Privacy Impact Assessment for the VA IT System called:

Central FEE

Veteran's Health Administration

Payment Operations

eMASS ID 98

Date PIA submitted for review:

11/18/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Akeel Omari	Akeel.omari@va.gov	404-828-5507
Information System Security Officer (ISSO)	Ashton Botts	Ashton. Botts@va.gov	(303)-398-7155
Information System Owner	Tony Sines	Tony.Sines@va.gov	316-249-8510

Abstract

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

The Central Fee System (Fee) at the Austin Information Technology Center (AITC) processes payments to private medical providers who provide for the treatment of veterans outside of Veterans Administration (VA) medical centers and clinics. In addition, Central Fee also reimburses veterans for associated travel and medical expenses.

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?

Central FEE processes payments to private medical providers who provide for the treatment of veterans outside of VA medical centers and clinics. In addition, Central Fee reimburses veterans for associated travel and medical expenses.

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

VA Owned and VA Operated.

2. Information Collection and Sharing

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?

Several million Veterans who have received services outside the VA. This includes current and historical data. This is an application, so the data stored is for Veteran and Vendor payment related. This data is provided through reports but access for that reporting is outside the application. The administrators of the application have access to make changes to programs through Audit change management processes.

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

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

Central Fee processes payments to private medical providers who provide for the treatment of veterans outside of VA medical centers and clinics. In addition, Central Fee reimburses veterans for associated travel and medical expenses. This includes medical care data and associated payment.

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

FMS- Payment related data and Payments
DSS- Work load capture
VSSC- Payment medical data loaded into a Data Cube for VA access to access for reporting and research.
ARC – Workload capture for providing funds back to VA facilities.
FPPS - data back to showing paid claim and adjudication information for 835 EDI message back to Vendors that provide care to Veterans.

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

F. 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.
AITC-production

PITC-Recovery site

The production and recovery site are the same configuration.

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

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

System of Record Notice SORN Non-VA Care (Fee) Records- VA 23VA10NB3 Title 5 U.S.C 301, Title 26 U.S.C 61. Title 38, U.S.C. sections 31, 109, 111, 501, 1151 1703, 1705, 1710, 1712, 1717, 1720, 1721, 1724, 1725, 1727, 1728, 1741-1743, 1781, 1786, 1787, 3102, 5701 (b)(6)(g)(2)(g)(4)(c)(1), 5724, 7105, 7332, and 8131-8137. 38 Code of Federal Regulations 2.6 and 45 CFR part 160 and 164. Title 44 U.S.C and Title 45 U.S.C. Veterans Access, Choice, and Accountability Act of 2014.

https://department.va.gov/privacy/system-of-records-notices/

H. What is the SORN?

23VA10NB3 Non-VA Care (Fee) Records- VA
https://www.govinfo.gov/content/pkg/FR-2015-07- 30/pdf/2015-18646.pdf

I. SORN revisions/modification

23VA10NB3 / 80 FR 45590 (07/30/2015)

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

No

4. System Changes

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

☐ *Yes*
☒ *No*

J. 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
- ☐ Gender/Sex
- ☐ Integrated Control Number (ICN)
- ☐ Military History/Service Connection
- ☐ Next of Kin
- ☐ Date of Death
- ☐ Business Email Address
- ☐ Electronic Data Interchange Personal Identifier (EDIPI)
- ☐ Other Data Elements (List Below)

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

Additional information
collected:
• VA Claim Information

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?
VistA Fee– Sends vendor/vet payment info; and receives payment confirmations and automated system messages which record the status of payments in Vista Fee from Central Fee. Receives report data concerning the processed payments and Authorizations.

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.

