Information, Health Insurance Beneficiary Numbers, Medications, Medical Records, Race/Ethnicity, Sex, Military History/Service, Marital Status	Contract and Business Associate Agreement	SSL or create a VPN/IPSEC Tunnel as required by the State Homes Network security with the VA administrators to be installed on Linux servers

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

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

Follow the format below:

Privacy Risk: The contractor would use VA data for unintended purposes, not in accordance with the contract.

Mitigation: All personnel with access to Veteran's information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually. SORNS identified in this PIA. Information is shared in accordance with SORNS identified in this PIA. All personnel accessing Veteran's information must first have a successfully adjudicated fingerprint check. This fingerprint check is conducted by the Federal Bureau of Investigation (FBI) Justice Information and criminal history records. Internal VA users access Veteran's data through Personal Identity Verification (PIV) card and an additional ID and password for those with elevated privileges. The State Home uses Login.gov or ID,me for authentication to the system. This ensures the identity of the user by requiring two-factor authentication. AEMMS does not provide public access. The Business Associate agreement supports the protections of the VA data by outlining additional requirements in accordance with HIPAA to include the contractor providing self-reporting about any incidents. Vendor has FedRAMP Certification that

requires implementation in accordance with organizational/federal requirements and is working to complete Risk Management Framework process to receive a VA authority to operate.

Section 6. Notice

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

6.1 The notice provided to the individual before collection of the information. Please provide a copy and/or screen shot of a web notice of the notice as an Appendix-A 6.1 on the last page of the document. (A notice may include a posted privacy policy, a Privacy Act notice on forms, notice given to individuals by the sources system, or a system of records notice published in the Federal Register.) If notice was not provided, explain why.

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

6.1a Provide the Privacy Notice provided to the public by this system or any source systems. Include a copy of the notice in Appendix A of the PIA, the Federal Register citation, or Privacy Statement from collection of information such as forms or surveys.

Yes, as per the 10-10SH, 10-10EZ/EZR, and 10-5588/A forms Privacy Act statement on forms. The links and Privacy Notice Attachment can be found in Appendix A.

6.1b If notice was not provided, explain why.

AEMMS provides the Privacy notice.

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

Every 10-10SH when opened displays a notice regardless of when it is opened which includes the archived state. The notice is provided in the 10-10SH form. The State Veteran Home's (SVH) intake specialist briefs the 10-10SH Privacy Act statement with the Veteran about how the collection of information will be used to complete the form in accordance with 38 CFR 51. The current notice is attached.

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.

Yes, the right to decline is available during admission process at the SVH. And denial of service may occur. However, eligibility will not be provided without all required information being provided. No allowance of per diem payment may be granted unless

the admission package is completed fully as required by law (38 CFR Part 51). (See Appendix A)

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.

Yes, as per the 10-10SH, 10-10EZ/EZR, and 10-5588/A forms Privacy Act statement on forms. See 38 CFR Part (https://www.law.cornell.edu/cfr/text/38/part-51) Once information is provided to the VA, the records are used, as necessary, to ensure the administration of statutory benefits to all Veterans eligible for nursing home care.

As such, the SHPDP Office does not provide individuals with the direct opportunity to consent to uses of information on the designated form. However, if an individual wish to remove consent for a particular use of their information, they or their representative should contact the nearest VA regional office, a list of which can be found at http://benefits.va.gov/benefits/offices.asp.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

Principle of Transparency: This is referring to sufficient notice provided to the individual.

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

Privacy Risk: Privacy rights are not provided before the collection occurs, no written notice and no signature obtained.

Mitigation: The VA mitigates this risk by providing veterans and other beneficiaries with multiple forms of notice of information collection, retention, and processing. Veterans are provided multiple forms of notice: VA Form Privacy Act statement upon enrollment of benefits, Federal Register posting of the System of Record Notice, this Privacy Impact Assessment and all Veterans are mailed a Notice of Privacy Practices every 3 years.

