Privacy Impact Assessment for the VA IT System called:

Fee Payment and Processing System (FPPS) Assessing

Veterans Health Administration

Office of Integrated Veterans Care

Date PIA submitted for review:

July 5, 2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Michael Hartmann	Michael.Hartmann@va.gov	303-780-4753
Information System Security Officer (ISSO)	Ashton Botts	Ashton.Botts@va.gov	303-398-7155
Information System Owner	Dena Liston	Dena.Liston@va.gov	304-886-7367

Abstract

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

The Fee Payment and Processing System (FPPS) provides claim data to all VA sites allowing them to process claims electronically whereas it would be a paper-based process. It further centrally receives electronic health care data from a contracted clearing house Health Insurance Health Insurance Portability and Accountability Act (HIPAA) Compliant 837, forwards claim data to 150+ VA Fee Processing Sites, collect payment record data from those sites to create electronic payment remittances (HIPAA Compliant 835). Remittances are then forwarded to the contracted clearinghouse. The system supports the entire VA's ability to pay health care claims electronically.

Overview

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

1 General Description

A. The IT system name and the name of the program office that owns the IT system.

Fee Payment Processing System (FPPS) Assessing, Office of Integrated Veteran Care

B. The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.

The system supports the population of over 9 million Veterans; however, contains information on health care claims for approximately 4 million Veterans. It centrally receives electronic health care data from a contracted clearing house (HIPAA Compliant 837s), forwards claim data to 150+ VA Fee Processing Sites, collect payment record data from those sites to create electronic payment remittances (HIPAA Compliant 835). Remittances are then forwarded to the contracted clearinghouse. The system supports the entire VA's ability to pay health care claims electronically.

C. Indicate the ownership or control of the IT system or project.

VA Owned and VA Operated

2. Information Collection and Sharing

D. The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.

The system supports the population of over 9 million Veterans; however, contains information on health care claims for approximately 4 million Veterans.

E. A general description of the information in the IT system and the purpose for collecting this information.

The Fee Payment and Processing System (FPPS) provides claim data to all VA sites allowing them to process claims electronically whereas it would be a paper-based process. The system supports the population of over 9 million veterans; however, contains information on health care claims for approximately 4 million Veterans.

F. Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.

FPPS centrally receives electronic health care data from a contracted clearing house (HIPAA Compliant 837s), forwards claim data to 150+ VA Fee Processing Sites, collect payment record data from those sites to create electronic payment remittances (HIPAA Compliant 835). Remittances are then forwarded to the contracted clearinghouse. The system supports the entire VA's ability to pay health care claims electronically.

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

This system is operated in only one site.

3. Legal Authority and SORN

H. A citation of the legal authority to operate the IT system.

23VA10NB3, Non-VA Care (Fee) Records - VA (7/30/2015)
24VA10A7, Patient Medical Records - VA (10/2/2020)
43VA008, Veterans, Dependents of Veterans, and VA Beneficiary Survey Records - VA (1/25/2021)
54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files - VA (3/3/2015)
58VA21/22/28, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records - VA (11/8/2021)
79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records - VA (12/23/2020)
88VA244, Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line System (CAR/CAROLS, combined system referred to as CAO) (8/13/2018)
147VA10, Enrollment and Eligibility Records - VA
(8/17/2021)

I. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?

No, it will not require amendment.

D. System Changes

J. Whether the completion of this PIA will result in circumstances that require changes to business processes

No, will not require changes to business processes.

K. Whether the completion of this PIA could potentially result in technology changes

No, will not result in technology changes.

Section 1. Characterization of the Information

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

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

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

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

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

- ☒ Name
- ☒ 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*
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☐ Medications
- ☐ Medical Records
- ☐ Race/Ethnicity
- ☒ Tax Identification Number
- ☐ Medical Record Number
- ☐ Gender
- ☐ Integrated Control Number (ICN)
- ☐ Military History/Service Connection
- ☐ Next of Kin
- ☒ Other Data Elements (list below)

Health Insurance Numbers, Current Procedural Terminology (CPT) and International Code Designator (ICD) Coded Billing Information, Billed Amounts, Other Health Insurance Information, Other Health Insurance Paid Amounts, Provider Name, Provider Phone Number, Provider Billing Address, Provider Physical Address, Provider Remit to Address.