FEE system receives data via a secure electronic data transfer from other VA systems.
The sources of information for the FEE system are listed below. Bi-directional Interfaces:
• VistA Fee/FBCS – Sends vendor/vet payment info; and receives payment confirmations and automated system messages which record the status of payments in Vista Fee from Central Fee. Receives report data concerning the processed payments and Authorizations.
• Financial Management System (FMS) - Receives payment information; and Sends confirmations to Central Fee. Processes Vendor update request from Central Fee sends updates of Vendors. Provides access to FMS payment system data to assist in process of Central Fee payments.
•Statistical Analysis Software (SAS) – Sends reports and statistical data
• Healthcare Claims Processing System (HCPS) - Dialysis payment statistical data and receives rejects/accept records. Sends updates to payment information like cancellations of payment:
•Beneficiary Identification & Records Locator System (BIRLS) - Sends Notice of death – updates Central Fee veteran file.
• Analytics & Business Intelligence (ABI) (Formerly VSSC)- receives payment, Veteran and Vendor data
• Decision Support System (DSS) – receives payment information
• Allocation Resource Center (ARC)– Pulls Payment data for workload data capture
• FPPS interface EDI update back through SFTP process.

1.2c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?
Central FEE creations reports based on the payment data being processed providing processing and payment status. This includes reporting of Monthly, quarterly and annual reports and totals of various payments.

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?
FEE system receives data via a secure electronic data transfer from other VA systems listed above in section 1.2.

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?

No form is involved for Central FEE, the data is electronic.

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 system has various checks in across payments including totals and other checks that ensure the totals and data are accurate. Rejects also are sent back to stations when issue are found.

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?

As information is imported from existing VA Systems, the accuracy is verified by the original source. System automated checks includes claim and date values, and vendor must be an authorized vendor. The system validates payment lines against the batch file total. The system also validates numeric and alpha fields to determine correct value type for the entry. All data checks are accomplished by the application programming.

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

FEE data standards and internal controls are regulated within the accordance of the following:

- System of Record Notice (SORN) 23VA10NB3, Non-VA Care (Fee) Records- VA
- Title 5 U.S.C 301, Departmental regulations
- Title 26 U.S.C 61, Gross income defined
- Title 38, U.S.C. Veterans' Benefits in the United States Code, sections 31, 109, 111, 501, 1151 1703, 1705, 1710, 1712, 1717, 1720, 1721, 1724, 1725, 1727, 1728, 1741-1743, 1781, 1786, 1787, 3102, 5701 (b)(6)(g)(2)(g)(4)(c)(1), 5724, 7105, 7332, and 8131-8137.
- Code of Federal Regulations (CFR) Title 38, Pensions, Bonuses, and Veterans' Relief
- 45 CFR part 160 (HIPAA Security Rule) and 164 (Security and Privacy).
- Title 44 U.S.C (the role of public printing and documents in the United States Code)
- Veterans Access, Choice, and Accountability Act of 2014 ((H.R. 3230; Pub. L. 113–146)

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:

FEE collects Personally Identifiable Information (PII) and other highly delicate Personal Health Information (PHI). If this information was breached or accidentally released to inappropriate parties or the public, it could result in financial, personal, and/or emotional harm to the individuals whose information is contained in the system.

Mitigation:

FEE employ a variety of security measures designed to ensure that the information is not.

inappropriately disclosed or released. These measures include access control, awareness and training; audit and accountability; certification, accreditation, and security assessments. configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning. personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity.

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
Name	File Identification purposes	Not used
Personal Mailing Address	For reporting and Processing	Not used
Social Security Number (SSN)	Veteran identification	Not used
Financial information	For reporting and processing	Processing reimbursement to Veterans and payment to vendors
Medical Records	Claim Management Payment explanation of benefits	Not used
Date of Birth (DOB)	Veterans Identification	Not Used
VA Claim Information	Veterans Identification	Not used
Tax Identification Number	Veterans Identification	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?

Data validation on incoming and outgoing files. These reports are scalable to the business requirements of the authorized user. Examples would be a VA station could run a specific report on what payments were made to a specific non-VA healthcare provider for a specific veteran or a

station could run a report showing the total payments made to all non-VA healthcare providers for a specific period (quarter, semi-annual, annual).

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.