Section 7. Access, Redress, and Correction

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

7.1 The procedures that allow individuals to gain access to their information.

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

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. ***For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at [VA Public Access Link-Home (efoia-host.com)] to obtain information about FOIA points of contact and information about agency FOIA processes.***

CFR 38 Part 51. As per the 10-10SH and 10-10EZ/EZR forms Privacy Act statement on forms (see Appendix A). These documents are maintained as part of the VAMC record, therefore the request for records would be submitted to the VA Medical Center.

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

This system is not exempted from the access provisions of the Privacy Act.

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

This system is not exempted from the access provisions of the Privacy Act.

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.

Please see VHA Directive 1605.01 for additional details on the procedures related to correcting inaccurate or erroneous information:

1. An individual may request amendment of a record pertaining to him or her contained in a specific VA system of records by mailing or delivering the request to the office concerned. The request must be in writing and must conform to the requirements in the VHA Directive. It must state the nature of the information in the record the individual believes to be inaccurate, irrelevant, untimely, or incomplete; why the record should be changed; and the amendment desired. The requester should be advised of the title and

address of the VA official who can assist in preparing the request to amend the record if assistance is desired.

2. Not later than 10 days, excluding Saturdays, Sundays, and legal public holidays, after the date of receipt of a request to amend a record, the VA official concerned will acknowledge in writing such receipt. If a determination has not been made, the acknowledgement will inform the individual when he or she may expect to be advised of action taken on the request. VA will complete a review of the request to amend or correct a record as soon as reasonably possible, in most cases within 30 days from receipt of the request.

3. Where VA agrees with the individual's request to amend his or her record(s), the requirements of 5 U.S.C. 552a(d) will be followed. The record(s) will be corrected, and the individual will be advised of the correction.

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 made aware of the procedures for correcting his or her information through the Privacy Act Notice provided at the time of data collection. An individual may request amendment of a record pertaining to him or her contained in a specific system of records by mailing or delivering the request to the office concerned.

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

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

Please see VHA Directive 1605.01 (and Section 7.1 above) for details on relating to accessing and corrections or amendments to those records.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department's access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. ***For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals***

involved might change their behavior. *(Work with your Privacy Officer (PO) to complete all Privacy Risk questions in this section).*

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

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

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

Follow the format below:

Privacy Risk: Veterans do not have access to the data maintained in the contractor system, therefore they do not know if their information is accurate.

Mitigation: Data is collected at the point of service and verified by the State Home staff in the VAMC. Veterans would seek correction from the SH VAMC supporting where the veteran will be located.

Section 8. Technical Access and Security

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

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

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

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

Once verified, VA users will work with the VAMC site admin to be provisioned into the Adobe Experience Manager portal with the proper roles and permissions based on their day-to-day responsibilities with the 10-10SH. The State Home admin works with their users to provide portal access and proper roles and permissions. The Health Information Manager works with State Home admins to approve this user access.

Upon State Home separation or as access is identified as no longer needed by State Home, the employee's access is deactivated, and an IT Ticket is submitted to remove their profile from the system.

All VA users leverage a VA PIV for authentication purposes. Site access is restricted to VAMC employee PIV card/ Identity and Access Management (IAM) by Registration of Users authenticated by the SHPDP Office. Registration of Users authenticated by the SHPDP Office. All users of this VA information and information systems are responsible for complying with the rules outlined in the VA National Rules of Behavior, as well as procedures and practices developed in support of the Rules of Behavior. All VA personnel with access to Veteran's information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually.

All non-VA users must complete a profile and verify their identity through ID.me or Login.gov. Non-VA staff are subject to a background investigation before given access to Veteran's information.

Access is granted by least privilege access which access is outlined by the employee job titles.

The SHPDP Office doesn't grant access to any other agency.

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

Users from other agencies will not have access to the system.

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

VA State Home per Diem Program (SHPDP) Administrative Staff admins can assign roles and receive notifications of the applications being completed.

The Clinical Team members can enter resident information.

Signature abilities are restricted by section; however, the SHPDP Administrative staff can assign these privileges.

The VA have read-only access for the review of the State Home only portion of the 10-10SH form.

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

Yes, contractors can have access to PII.