PII Mapping of Components (Servers/Database)

FPPS consists of 1 database. It has been analyzed to determine if any elements of that component collect PII. The type of PII collected by FPPS 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 the server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

Internal Database Connections

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
Claims Database	Yes	Yes	Name, Social Security Number, Date of Birth, Address, Zip Code, Health Insurance Beneficiary Numbers/Account Numbers, Current Medications, Provider's TIN and Address information.	Required Data for proper claim adjudication	Encrypted; VA Network via TCP port 1521

1.2 What are 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?

The sources of information are ultimately the Beneficiary and providers. The system supports HIPAA mandated claims processing which includes electronic processing of health care claims. The system centrally receives electronic health care data from a contracted clearing house, who received

it from the provider, who received it from the Beneficiary (HIPAA Compliant 837s), forwards claim data to 150+VA Fee Processing Sites, collect payment record data from those sites to create electronic payment remittances (HIPAA Compliant 835). Remittances are then forwarded to the contracted clearinghouse. The system supports the entire VA's ability to pay health care claims electronically.

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.

The sources of information are ultimately the Beneficiary and providers. The system supports HIPAA mandated claims processing which includes electronic processing of health care claims. The system centrally receives electronic health care data from a contracted clearing house, who received it from the provider, who received it from the Beneficiary (HIPAA Compliant 837s), forwards claim data to 150+VA Fee Processing Sites, collect payment record data from those sites to create electronic payment remittances (HIPAA Compliant 835). Remittances are then forwarded to the contracted clearinghouse. The system supports the entire VA's ability to pay health care claims electronically.

1.2c If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

Not Applicable, system does not create information.

1.3 How is the information collected?

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 system centrally receives electronic health care data from a contracted clearing house, who received it from the provider, who received it from the Beneficiary (HIPAA Compliant 837s), forwards claim data to 150+ VA Fee Processing Sites, collect payment record data from those sites to create electronic payment remittances (HIPAA Compliant 835). Remittances are then forwarded to the contracted clearinghouse. The system supports the entire VA's ability to pay health care claims electronically.

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

Not applicable, information is not collected on a form.

1.4 How will the information be checked for accuracy? 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 a number of commercially acquired integrity checks that automatically reject claims that do not meet HIPAA mandated requirements. If a claim is not properly developed the system rejects the claim and the clearinghouse must go back to the provider to correct the information prior to acceptance by VA.

1.4b If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

The system has a number of commercially acquired integrity checks that automatically reject claims that do not meet HIPAA mandated requirements. If a claim is not properly developed the system rejects the claim and the clearinghouse must go back to the provider to correct the information prior to acceptance by VA.

1.5 What specific legal authorities, arrangements, and agreements defined the collection of information?

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

23VA10NB3, Non-VA Care (Fee) Records - VA (7/30/2015)
24VA10A7, Patient Medical Records - VA (10/2/2020)
43VA008, Veterans, Dependents of Veterans, and VA Beneficiary Survey Records - VA (1/25/2021)
54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files - VA (3/3/2015)
58VA21/22/28, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records - VA (11/8/2021)
79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records - VA (12/23/2020)
88VA244, Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line System (CAR/CAROLS, combined system referred to as CAO) (8/13/2018)
147VA10, Enrollment and Eligibility Records - VA (8/17/2021)
38 U.S. Code. § 501 - VETERANS' BENEFITS Rules and regulations