Central FEE does not interface with the veterans, Data that it is in the system comes from the system of record Vista Fee. Central FEE does not create any new data/information or derived data.

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?

All data received and stored in the system are encrypted.

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).

All data transfers and storage are encrypted along with access is controlled and monitored.

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

This application is behind the firewall and is not public facing.

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?

Access to Central FEE is controlled through the IAM and Top Secret on the mainframe. This is managed through the VA manager request/ approval. The SORN defines the information collected from veterans, use of the information, and how the information is accessed and stored. The information collected is used for determining a veteran. Benefits, such as compensation or education.

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?

The minimum-security controls for the FEE application cover 17 security areas regarding. protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems.
The security areas include access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management. contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment. systems and services acquisition; system and communications protection; and system and information integrity. The FEE application team has implemented the required security controls. based on the tailoring guidance of NIST Special Publication 800-53 Rev 4 and VA directives or handbooks. VA Records Management Policy VA 6300.1, VA 6500 HB, National Rules of Behavior (ROB), and VA 6502.1, VA6502.3, VA 6502.4 Privacy Policies govern how veterans. information is used, stored, and protected.

2.4c Does access require manager approval?

Yes

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

All access to file is logged.

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

Mainframe MFA (Multi Factor Authentication) and other controls are in place to assure proper access is controlled. This is through the mainframe TOP secrete and IAM processes.

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
• Date of Birth
• Mailing Address
• Zip Code
• Financial Account Information
• Medical codes
• VA Claim Information

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.*

Central FEE stores historic data on payment history provided to non-VA providers, in the support of patient care of a veteran, indefinitely for reporting and research. Paper and electronic documents at the authorizing healthcare facility related to authorizing the Non-VA Care (fee) and the services authorized, billed and paid for are maintained in ‘‘Patient Medical Records—VA’’ (24VA10P2). These records are retained at healthcare facilities for a minimum of three. years after the last episode of care. After the third year of inactivity the paper records are transferred to a records facility for seventy-two (72) more years of storage. Automated storage media, imaged Non-VA Care (fee) claims, and other paper documents that are included in this. system of records and not maintained in ‘‘Patient Medical Records—VA’’ (24VA10P2) are. retained and disposed of in accordance with disposition authority approved by the Archivist of the United States. Paper records that are imaged for viewing electronically are destroyed after. they have been scanned, and the electronic copy is determined to be an accurate and complete. copy of the paper record imaged.
The Records Control Schedule (RCS) 10-1 provides Veterans Health Administration (VHA) records retention and disposition requirements for VHA Central Office, Program Offices, and field facilities. The National Archives and Records provides the General Records Schedule (GRS) disposal authorities for temporary administrative records common to all Federal agencies. It covers records relating to personnel, budget and finance, procurement, information. technology, and other common functions and activities of Federal agencies approved by the Archivist of the United States. Any deviation from the GRS must be authorized by NARA in accordance with 36 Code of Federal Regulations (CFR) 1228.42(B). Requests for deviations

from either the RCS 10-1 or GRS retention and disposition requirements are to be submitted to the VHA Records Management Office via the Facility requesting the change and the primary. VHA Program Office with authority over the record type that is being requested for change. The financial records that we discussed today fall under the General Records Schedule (GRS).

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, Benefits records are governed by Records Control Schedule (RCS) VB-1, Part II Revised for VBA http://benefits.va.gov/WARMS/docs/admin20/rcs/part2/VB-1PartII.doc and VHA Records are governed by RCS 10-1 www.va.gov/vhapublications/rcs10/rcs10-1.pdf. The following NARA schedules cover some of the record types retained in FEE https://www.archives.gov/records-mgmt/grs

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

The GENERAL RECORDS SCHEDULE 1.1: Financial Management and Reporting Records 4000.1b Temporary: Destroy when 3 years old, but longer retention is authorized if needed for business use. (DAA-GRS-2016-0013-0001)
Official record held in the office of record. Temporary; destroy 6 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) All Other copies. Temporary; destroy when business use ceases (GRS 1.1 item 011) (DAA-GRS-2013-0003-0002)

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.