8.2b. What involvement will contractors have with the design and maintenance of the system?

Contractor access is determined by the VA System Owner regarding Role and Access; the controls of periodic review will inherit from the current controls in place for: Active Directory. The clearance requirements will follow VA Directive and Handbook 0735 and VHA Directive to obtain a CAC/PIV card.

The contractor aids in routine maintenance in AEMMS, which involves the contractor optimizing indexes for efficient queries, cleaning up old content revisions and unreferenced data to manage repository growth, and purging completed workflows daily. Regularly managing audit logs, monitoring disk space, and scheduled launches facilitate pre-planned updates.

Here is a link that provides further context to AEMMS site maintenance.

8.2c. Does the contractor have a signed confidentiality agreement?

BAA is in place between VA and Four Points Technology, LLC, last reviewed 9/2024.

8.2d. Does the contractor have an implemented Business Associate Agreement for applicable PHI?

BAA is in place between VA and Four Points Technology, LLC, last reviewed 9/2024.

8.2e. Does the contractor have a signed non-Disclosure Agreement in place?
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.

The contractor, Four Points Technology, LLC. does have a signed Non-Disclosure Agreement in place.

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.

> As per the VHA Privacy training modules in Talent Management System (TMS). Personnel who will be accessing information systems must read and acknowledge their receipt and acceptance of the VA Information Security Rules of Behavior (RoB) prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training that all personnel must complete via the VA's TMS. After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training. Acceptance obtained through electronic acknowledgment is tracked through the TMS system. All VA employees that have access to VA data or systems must complete the VA 10176: Privacy and Info Security Awareness and Rules of Behavior training. Additional training may include but is not limited to, the following TMS Courses:

VA 10203: Privacy and HIPAA Training
VA 3812493: Annual Government Ethics

And dependent on the role of the individual:

VA 1016925: Information Assurance for Software Developers IT Software Developers
VA 1357084: Information Security Role-Based Training for Data Managers
VA 64899: Information Security Role-Based Training for IT Project Managers
VA 3197: Information Security Role-Based Training for IT Specialists
VA 1357083: Information Security Role-Based Training for Network Administrators
VA 1357076: Information Security Role-Based Training for System Administrators
VA 3867207: Information Security Role-Based Training for System Owners
VA 3914040: Contingency Plan – Role-Based Training
VA 64880: Information Security and Privacy Role-Based Training for VA Executives
VA 64859: Information Security and Privacy Role-Based Training for Acquisition Personnel
VA 3867207: Information Security and Privacy Role-Based Training for Information System Owners
VA 4481886: Information Security and Privacy Role-Based Training for Non-Technical Roles

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 10/25/2023
3. *The Authorization Status:* Authorization to Operate (ATO)
4. *The Authorization Date:* 5/10/2024
5. *The Authorization Termination Date:* 5/10/2025
6. *The Risk Review Completion Date:* 5/3/2024
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* MODERATE

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

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

This system has an ATO.

Section 9 – Technology Usage

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

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

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties. ***(Refer to question 1.8 of the PTA)***

This system is a Software as a Service (SaaS) that uses cloud technology. The system is currently FedRAMP Authorized and active on the FedRAMP Marketplace under FedRAMP ID F1509037239.

9.2 Does the contract with the Hosting Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). ***(Refer to question 3.3.1 of the PTA)*** *This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

The office of Patient Care Services (PCS) has ownership rights over data including PII. The contract number is NNG15SD22B 36C1023F0091 - 10-10SH Modernization SaaS.

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.

Logging information is stored on: New Relic Service also on AWS GovCloud; the data is stored is subject to the same policies as the AEM Server. The Adobe team has ownership of this information; however, the VA can attain access to this information by reaching out to CSC.

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

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

Yes. Adobe Managed Services is separated in terms of access from the rest of Adobe. Only personnel that support the project have access. The Adobe Consultants need VA permission to gain access as do any other Adobe employees.

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).