38 U.S. Code § 1703 - Contracts for hospital care and medical services in non-Department facilities
38 U.S. Code § 1720G - Assistance and support services for caregivers
38 U.S. Code § 1781 - Medical care for survivors and dependents of certain veterans
38 U.S. Code § 1787 - Health care of family members of veterans stationed at Camp Lejeune, North Carolina
38 U.S. Code § 1802 - CHILDREN OF VIETNAM VETERANS BORN WITH SPINA BIFIDA- Spina bifida conditions covered 1803
38 US. Code Sec. § 1803 - CHILDREN OF VIETNAM VETERANS BORN WITH SPINA BIFIDA -Health care 1812
38 U.S. Code 1812 Children of Women Vietnam Veterans Born with Certain Birth Defects - Covered Birth Defects1813
38 U.S. Code 1813 Children of Women Vietnam Veterans Born with Certain Birth Defects-Health Care
38 U.S. Code § 1821 - Benefits for children of certain Korea service veterans born with spina bifida
Public Law 103–446, section 107 Veterans Education and Benefits Expansion Act of 2001"- Sec. 107. Expansion of work-study opportunities
38 U.S. Code § 1724 - Hospital care, medical services, and nursing home care abroad
38 U.S. Code § 1725 - Reimbursement for emergency treatment
38 U.S. Code § 1728 - Reimbursement of certain medical expenses
38 U.S. Code § 1703 - Contracts for hospital care and medical services in non-Department facilities
38 U.S. Code § 1720 - Transfers for nursing home care; adult day health care
Public Law 111–163 section 101. CAREGIVERS AND VETERANS OMNIBUS HEALTH SERVICES ACT OF 2010- Sec. 101. Assistance and support services for caregivers
5 U.S.C. § 301 - Departmental regulations
26 U.S. Code § 61 - Gross income defined (a) (12) Income from discharge of indebtedness
38 U.S.C. 31 Foreign Medical Program
38 U.S. Code § 109 - Benefits for discharged members of allied forces
38 U.S. Code § 111 - Payments or allowances for beneficiary travel
38 U.S. Code. § 501 - VETERANS' BENEFITS Rules and regulations
38 U.S. Code § 1151 - Benefits for persons disabled by treatment or vocational rehabilitation
38 U.S. Code § 1703 - Contracts for hospital care and medical services in non-Department facilities
38 U.S. Code § 1705 - Management of health care: patient enrollment system
38 U.S. Code § 1710 - Eligibility for hospital, nursing home, and domiciliary care
38 U.S. Code § 1712 - Dental care; drugs and medicines for certain disabled veterans; vaccines
38 U.S. Code § 1717 - Home health services; invalid lifts and other devices
38 U.S. Code § 1720 - Transfers for nursing home care; adult day health care
38 U.S.C. § 1721 - POWER TO MAKE RULES AND REGULATIONS
38 U.S. Code § 1724 - Hospital care, medical services, and nursing home care abroad
38 U.S. Code § 1725 - Reimbursement for emergency treatment
38 U.S.C. § 1727 - PERSONS ELIGIBLE UNDER PRIOR LAW
38 U.S. Code § 1728 - Reimbursement of certain medical expenses
38 U.S.C. 1741-1743 Per Diem Grant- State Home
38 U.S. Code § 1781 - Medical care for survivors and dependents of certain veterans
38 U.S. Code § 1786 - Care for newborn children of women veterans receiving maternity care
38 U.S. Code § 1787 - Health care of family members of veterans stationed at Camp Lejeune, North Carolina
38 U.S. Code § 3102 - Basic entitlement-A person shall be entitled to a rehabilitation program
38 U.S. Code § 5701 - Confidential nature of claims

38 U.S. Code § 5724 - Provision of credit protection and other services
38 U.S. Code § 5727 – Definitions38 U.S. Code § 7105 - Filing of notice of disagreement and appeal
38 U.S. Code § 7332 - Confidentiality of certain medical records
38 U.S.C. 8131-8137. Construction Grant- State Home
44 USC - PUBLIC PRINTING AND DOCUMENTS
Veterans Access, Choice, and Accountability Act of 2014
38 CFR 2.6 - Secretary's delegations of authority to certain officials (38 U.S.C. 512).
TITLE 45 CFR—Public Welfare Subtitle A—DEPARTMENT OF HEALTH AND HUMAN SERVICES-PART 160—GENERAL ADMINISTRATIVE REQUIREMENTS
45 CFR Part 164 - SECURITY AND PRIVACY

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: Explain how the collection ties with the purpose of the underlying mission of the organization and its enabling authority.

Principle of Minimization: Is the information directly relevant and necessary to accomplish the specific purposes of the program?

Principle of Individual Participation: Does the program, to the extent possible and practical, collect information directly from the individual?

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

Follow the format below when entering your risk assessment:

Privacy Risk: Inaccurate information is received from VA systems, which may result in incorrect fee payment of claims.

Mitigation: The information contained within the system in not originated by VA but is used by VA for purpose of claims payment to providers and Beneficiaries. The system contains coded data that is industry standard and complies with the Health Insurance Portability and Accountability Act (HIPAA) requirements. The system is scanned by National Security Operations Center (NSOC) for vulnerabilities and those vulnerabilities addressed to the extent possible. The system is also only accessible by authorized staff on the VA network. The system is unreachable without approved remote access protocols from the outside world. All incoming and outgoing data to and from the system is sent through Federal Information Processing

Standard (FIPS) 140-2 approved encryption. The only data collected in the system is that required by law to accurately pay a health care claim.