Electronic media sanitization, when the records are authorized for destruction (or upon system decommission), will be carried out in accordance with VA 6500.1 HB Electronic Media Sanitization. Disposition of Printed Data: Forms and other types of printed output produced by any computer systems and related peripherals will be evaluated by the responsible staff member. for data sensitivity. Printed output containing sensitive data will be stored in locked cabinets or desks, and disposed of properly (when the approved records schedule permits destruction) by shredding or similar VA approved methods in accordance with VA Directive 6371. Program listings and documentation relating to the use of or access to a computer system require special.

handling if the listings or documentation provide information about a system which processes. sensitive data. VA personnel are responsible for retrieving/removing all printed outputs they request from printers.

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.

Central Fee data is sometimes used in testing environment, PII data is protected. For Mainframe applications like Central Fee, CA Top Secret offers security protection for all required Started. Tasks (STC) definitions and STCs that reference sensitive data or affect system integrity. The mainframe does not offer lesser mainframe protection for data as PII in all environments and/or networks as well as all applications

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: There is a risk that the information maintained by FEE could be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached.

Mitigation: To mitigate the risk posed by information retention, FEE only retains the necessary data for historically recording payments to non-VA providers for health care treatment of veterans. FEE controls access to that data so only users with approved business need-to-know functions can access the information. Additionally, when the records are approved for destruction FEE staff will ensure it is carried out in accordance with VA policy.
The GENERAL RECORDS SCHEDULE 1.1: Financial Management and Reporting Records 4000.1b Temporary: Destroy when 3 years old, but longer retention is authorized if needed for business use. (DAA-GRS-2016-0013-0001) Official record held in the office of record.
Temporary; destroy 6 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)
All Other copies.
Temporary; destroy when business use ceases (GRS 1.1 item 011) (DAA-GRS-2013-0003-0002)

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. Central FEE consists of one key component. Each component has been analyzed to determine if any.
elements of that component collect PII. The type of PII collected by Central FEE and the functions that collect it are mapped below.
The type of PII collected by **Central FEE** 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

AITC Z16 Mainframe	Yes	Yes	Name • Social Security Number (SSN) • Mailing Address • Zip Code • Financial Account Information • VA Claim Information	Pay private. physicians, hospitals (inpatient) and pharmacists for products and services dispersed to approved Veterans for non-VA care. Also helps to reimburse Veterans for medical care and travel	VA, IO Datacenter and FEE application staff have implemented required security and privacy controls for Federal information systems and organizations according to NIST SP 800-53 and VA handbook 6500, Risk management Framework for VA Information Systems. Such us encryption of data at rest and data in transit.

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***
Veterans' Health Information Systems Technology Architecture (VistA)	Central Fee receives. vendor/vet payment information from VistA and sends. payment confirmation back	• Name • Social Security Number (SSN) • Date of Birth (DOB) • Mailing Address • Zip Code • Financial Account Information • VA Claim Information	Encrypted electronic. message via mailman service in VISTA
Financial Management System (FMS)	Accounting system of record for funds control, budget. execution, standard general ledger, cost accounting and serves as the primary. repository of VA financial data. Sends payment information. and receives. confirmations.	• Name • Social Security Number (SSN) • Date of Birth (DOB) • Mailing Address • Zip Code • Financial Account Information • VA Claim Information	Secure electronic flat file transmission within the mainframe
Allocation Resource Center (ARC)	Sends cumulative. Fee payment history info for workload measure VERA model	• Name • Social Security Number (SSN) • Date of Birth (DOB) • Mailing Address • Zip Code • Financial Account	Secure electronic flat file transmission via SFTP