The system does not use RPA.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

ID	Privacy Controls
AP	**Authority and Purpose**
AP-1	Authority to Collect
AP-2	Purpose Specification
AR	**Accountability, Audit, and Risk Management**
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-7	Privacy-Enhanced System Design and Development
AR-8	Accounting of Disclosures
DI	**Data Quality and Integrity**
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
DM	**Data Minimization and Retention**
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
IP	**Individual Participation and Redress**
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
SE	**Security**
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR	**Transparency**
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

DENNIS LAHL Digitally signed by DENNIS LAHL
Date: 2025.05.02 15:59:34 -04'00'

Privacy Officer, Dennis Lahl

SCOTT MILLER Digitally signed by SCOTT MILLER
Date: 2025.04.25 11:50:18 -04'00'

Information System Security Officer, Scott Miller

DAVID CROALL Digitally signed by DAVID CROALL
Date: 2025.05.09 09:32:45 -04'00'

Information System Owner, David Croall

APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy; a Privacy Act notice on forms; screen shot of a website collection privacy notice). Link showing AEMMS compliance to OMB Memorandum M-06-15: https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2006/m-06-15.pdf

The below links are SORNS that apply to the AEMMS system notice.

https://www.federalregister.gov/documents/2019/07/30/2019-16102/agency-information-collection-activity-state-home-programs-for-veterans

https://www.federalregister.gov/documents/2020/04/23/2020-08611/privacy-act-of-1974-system-of-records

https://www.govinfo.gov/content/pkg/FR-2020-04-23/pdf/2020-08611.pdf

10-10 SH Privacy Statement: https://vaww.va.gov/vaforms/Search_action.asp

10-10SH (PDF) State Home Program Application for Veteran Care Medical Certification 06/01/2016 09/2016 5

PAPERWORK REDUCTION ACT OF 1995 AND PRIVACY ACT STATEMENT

The Paperwork Reduction Act of 1995 requires us to notify you that this information collection is in accordance with the clearance requirements of section 3507 of the Paperwork Reduction Act of 1995. We may not conduct or sponsor, and you are not required to respond to, a collection of information unless it displays a valid OMB number. We anticipate that the time expended by all individuals who must complete this form will average 20 minutes. This includes the time it will take to read instructions, gather the necessary facts and fill out the form. Although completion of this form is voluntary, VA will be unable to provide reimbursement for services rendered without a completed form. Failure to complete the form will have no effect on any other benefits to which you may be entitled. This information is collected under the authority Of Title 38 CFR Parts 51 and 52. The information requested on this form is solicited under the authority of Title 38, U.S.C., Sections 1741, 1742 and 1743. It is being collected to enable us to determine your eligibility for medical benefits in the State Home Program and will be used for that purpose. The income and eligibility you supply may be verified through a computer matching program at any time and information may be disclosed outside the VA as permitted by law; possible disclosures include those described in the "routine uses" identified in the VA system of records 24VA136, Patient Medical Record-VA, published in the Federal Register in accordance with the Privacy Act of 1974. Disclosure is voluntary; however, the information is required in order for us to determine your eligibility for the medical benefit for which you have applied. Failure to furnish the information will have no adverse effect on any other benefits to which you may be entitled. Disclosure of Social Security

number(s) of those for whom benefits are claimed is requested under the authority of Title 38, U.S.C., and is voluntary. Social Security numbers will be used in the administration of veteran's benefits, in the identification of veterans or persons claiming or receiving VA benefits and their records and may be used for other purposes where authorized by Title 38, U.S.C., and the Privacy Act of 1974 (5 U.S.C. 552a) or where required by other statute.