Section 2. Uses of the Information

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

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

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

The system centrally receives electronic health care data from a contracted clearing house, who received it from the provider, who received it from the Beneficiary (HIPAA Compliant 837s), the system then forwards claim data to 150+ VA Fee Processing Sites, collect payment record data from those sites to create electronic payment remittances (HIPAA Compliant 835). Remittances are then forwarded to the contracted clearinghouse. The system supports the entire VA's ability to pay health care claims electronically.
Name: to properly adjudicate and pay claims
Social Security Number: to properly adjudicate and pay claims
Date of Birth: to properly adjudicate and pay claims
Mother's Maiden Name: to properly adjudicate and pay claims
Mailing Address, Zip Code: to properly adjudicate and pay claims
Phone Number(s): to properly adjudicate and pay claims
Financial Account Information, Health Insurance Beneficiary Numbers Account numbers: to properly adjudicate and pay claims
Previous Medical Records: to properly adjudicate and pay claims
Provider's TIN: to properly adjudicate and pay claims
Provider Address: to properly adjudicate and pay claims
Provider telephone number: to properly adjudicate and pay claims
Provider National Provider Identification Number (NPI): to properly adjudicate and pay claims

2.2 What types of tools are 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.

Sybase maps are used to sort through the data and ensure all data meets the mandatory HIPAA compliance. These maps along with the associated Sybase software reject claims that do not meet

the HIPAA requirements. Claims are individual records, and they are stored on a claim level and not by an individual. Sybase is the company, and the maps are the flat files used to determine if a claim has the right characteristics to be accepted by the system.

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.

FPPS does not create or make available new or any previous unutilized information.

2.3 How is the information in the system 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 in transit is protected by means of industry standard encryption protocols (e.g., HTTPS, VPN, etc.). Data at rest is FIPS 140-3 compliant and fully encrypted at aggregate-level. All data is encrypted while at rest and during transmission. Appropriate security controls are in place to guard against unauthorized access to the data.

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

The system is only accessed through VA Intranet by means of GFE laptops, Citrix Access Gateway (CAG), VA workstations. All three means of access are subject to standard VA encryption. Appropriate security controls are in place to guard against unauthorized access to the data.

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

The Technical Safeguards used by FPPS to protect PII/{HI data are, two factor authentication (2FA), authorized access through the VA intranet only, the 15 minute timeout/session lock. For those with elevated privileges approval is required before an Electronic Permissions Access System (ePAS) can be submitted for approval.

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. ***<u>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.</u>***

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

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

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

2.4a How is access to the PII determined?

All access requests for FPPS are submitted and processed internally through the FPPS system. FPPS also uses Active Directory (AD)/ Windows NT passthrough authentication. A request can only be approved if the submitter is a "Tier" or "Role" above the individual gaining access. No user can request access for themselves.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented?
Yes

2.4c Does access require manager approval?
Yes

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

2.4e Who is responsible for assuring safeguards for the PII?

The VA Administrators within the Health Administrative Center Denver.

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

All data is retained by the system for the purpose of congressional inquiries, claims appeals, and researching Veteran, Beneficiary, and provider inquiries. The following PII/PHI is collected: Name, Social Security Number (SSN), Date of Birth (DOB), Address, Zip Code, Phone Number, Fax Number, Email Address, Race/Ethnicity, Health Insurance Numbers, CPT and International Code Designator (ICD) Coded Billing Information, Current Medications, Billed Amounts and Other Health Insurance 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? This question is related to privacy control DM-2, Data Retention and Disposal.*

Retention period is 6 years after all individuals in the record become ineligible for program benefits. Financial management and reporting administrative records are destroy when 3 years old, but longer retention is authorized if needed for business use. Destroyed 7 years after final action, but longer retention is authorized if required for business needs.

3.3 Has the retention schedule been 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. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner. Please work with the system Privacy Officer and 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.

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

Yes, , follows VA policy regarding retention of records. For Patient medical records are retained for a total of 75 years after the last episode of care. As directed by the Department Veterans Affairs, Veterans Health Administration Record Control Schedule (RCS) 10-1
VHA RCS 10-1: https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf

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 data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with VA Directive

6500 VA Cybersecurity Program (February 24, 2021) and VA Handbook 6500.1 Electronic Media Sanitization. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destruction. https://www.va.gov/vapubs/search_action.cfm?dType=1

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.

Yes, the system uses de-identified data whenever possible.

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 ISSO 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: Does the project retain only the information necessary for its purpose? Is the PII retained only for as long as necessary and relevant to fulfill the specified purposes?