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 • VA Claim Information	
Statistical Analysis Software (SAS)	Sends reports and statistical data	• Name • Social Security Number (SSN)	Secure electronic flat file transmission within the mainframe
Beneficiary Identification & Records Locator System (BIRLS)	Receive Data files from BIRLS	• Name • Social Security Number (SSN) • Date of Birth (DOB)	Secure electronic flat file transmission. within the mainframe
Fee Payment Processing System (FPPS)	Sends Payment Adjudication Information	• VA Claim Information • Financial Account Information	Secure electronic flat file transmission via SFTP
Healthcare Claims Processing System (HCPS)	Sends payment. information; and receives confirmations	• Name • Social Security Number (SSN) • Date of Birth (DOB) • Mailing Address • Financial Account Information • VA Claim Information	Secure electronic flat file transmission via SFTP
Decision Support System (DSS)	Name, SSN, Date of Birth (DOB), Mailing Address, Zip Code, Financial Account Information, Medical Records	• Name • Social Security Number (SSN) • Date of Birth (DOB) • Mailing Address • Financial Account Information • VA Claim Information	Secure electronic flat file transmission within the mainframe

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: The privacy risk associate with maintaining PII is that sharing data within the Department of Veterans' Affairs could happen and that the data may be disclosed to individuals who do not require access and heightens the threat of the information being misused.

Mitigation: The principle of need-to-know is strictly adhered to by the staff who support and use Central FEE. Only staff with a clear business purpose are allowed access to the system and the information contained within. Use of secure passwords, PIV Cards, PIN numbers, encryption, and access authorization are all measures that are utilized within the facility.

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***
N/A	N/A	N/A	N/A	N/A

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 privacy risk associated with maintaining PII is that sharing data outside of the Department of Veteran's Affairs could increase the risk that data may be disclosed to individuals who do not require access and heightens the threat of the information being misused.

Mitigation: The principle of need-to-know is strictly adhered to by FEE personnel. Only personnel with a clear business purpose is allowed access to the system and the information contained within the system.

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.

1) The System of record Notice (SORN) Non-VA Fee Basis Records-VA 23VA10NB3. The SORN can be found online at https://department.va.gov/privacy/system-of-records-notices
Version Date: May 1, 2021

2) This Privacy Impact Assessment (PIA) also serves as notice of the system's existence and its PII collection, use, maintenance, and dissemination practices. This PIA is available online for public notification, review, and use, as required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii)

6.1b If notice was not provided, explain why.

Central FEE does not interface with the veterans, it is a processing system. Data that is in the system comes from the system of record Vista Fee.

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

Central FEE does not interface with the veterans, it is a processing system. Data that is in the system comes from the system of record Vista Fee.

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.

VHA Handbook 1605.1 Appendix D 'Privacy and Release Information', section 5 lists the rights. of the Veterans to request VHA to restrict the uses and/or disclosures of the individual's individually identifiable health information to carry out treatment, payment, or health care. operations. The Veterans have the right to refuse to disclose their SSN to VHA. The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose. to VHA an SSN (see 38 CFR 1.575(a)

Central FEE does not interface with the veterans it is a processing system. Data that is in the system comes from the system of record Vista Fee.

6.3 Do individuals have the right to consent to 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.

VHA Handbook 1605.1 Appendix D 'Privacy and Release Information', section 5 lists the rights. of the Veterans to request VHA to restrict the uses and/or disclosures of the individual's individually identifiable health information to carry out treatment, payment, or health care. operations. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that. maintains the record.

Central FEE does not interface with the veterans it is a processing system. Data that is in the system comes from the system of record Vista Fee.

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

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

<u>Principle of Transparency:</u> This is referring to sufficient notice provided to the individual.

<u>Principle of Use Limitation:</u> The information used only for the purpose for which notice was provided either directly to the individual or through a public notice. The procedures in place must ensure that information is used only for the purpose articulated in the notice.