10-10 EZ/EZR Privacy Statement: https://vaww.va.gov/vaforms/Search_action.asp?FormNo=10-10EZ&tkey=&Action=Search
10-10EZ (PDF) Instrucciones Para Solicitar La Afiliacion A Los Beneficios Medicos 07/13/2018 7/2018 3
10-10EZ (pdf) (PDF) Instructions For Completing Enrollment Application For Health Benefits 07/10/2016 01/2020 5
10-10EZR (PDF) Health Benefits Update Form (Fillable) 11/01/2004 01/2020 4

10-10EZ-Privacy Act Information: VA is asking you to provide the information on this form under 38 U.S.C. Sections 1705,1710, 1712, and 1722 in order for VA to determine your eligibility for medical benefits. Information you supply may be verified from initial submission forward through a computer-matching program. VA may disclose the information that you put on the form as permitted by law. VA may make a "routine use" disclosure of the information as outlined in the Privacy Act systems of records notices and in accordance with the VHA Notice of Privacy Practices. Providing the requested information is voluntary, but if any or all of the requested information is not provided, it may delay or result in denial of your request for health care benefits. Failure to furnish the information will not have any effect on any other benefits to which you may be entitled. If you provide VA your Social Security Number, VA will use it to administer your VA benefits. VA may also use this information to identify Veterans and persons claiming or receiving VA benefits and their records, and for other purposes authorized or required by law.

10-10EZR- Privacy Act Information: VA is asking you to provide the information on this form under 38 U.S.C. Sections 1710, 1712, and 1722 in order for VA to determine your eligibility for medical benefits. Information you supply may be verified from initial submission forward through a computer matching program. VA may disclose the information that you put on the form as permitted by law. VA may make a "routine use" disclosure of the information as outlined in the Privacy Act systems of records notices and in accordance with the Notice of Privacy Practices. Providing the requested information is voluntary, but if any or all of the requested information is not provided, it may delay or result in denial of your request for health care benefits. Failure to furnish the information will not have any effect on any other benefits to which you may be entitled. If you provide VA your Social Security Number, VA will use it to administer your VA benefits. VA may also use this information to identify veterans and persons claiming or receiving VA benefits and their records, and for other purposes authorized or required by law.

10-5588/A Privacy Statement: https://vaww.va.gov/vaforms/Search_action.asp?FormNo=10-5588&tkey=&Action=Search

10- 5588A (PDF) Claim for Payment for Nursing Home Care Provided to Veterans Awarded Retroactive Service Connection 05/31/2017 04/2016 2

PAPERWORK REDUCTION ACT OF 1995 AND PRIVACY ACT STATEMENT

The Paperwork Reduction Act of 1995 requires us to notify you that this information collection is in accordance with the clearance requirements of section 3507 of the Paperwork Reduction Act of 1995. We may not conduct or sponsor, and you are not required to respond to, a collection of information unless it displays a valid OMB number. We anticipate that the time expended by all individuals who must complete this form will average 20 minutes. This includes the time it will take to read instructions, gather the necessary facts and fill out the form. Although completion of this form is voluntary, VA will be unable to provide reimbursement for services rendered without a completed form. Failure to complete the form will have no effect on any other benefits to which you may be entitled. This information is collected under the authority Of Title 38 CFR Parts 51 and 52. The information requested on this form is solicited under the authority of Title 38, U.S.C., Sections 1741, 1742 and 1743. It is being collected to enable us to determine your eligibility for medical benefits in the State Home Program and will be used for that purpose. The income and eligibility you supply may be verified through a computer matching program at any time and information may be disclosed outside the VA as permitted by law; possible disclosures include those described in the "routine uses" identified in the VA system of records 24VA136, Patient Medical Record-VA, published in the Federal Register in accordance with the Privacy Act of 1974. Disclosure is voluntary; however, the information is required in order for us to determine your eligibility for the medical benefit for which you have applied. Failure to furnish the information will have no adverse effect on any other benefits to which you may be entitled. Disclosure of Social Security number(s) of those for whom benefits are claimed is requested under the authority of Title 38, U.S.C., and is voluntary. Social Security numbers will be used in the administration of veterans benefits, in the identification of veterans or persons claiming or receiving VA benefits and their records and may be used for other purposes where authorized by Title 38, U.S.C., and the Privacy Act of 1974 (5 U.S.C. 552a) or where required by other statute.

Link showing AEMMS compliance to OMB Memorandum M-06-15:
https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2006/m-06-15.pdf

HELPFUL LINKS:

Records Control Schedule 10-1 (va.gov)

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

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

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

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

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