Principle of Data Quality and Integrity: Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?
This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:

Privacy Risk: The system is only accessible to VA employees who have been determined to have a need for access. The users of the system are role based and only have access to the information allowed to do their jobs. The only privacy risk is potential abuse by authorized users, which is mitigated through access control, system logs, and supervisory reviews. Hackers are a risk to all systems but as discussed there are multiple layers of protection. Loss of backup tapes poses almost no risk as they are FIPS-140-2 certified encrypted and the keys are not stored with the tapes.

Mitigation: Access controls are in place at the wide area level through the NSOC gateways and firewalls. Access is further controlled by the use of Active Directory (AD) thus making only VA approved users able to be added as a user of the system. Further role-based security allows users to access sonly that data needed to accomplish their mission. Hackers are a risk to all systems but as discussed there are multiple layers of protection. Loss of backup tapes poses almost no risk as they FIPS-140-2 certified encrypted, and the keys are not stored with the tapes. PA Mitigation Risk- Talent Management System (TMS) 10203, Privacy and HIPAA training-required annual training, Business Associate Agreements-For all contracts which may have exposure or access to VA Sensitive Personal Information (SPI)/Personal Health Information (PHI)/Personally Identifiable Information (PII) information, Functional Categories are assigned by the supervisor and verified annually. ISO Mitigation Risk-TMS 10176, VA Privacy and Information Security Awareness and Rules of Behavior-required annual training which includes National Rules of Behavior.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Office of Veteran Integrated Care MOVEit	Pass through vehicle that transfers transactions for claims processing	Name, Social Security Number (SSN), Date of Birth (DOB), Address, Phone Numbers, Email Addresses, Health Insurance Beneficiary Numbers, Account Numbers, Current Medications, Previous Medical Records	Via Secure File Transfer Protocol (SFTP), System in internal to the VA. Only approved employees and contractors have access to the system.
Veterans Health Administration EDI Gateway	To process claims payments for providers and Beneficiaries	Name, Social Security Number, Date of Birth, Mailing Address, Zip Code, Health Insurance Beneficiary Numbers/Account Numbers, Current Medications, Provider's TIN and Address information.	Electronically Via Secure File Transfer Protocol (SFTP), System in internal to the VA. Only approved employees and contractors have access to the system.
Veterans Health Administration Claims Database	Veteran healthcare claim data that includes all PII and all related PHI values which support claim adjudication.	Name, Social Security Number, Date of Birth, Address, Zip Code, Health Insurance Beneficiary Numbers/Account Numbers, Current Medications, Provider's TIN and Address information.	Via Secure File Transfer Protocol (SFTP), System in internal to the VA. Only approved employees and contractors have access to the system.
Veterans Health Administration Electronic Web Viewer (EWV)	Veteran healthcare claim data that includes all PII and all related PHI values which support claim adjudication.	Name, Social Security Number, Date of Birth, Mailing Address, Zip Code, Health Insurance Beneficiary Numbers/Account Numbers, Current Medications, Provider's TIN and Address information.	Via Secure File Transfer Protocol (SFTP), System in internal to the VA. Only approved employees and contractors have access to the system.

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: Risk that the data could be shared with an inappropriate VA employee or others of which could results in a breach of privacy and disclosure of PII and/or PHI to unintended recipients.

Mitigation: Safeguards implemented to ensure data is not sent to the wrong VA organization are employee security and privacy training and awareness are required reporting of suspicious activity. Use of secure passwords, access for need-to-know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized within the facilities. Access to sensitive information and the systems where the information is stored is controlled by the VA using a "least privilege/need to know" policy. Access must be requested and only the access required by VA persons or processes acting on behalf of VA persons is to be requested or granted.
Community Care: Privacy Act (PA) Risk Violation Reporting - Internal Control: Breach Reporting:

1. Business Associate or Supervisor notifies the PA office
2. Conduct preliminary investigation, collect who violated (VA Employee, Non-VA employee, Business Associate), mode of violation, how many persons affected, loss of control, and what information was compromised.
3. Report Breach through Remedy- Veterans Affairs Privacy Incident Reporting system
4. Log Breach on Spreadsheet
5. Create Incident folder
6. Conduct Mitigation/Corrective Action Investigation - Report from Supervisor on recovery of items, Time loss of control, training, new policy/protocol in place, employee sanctions, (this will include providing a 10203 training certificate, Functional Category form (signed), and Rules of Behavior).
7. Enter Mitigation/Corrective Action into Remedy
8. If incident requires Credit Monitoring Letters, you will receive the credit monitoring case number from PSETS
9. Create the Credit Monitoring Letters
10. Delegated authority signs letters
11. Receive signed letters
12. Scan Letters into file (Incident Reporting)
13. Redact Letters of Names and addresses
14. Upload redacted letters into Remedy
15. Request Remedy case/ticket closure
16. Mail Letters via FEDEX.