This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.
Follow the format below:

Privacy Risk: There is a risk that members of the public may not know that the FEE system exists within the Department of Veterans Affairs

Mitigation: The VA mitigates this risk by providing the public with two forms of notice that the system exists, as discussed in detail in question 6.1, including the Privacy Act statement and a System of Record Notice

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.***

Central FEE does not interface with the veterans; it is processing system. Data that is the system comes from the system comes from the of record Vista FEE

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

Individuals wishing to obtain more information about access, redress and record correction of FEE system should contact the Department of Veteran's Affairs regional as directed in the System of Record
Notice (SORN) Non-VA Fee Basis Records-VA 23VA10NB3 The SORN can be found online at *https://department.va.gov/privacy/system-of-records-notices/*

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?

Central FEE does not interface with the veterans; it is processing system. Data that is the system comes from the system comes from the of record Vista FEE.

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

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

Individuals wishing to obtain more information about access, redress and record correction of FEE system should contact the Department of Veteran's Affairs regional as directed in the System of Record Notice (SORN) Non-VA Fee Basis Records-VA 23VA10NB3 The SORN can be found online at https://department.va.gov/privacy/system-of-records-notices/

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 seeking information regarding access, redress, record correction and contesting of records in this system may write or call the Director of National Data Systems (10P2C), Austin Automation Center, 1615 Woodward Street, Austin, Texas 78772, or call the VA Austin Automation Center Help Desk and ask to speak with the VHA Director of National Data Systems at (512) 326–678.

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 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.

Formal redress procedures are published in SORN 23VA16. Individuals seeking information regarding access to and contesting of VA fee basis records may write, call or visit the last VA facility where medical care was authorized or provided. Individuals seeking information regarding access to health records and/ or contesting health l records may write, call or visit the VA facility where medical care was last authorized or provided. Individuals seeking information regarding access to claims and/or billing records will write to the VHA Chief Business Office Purchased Care, Privacy Office, PO BOX 469060, Denver, CO.

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 can prevent information about them obtained for one purpose from being used for other purposes without their knowledge.
This question is related to privacy control IP-3, Redress.

Follow the format below:

Privacy Risk: There is a risk that individuals may seek to access, correct or redress records about them held by the VA Office and become frustrated with the results of their attempt.

Mitigation: By publishing this PIA, and the applicable SORN described in section 6.1, the VA makes the public aware of the FEE system. Furthermore, this document and the SORN provide the point of contact for members of the public who have questions or concerns about their files.

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?
Users gain access to Central Fee using IAM request for access sent through their Managers and the IAM admin.

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?

There are no users outside our program team, Mainframe system admins and similar roles who have access to the Central Fee application.

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.

Mainframe system Admin, Operations Manager and Programmers for the Central Fee application.

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

Yes

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

Contractor's assist maintaining the system and help with operational duties under supervision of FTE leads.

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

Yes.

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

Yes

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.

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

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

Personnel that will be accessing information systems or VA sensitive information must read and acknowledge their receipt and acceptance of the VA National 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 which all personnel must complete via the VA's Talent Management System (TMS). After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the privacy and security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Completed
2. *The System Security Plan Status Date:* 10-17-2024
3. *The Authorization Status:* ATO
4. *The Authorization Date:* 11-04-2024
5. *The Authorization Termination Date:* 11-04-2027
6. *The Risk Review Completion Date:* 09-*19-2024*
7. *The FIPS 199 classification of the system: 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.***

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 is not applicable to FEE. FEE is not in the cloud environment and does not use cloud technology.

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.*

This is not applicable to FEE. FEE is not in the cloud environment and does not use cloud technology.

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.

This is not applicable to FEE. FEE is not in the cloud environment and does not use cloud technology.

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.

This is not applicable to FEE. FEE does not use cloud technology.

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).

This is not applicable to FEE.

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.

AKEEL OMARI Digitally signed by AKEEL OMARI
Date: 2024.12.10 16:26:41 -05'00'

Privacy Officer, Akeel Omari

ASHTON BOTTS Digitally signed by ASHTON BOTTS
Date: 2024.12.11 11:32:14 -07'00'

Information System Security Officer, Ashton Botts

TONY SINES Digitally signed by TONY SINES
Date: 2024.12.13 14:55:34 -06'00'

Information System Owner, Tony Sines

APPENDIX A-6.1

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

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)