17. Create a copy of the Credit Monitoring Information In a file under (Credit Monitoring)

Section 5. External Sharing/Receiving and Disclosure

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

5.1 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

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

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

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

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

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

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***

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.

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: Not Applicable, FPPS does not share information.

Mitigation: Not Applicable, FPPS does not share information.

Section 6. Notice

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

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an Appendix-A 6.1 on the last page of the document. Also provide notice given to individuals by the source system (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

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 This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

FPPS does not collect information from the individual. VHA Notice of Privacy Practices

23VA10NB3, Non-VA Care (Fee) Records - VA (7/30/2015)
24VA10A7, Patient Medical Records - VA (10/2/2020)

43VA008, Veterans, Dependents of Veterans, and VA Beneficiary Survey Records - VA (1/25/2021)
54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files - VA (3/3/2015)
58VA21/22/28, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records - VA (11/8/2021)
79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records - VA (12/23/2020)
88VA244, Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line System (CAR/CAROLS, combined system referred to as CAO) (8/13/2018)
147VA10, Enrollment and Eligibility Records - VA (8/17/2021)
https://department.va.gov/privacy/system-of-records-notices/

6.1b If notice was not provided, explain why. If it was provided, attach a copy of the current notice.

FPPS does not collect information from the individual.

6.1c Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

FPPS does not collect information from the individual. VHA Notice of Privacy Practices

23VA10NB3, Non-VA Care (Fee) Records - VA (7/30/2015)
24VA10A7, Patient Medical Records - VA (10/2/2020)
43VA008, Veterans, Dependents of Veterans, and VA Beneficiary Survey Records - VA (1/25/2021)
54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files - VA (3/3/2015)
58VA21/22/28, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records - VA (11/8/2021)
79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records - VA (12/23/2020)
88VA244, Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line System (CAR/CAROLS, combined system referred to as CAO) (8/13/2018)
147VA10, Enrollment and Eligibility Records - VA (8/17/2021)
https://department.va.gov/privacy/system-of-records-notices/

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.

FPPS does not collect information from the individual. VHA Notice of Privacy Practices

23VA10NB3, Non-VA Care (Fee) Records - VA (7/30/2015)
24VA10A7, Patient Medical Records - VA (10/2/2020)
43VA008, Veterans, Dependents of Veterans, and VA Beneficiary Survey Records - VA (1/25/2021)
54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files - VA (3/3/2015)
58VA21/22/28, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records - VA (11/8/2021)
79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records - VA (12/23/2020)
88VA244, Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line System (CAR/CAROLS, combined system referred to as CAO) (8/13/2018)
147VA10, Enrollment and Eligibility Records - VA (8/17/2021)
https://department.va.gov/privacy/system-of-records-notices/

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.

FPPS does not collect information from the individual. VHA Notice of Privacy Practices

23VA10NB3, Non-VA Care (Fee) Records - VA (7/30/2015)
24VA10A7, Patient Medical Records - VA (10/2/2020)
43VA008, Veterans, Dependents of Veterans, and VA Beneficiary Survey Records - VA (1/25/2021)
54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files - VA (3/3/2015)
58VA21/22/28, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records - VA (11/8/2021)
79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records - VA (12/23/2020)
88VA244, Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line System

(CAR/CAROLS, combined system referred to as CAO) (8/13/2018)
147VA10, Enrollment and Eligibility Records - VA (8/17/2021)
https://department.va.gov/privacy/system-of-records-notices/

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 System ISSO 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: Has sufficient notice been provided to the individual?

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

Privacy Risk: There is a risk that the veterans and other members of the public will not know the system is part of the transfer capabilities to collect and/or disseminate PII, and/or PHI about them.

Mitigation: This risk is mitigated by the common practice of providing the Notice of Privacy Practice (NOPP) when Veterans are enrolled for healthcare. Employees and contractors are required to review, sign, and abide by the National Rules of Behavior on a yearly basis as required by VA Handbook 6500 as well as complete the annual mandatory Information Security and Privacy Awareness training. Additional mitigation is provided by making the System of Record Notices (SOR) and Privacy Impact Assessment (PIA) available to review online, as discussed in question 6.1 and the Overview section of this PIA.

Section 7. Access, Redress, and Correction

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

7.1 What are the procedures that allow individuals to gain access to their information?

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 http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.

Records Notices (which are published in the Federal Register) 23VA10NB3 and 54VA10NB3 the location where a person may request records about themselves. First party would be a Privacy Act Request, 3rd party requests can only be processed with a signed authorization to disclose using a VHA-10-5345-REQUEST FOR AND AUTHORIZATION TO RELEASE MEDICAL RECORDS OR HEALTH INFORMATION, or a court document signed by a judge. All other requests would fall under the FOIA regulation as outlined in the U.S. Department of Justice Guide to the Freedom of Information Act. VA Privacy Regulations: VA Handbook 6300.4(Procedures for Processing Requests for Records Subject to the Privacy Act; VHA Handbook 1605.1(Privacy and Release of Information). VA FOIA Regulation: VA Handbook 6300.3 Procedures for Implementing the Freedom of Information Act. Point of Service at the VAMC provides rights, a link to the VA Notice of Privacy Practices is available at Appendix A.

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).

FPPS does not collect information from the individual. VHA Notice of Privacy Practices

23VA10NB3, Non-VA Care (Fee) Records - VA (7/30/2015)
24VA10A7, Patient Medical Records - VA (10/2/2020)
43VA008, Veterans, Dependents of Veterans, and VA Beneficiary Survey Records - VA (1/25/2021)
54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files - VA (3/3/2015)
58VA21/22/28, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records - VA (11/8/2021)
79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records - VA (12/23/2020)
88VA244, Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line System (CAR/CAROLS, combined system referred to as CAO) (8/13/2018)
147VA10, Enrollment and Eligibility Records - VA (8/17/2021)
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.

FPPS does not collect information from the individual. VHA Notice of Privacy Practices

23VA10NB3, Non-VA Care (Fee) Records - VA (7/30/2015)
24VA10A7, Patient Medical Records - VA (10/2/2020)
43VA008, Veterans, Dependents of Veterans, and VA Beneficiary Survey Records - VA (1/25/2021)
54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files - VA (3/3/2015)
58VA21/22/28, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records - VA (11/8/2021)
79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records - VA (12/23/2020)
88VA244, Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line System (CAR/CAROLS, combined system referred to as CAO) (8/13/2018)
147VA10, Enrollment and Eligibility Records - VA (8/17/2021)
https://department.va.gov/privacy/system-of-records-notices/

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.

FPPS does not collect information from the individual. VHA Notice of Privacy Practices
23VA10NB3, Non-VA Care (Fee) Records - VA (7/30/2015)
24VA10A7, Patient Medical Records - VA (10/2/2020)
43VA008, Veterans, Dependents of Veterans, and VA Beneficiary Survey Records - VA (1/25/2021)
54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files - VA (3/3/2015)
58VA21/22/28, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records - VA (11/8/2021)
79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records - VA (12/23/2020)
88VA244, Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line System (CAR/CAROLS, combined system referred to as CAO) (8/13/2018)
147VA10, Enrollment and Eligibility Records - VA (8/17/2021)

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.

See answer from 7.1. above. VHA Notice of Privacy Practices

23VA10NB3, Non-VA Care (Fee) Records - VA (7/30/2015)
24VA10A7, Patient Medical Records - VA (10/2/2020)
43VA008, Veterans, Dependents of Veterans, and VA Beneficiary Survey Records - VA (1/25/2021)
54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files - VA (3/3/2015)
58VA21/22/28, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records - VA (11/8/2021)
79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records - VA (12/23/2020)
88VA244, Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line System (CAR/CAROLS, combined system referred to as CAO) (8/13/2018)
147VA10, Enrollment and Eligibility Records - VA (8/17/2021)

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

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.

Individuals have a right to contact the VHA call center to gain access to their information. Disclosure of Social Security numbers of those for whom benefits are claimed is requested under the authority of 38 USC and is voluntary. Social Security numbers will be used in the administration of Veterans' benefits and 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 38 USC and the Privacy Act of 1974 (5 USC 552a) or where required by other statutes.

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 System ISSO to complete all Privacy Risk questions inside the document this section).*

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

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

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

Follow the format below:

Privacy Risk:
There is a risk that the individuals may not know how to obtain access to their records or how to request corrections to their records.

Mitigation:
As stated in section 7.3, the Notice of Privacy Practice (NOPP), which every patient signs prior to receiving treatment, discusses the process for requesting an amendment to one's records. Beneficiaries are reminded of this information when obtaining a copy of the NOPP. The VA Release of Information (ROI) office is available to assist individuals with obtaining access to their medical records and other records containing personal information.

Section 8. Technical Access and Security

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

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

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 are restricted by role-based assignments access to only that data needed to process the claim. Hacking attempts are thwarted through a multifaceted approach of NSOC manned firewalls and gateways, AD account requirements, role-based assignments and login credentials. The system is scanned by NSOC for vulnerabilities and those vulnerabilities addressed to the extent possible. The system is also only accessible by authorized staff on the VA network. The system is unreachable without approved remote access protocols from the outside world. All incoming and outgoing data to and from the system is sent through FIPS 140-2 approved encryption. The only data collected by the system is that required by law to accurately pay a health care claim.

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 do not have access to the FPPS 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.

Administrator/Privileged Accounts – issues to accomplish administrative tasks. These accounts are separate from the SUA and are Non-Mailbox Enabled Accounts (NMEA). Only cleared production operations individuals have access to data as part of their normal job function. Guest/anonymous or temporary accounts are not permitted. There are no outside agencies from the VA having assess to the system.

8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII. This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

Yes, VA is highly dependent on contract augmentation of its workforce. However, contractors must go through background checks, sign the rules of behavior and have the same restrictions as VA staff.

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

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

All Community Care:(IVC) employees are required to take Annual 10203 (Privacy and HIPAA Focused Training). Departments that provide direct contact with the customers are provided additional training based on the system of records notice for this system. Also, all employees receive New Employee Orientation which includes Privacy, HIPAA and Records Management Training. Education, and Awareness- VA Privacy and Information Security Awareness and Rules of Behavior (10176), Policy: VA Directive 6500 requires mandatory periodic training in computer security awareness and accepted computer security practices for all VA employees, contractors, and all other users of VA sensitive information and VA information systems. All members of the workforce are required to complete computer security training annually and must complete computer security awareness training before they can be authorized to access any VA computer system. Each site identifies personnel with significant information system security roles and responsibilities (i.e., management, system managers, system administrators, contracting staff, HR staff), documents those roles and responsibilities, and provides appropriate additional information system security training. Security training records will be monitored and maintained. Procedure: Orientation training will be conducted for all new employees in accordance with the New Employee Orientation program. For those individuals who cannot immediately attend new employee orientation, the service will provide basic security awareness training.

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

Yes

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 11/21/2022
3. *The Authorization Status:* Authorization to Operate (ATO)
4. *The Authorization Date:* 01/20/2023
5. *The Authorization Termination Date:* 07/19/2023
6. *The Risk Review Completion Date:* 12/28/2022
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.***

FPPS ATO awarded on 01/20/2023and expiring 07/19/2023.

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.

No, this system is not utilizing the Cloud.

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.*

This system is not in the Cloud.

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 system is not in the Cloud.

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 system is not in the Cloud.

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 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**

ID	Privacy Controls
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

MICHAEL HARTMANN

Digitally signed by MICHAEL HARTMANN
Date: 2023.08.07 12:16:30 -06'00'

Privacy Officer, Michael Hartmann

ASHTON BOTTS

Digitally signed by ASHTON BOTTS
Date: 2023.08.08 13:54:02 -06'00'

Information Systems Security Officer, Ashton Botts

DENA LISTON

Digitally signed by DENA LISTON
Date: 2023.08.07 17:33:01 -04'00'

Information Systems Owner, Dena Liston

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).

- Department of Veterans Affairs Veterans Health Administration NOTICE OF PRIVACY PRACTICES
- 23VA10NB3, Non–VA Care (Fee) Records – VA (7/30/2015)
- 24VA10A7, Patient Medical Records – VA (10/2/2020)
- 43VA008, Veterans, Dependents of Veterans, and VA Beneficiary Survey Records - VA (1/25/2021)
- 54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files – VA (3/3/2015)
- 58VA21/22/28, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records - VA (11/8/2021)
- 79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records – VA (12/23/2020)
- 88VA244, Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line System (CAR/CAROLS, combined system referred to as CAO) (8/13/2018)
- 147VA10, Enrollment and Eligibility Records - VA (8/17/2021)
- https://department.va.gov/privacy/system-of-records-notices/

HELPFUL LINKS:

Record Control Schedules:

https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

General Records Schedule 1.1: Financial Management and Reporting Records (FSC):

https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

National Archives (Federal Records Management):

https://www.archives.gov/records-mgmt/grs

VHA Publications:

https://www.va.gov/vhapublications/publications.cfm?Pub=2

VA Privacy Service Privacy Hub:

https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices