Privacy Impact Assessment for the VA IT System called:

Payer EDI TAS (PED)

Veterans' Health Administration (VHA)

Office of Integrated Veteran Care

eMASS ID #1317

Date PIA submitted for review:

May 29, 2025

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Eller Pamintuan	Eller.Pamintuan@va.gov	303-331-7512
Information System Security Officer (ISSO)	Paul Bartholomew	Paul.Bartholomew@va.gov	787-641-7582
Information System Owner (ISO)	Dena Liston	Dena.Liston@va.gov	304-886-7367

Abstract

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

The Payer Electronic Data Interchange (EDI) Transactions Applications Suite (TAS) is a cloud-based system that supports Community Care Payer services for the U.S. Department of Veterans Affairs (VA). It modernizes business processes by transitioning to a solution that complies with the Health Insurance Portability and Accountability Act (HIPAA) and utilizes the X12 standard for EDI transactions. The Payer EDI TAS (PED) platform routes and maps data to the appropriate systems, supports financial transactions with the VA's Financial Services Center in Austin, and enables secure data access for external partners. It plays a critical role in ensuring timely payments to private healthcare providers, fostering ongoing support for Veteran care.

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?

The PED environment is a cloud-based information system that efficiently supports the VA in processing healthcare claims, including professional, institutional, dental, and pharmacy transactions. Acting as the primary gateway, PED manages all inbound and outbound data exchanges between VA systems and external business partners, ensuring secure, accurate, and compliant transmission of sensitive health and financial information.

As the system's orchestration engine, PED oversees the full lifecycle of claim-related data. It coordinates scheduling, directs transmissions to the appropriate destinations, and archives data in raw, active, and completed states within a secure Structured Query Language (SQL) database.

PED plays a vital role in advancing the VA's mission to provide timely and accurate healthcare benefits to Veterans. Streamlining interactions with private-sector providers and payers upholds data integrity, operational efficiency, and accountability. Furthermore, it reinforces the VA's position as the official steward of Veteran data, as outlined in established Memoranda of Understanding (MOUs) and Interconnection Security Agreements (ISAs) with participating entities.

MOU/ISA

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

The PED system is a VA-owned and VA-operated information system. The VA has complete control, operational authority, and system oversight. The system is governed in accordance with federal cybersecurity and privacy regulations and is recorded within the

VA's Enterprise Mission Assurance Support Service (eMASS) as a VA-authorized asset. All administrative, technical, and operational responsibilities are managed by VA personnel, ensuring that data stewardship, compliance, and risk management remain under the agency's direct control.

2 Information Collection and Sharing

A. 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?

The PED platform supports the healthcare claims processing needs of over 660,000 Veterans and their eligible beneficiaries. These individuals are typically recipients of VA-funded care through community providers. While the system does not directly process payments, it facilitates the secure receipt, translation, and routing of healthcare claims data to designated VA systems for adjudication and settlement. The system operates fully automatically, without direct interaction with individuals, and processes structured claim-related data elements as part of its core function.

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

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

The PED system processes and routes healthcare claims data between the VA and various internal and external systems involved in claims adjudication and provider payment. These systems include, but are not limited to, Signature Choice CXM, Change Healthcare Clearinghouse, Optum Rx, Claims Eligibility & Processing (CPE), Financial Management System (FMS), and Program Integrity Tool (PIT). While some transactions occur in real time, most are exchanged in secure batch files, consistent with the system's primarily batch-based architecture.

The information collected and transmitted by PED includes sensitive healthcare claims data, often containing Veterans' Personally Identifiable Information (PII) and Protected Health Information (PHI). Although the system does not directly influence patient care decisions, it is critical in ensuring accurate claims routing, eligibility verification, and

payment processing. In accordance with the Privacy Act, Title 38 confidentiality requirements, and the Health Insurance Portability and Accountability Act (HIPAA), PED employs robust safeguards to protect this data. These safeguards include end-to-end encryption, restricted access for interfacing partners, and controlled use within the VA Enterprise Cloud (VAEC) hosted on Amazon Web Services (AWS) (VAEC-AWS).

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

The PED environment is a fully automated system that facilitates the secure exchange of healthcare claims information in support of Community Care Payer services. It acts as a central data integration and routing hub, receiving, translating, and transmitting structured claims data to designated VA systems and external business partners responsible for claims adjudication, eligibility verification, and financial processing.

The system shares information with multiple components and interfacing platforms, including the Signature Choice Care Experience Management (CXM) system, Change Healthcare Clearinghouse, Optum Rx, Claims Eligibility & Processing (CPE), Financial Management System (FMS), and the Program Integrity Tool (PIT), among others. These integrations enable the coordinated delivery of healthcare reimbursement services to Veterans and their eligible dependents.

PED manages data on over 660,000 Veterans and beneficiaries, including PII, PHI, and limited financial data. All data exchanges are conducted using secure protocols, with encryption applied during transit and at rest. The system reduces human interaction, relying instead on system-to-system communication governed by predefined workflows, access controls, and strict compliance with federal privacy and security requirements.

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

PED does not contain separate modules or subsystems.

E. 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?

The PED system operates solely within the VA VAEC-AWS in a primary cloud environment. Although the system does not employ multiple operational sites, it upholds strong continuity and data protection capabilities through built-in cloud redundancy and geographically resilient backup storage.

In collaboration with the Information System Owner (ISO), the Office of Information and Technology (OIT) identifies and manages critical system software and security-related data to ensure recovery readiness. PED is backed up at least once every 24 hours, with all backups stored in AWS environments that feature local redundancy and asynchronous replication to a geographically separate location. These backups are encrypted in transit and at rest using Advanced Encryption Standard (AES) 256-bit encryption, fully compliant with Federal Information Processing Standard (FIPS) 140-2.

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

F. What is the citation of the legal authority?

Legal Authority: 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.

Legal Authority: Title 38, United States Code, Sections 501(b) and 304.

Legal Authority: Title 38, United States Code, sections 501(a), 501(b), 1703, 1720G, 1724, 1725, 1728, 1781, 1787, 1802, 1803, 1812, 1813, 1821, Public Law 103–446 section 107 and Public Law 111–163 section 101.

Legal Authority: Title 10 United States Code, Chapters 106a, 510, 1606 and 1607 and title 38, United States Code, § 501(a) and Chapters 3, 11, 13, 15, 18, 19, 21, 23, 30, 31, 32, 33, 34, 35, 36, 37, 39, 51, 53, 55, and 77. Title 5 United States Code, Section 5514.

Legal Authority: Title 38, United States Code, Section 7301(a).

Legal Authority: Title 28, United States Code, Title 38, United States Code, Sections 501(a), 1705, 1710, 1722, and 5317.

G. What is the SORN?

23VA10NB3, Non-VA Care (Fee) Records - VA (7/30/2015),
https://www.govinfo.gov/content/pkg/FR-2015-07-30/pdf/2015-18646.pdf

24VA10A7, Patient Medical Records - VA (10/2/2020),
https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry, and Payment Files -VA (3/3/2015),
https://www.govinfo.gov/content/pkg/FR-2015-03-03/pdf/2015-04312.pdf

58VA21/22/28, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records - VA (11/8/2021),
https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records –VA (12/23/2020),
https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf

147VA10, Enrollment and Eligibility Records -VA (8/17/2021),

https://www.govinfo.gov/content/pkg/FR-2021-08-17/pdf/2021-17528.pdf

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

if yes, <<ADD ANSWER HERE>>

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 (DOB)
☐ Mother's Maiden Name
☒ Personal Mailing Address
☒ Personal Phone Number(s)
☐ Personal Fax Number
☒ Personal Email Address
☐ Emergency Contact Information (Name, Phone Number, etc. of a Different Individual)
☒ Financial Information
☒ Health Insurance Beneficiary Numbers Account Numbers
☐ Certificate/License Numbers[1]
☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☒ Medications
☒ Medical Records
☐ Race/Ethnicity
☒ Tax Identification Number
☒ Medical Record Number
☐ Sex
☐ Integrated Control Number (ICN)
☐ Military History/Service Connection
☐ Next of Kin
☒ Date of Death (DOD)
☐ Business Email Address
☐ Electronic Data Interchange Personal Identifier (EDIPI)
☒ Other Data Elements (List Below)

Other PII/PHI Data Elements:

- 2nd Address
- Member Identification Number
- Patient Control Number
- Coverage Dates
- Plan Name
- Current Procedural Terminology
- CPT/International Code Designator (ICD)
- Coded Billing Information (Claim Index)
- Billed Amounts
- Other Health Insurance Information
- Insurance Financial Management System (FMS) Document ID
- Paid Amounts
- Check or Remittance Numbers
- Provider Name
- Provider Phone Number
- Provider Billing Address
- Provider Physical Address
- Provider Remit to Address
- Diagnosis Codes
- Treatment Codes
- Prescription Numbers
- National Council for Prescription Drug Programs (NCPDP) Codes

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

- Date of Service (DOS)
- Place of Service (POS)
- Charge Amount
- Coverage Details

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?

The PED system does not directly collect information from Veterans or their beneficiaries. Instead, the data is initially submitted by the Veteran or beneficiary to a community healthcare provider delivering the covered service. These providers then send the claims and associated information to the VA through a third-party clearinghouse. PED acts as an intermediary, receiving, translating, and routing the claims data within the VA's enterprise systems.

The system collects, processes, and maintains sensitive information, including Veterans' PII and, when applicable, PHI. To ensure traceability and data integrity during claims processing, each transaction is tagged with a unique Patient Document Identifier (PDI). This identifier allows for linking related claims and ensures complete record continuity.

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.

PED receives healthcare claims information indirectly through industry providers and third-party clearinghouses, rather than directly from Veterans or their beneficiaries. This approach is necessary because Veterans obtain care from external, community-based providers responsible for documenting and submitting claims for reimbursement to the VA.

These clearinghouses serve as secure intermediaries that standardize and transmit claims data to the VA's EDI Gateway for further processing. This system design ensures compatibility with healthcare industry standards and enables high-volume, automated claims processing without requiring direct interaction from VA users. Utilizing this data source streamlines the reimbursement process, reduces administrative burdens, and assists the VA in providing timely payments for services rendered to Veterans.

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

PED does not independently generate new information, such as scores, analytical outcomes, or reports intended for decision-making about individuals. Instead, it functions as a secure data routing and transformation system that facilitates the structured exchange of

healthcare claims data between external providers and internal VA systems through third-party clearinghouses.

While PED ensures that data is formatted to meet technical and regulatory standards (such as HIPAA X12 transaction sets), it does not perform analytical functions or create standalone reports or evaluations. All data received and transmitted by the system originates from external sources, primarily healthcare providers. It is maintained in its processed state for traceability, validation, and integration into downstream claims adjudication systems within the VA enterprise.

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?

PED is a privacy-sensitive system that collects, processes, and maintains healthcare claims data for veterans and their beneficiaries. The primary data collection method involves secure electronic transmission from external healthcare service providers that submit claims via Change Healthcare Clearinghouse. These electronic submissions adhere to industry-standard formats, such as HIPAA-compliant X12 transaction sets, and are transmitted to the VA through encrypted channels.

In rare instances, a small subset of claims may originate from veterans or their beneficiaries and be submitted through traditional methods like the United States Mail. Once received by the VA, these paper-based claims are digitized and integrated into the electronic claims processing stream.

All data the system receives, regardless of origin, is managed using secure technologies that store and transmit information in a recognizable form. The system employs encryption, role-based access controls, and secure data routing mechanisms to ensure the protection and confidentiality of all PII and PHI throughout the data lifecycle.

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?

In this context, PED does not collect information through VA-issued forms and is therefore not subject to the Paperwork Reduction Act (PRA). Data is not gathered directly from individuals via standardized information collection instruments. Instead, the system receives claims data electronically from healthcare industry providers through third-party clearinghouses. These transactions are transmitted using secure protocols such as Secure Sockets Layer (SSL) and adhere to standardized EDI formats, including HIPAA-compliant X12 formats. Consequently, no Office of Management and Budget (OMB) control number or agency form number applies to this system's data intake process.

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.

PED employs multiple mechanisms to ensure the data's accuracy and integrity. Upon receipt, healthcare claims undergo a series of automated edits and integrity checks, many of which are embedded within the commercially acquired EDI processing tools integrated into the system. These validations include conformity with the HIPAA-mandated transaction formats and compliance with business rules.

Claims that do not meet established data quality or structural standards are automatically rejected. In such cases, the clearinghouse is notified, and the claim is returned to the originating healthcare provider for correction and resubmission. This automated loop ensures that only accurate and properly formatted data enters the VA's claims processing environment.

Additionally, the system supports batch and real-time processing modes, during which internal data reconciliation and table-level validation checks are performed to prevent corruption or unintentional alterations during data movement. Aggregated reports on claims activity, organized by identifiers such as Claim ID and Sponsor, are generated in accordance with Veterans Health Administration (VHA) control standards, further, to support auditing, reconciliation, and oversight functions.

Currently, there are no formal computer matching agreements with other federal agencies. However, internal checks ensure that data is validated before processing decisions regarding a claim or individual are made.

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?

PED does not verify data accuracy through any commercial aggregator or third-party data enrichment service. Instead, data integrity and completeness are managed internally through the system's built-in validation and processing routines. The volume of data received corresponds to the structured deliverables transmitted by healthcare providers via clearinghouses.

PED's primary responsibility is to ensure that all received data is handled securely, validated against established business rules, and protected throughout its lifecycle. The system focuses on safeguarding PII and maintaining data quality through technical controls rather than external verification sources. There are no contractual requirements or processes involving commercial aggregators for accuracy validation.

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

The operation of the PED platform, and its collection and processing of PII and PHI, is supported by a robust framework of federal laws, regulations, and statutory authorities. These authorities empower the VA to manage healthcare delivery, claims processing, and benefits administration for Veterans and their beneficiaries. The legal basis includes:

- **Title 38, United States Code (U.S.C.)** – The primary statutory authority for VA operations, including sections that govern medical care (e.g., §§ 1703, 1710, 1720, 1724, 1725, 1728), benefits eligibility, and healthcare administration. Sections 501(a) and 501(b) authorize the VA Secretary to prescribe rules and regulations necessary to carry out the provisions of Title 38.
- **Title 5, U.S.C. § 301 and § 5514** – Provides authority for departmental governance and federal employees' collection of debts owed to the United States.
- **Title 10, U.S.C., Chapters 106a, 510, 1606, and 1607** – Provides authority regarding specific Veteran education and reserve component benefits relevant to the population served.
- **Title 26, U.S.C. § 61** – Defines gross income for tax purposes, which may intersect with benefits processing in claims handling contexts.
- **Title 44, U.S.C.** – Authorizes federal information management, including records management and privacy obligations under the Federal Information Security Modernization Act (FISMA).
- **Title 45, Code of Federal Regulations (CFR), Parts 160 and 164** – Implements the Health Insurance Portability and Accountability Act (HIPAA), mandating the protection of individually identifiable health information and establishing national standards for electronic healthcare transactions.
- **38 CFR § 2.6** – Defines the duties of VA officials, including those responsible for claims, information systems, and data handling.
- **Veterans Access, Choice, and Accountability Act of 2014** – Authorizes expanded access to community care, under which many of the claims processed by Payer EDI TAS originate.
- **Public Laws 103–446 § 107 and 111–163 § 101** – Provide specific enhancements to Veteran benefits and administrative capabilities.
- **Title 28, U.S.C.** – Governs federal judiciary operations relevant to legal compliance and data handling.
- **Title 38, U.S.C. §§ 7301(a), 7332, and 5701** – Establish provisions related to the organization and confidentiality of VA medical services and the protection of Veteran records.

These authorities collectively create the legal framework for collecting, using, and protecting personal and health information processed by the PED system in support of VA healthcare operations.

1.6 <u>PRIVACY IMPACT ASSESSMENT: Characterization of the information</u>

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks.

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: The system collects and processes a significant volume of PII and PHI related to Veterans and their beneficiaries. A key privacy risk is that the system may retain more information than is strictly necessary to fulfill its operational purpose. If this data were improperly accessed, disclosed, or breached, it could substantially harm affected individuals, including identity theft, loss of privacy, financial fraud, and reputational and legal consequences for the VA.

Mitigation: The system adheres to strict data minimization principles to mitigate this risk by processing only the structured data elements required to support healthcare claims routing and adjudication. Although the VA does not initially generate the data, all information is handled in accordance with federal privacy and security regulations, including the HIPAA.

The system leverages industry-standard data coding practices and is protected by multiple technical and operational control layers. These include:

- **Encryption**: All data in transit and at rest is secured using encryption protocols compliant with Federal Information Processing Standard (FIPS) 140-2.
- **Access Control**: Access is strictly limited to authorized VA personnel and contractors with a validated business need, and all users must authenticate through approved VA identity management protocols.
- **Monitoring and Vulnerability Management**: The VA's Cyber Security Operations Center (CSOC) continuously monitors the system for vulnerabilities and promptly addresses them through the VA's established incident response and remediation processes.
- **Training and Oversight**: All users must complete annual VA privacy and security training, which reinforces their responsibilities for safeguarding sensitive information.

These measures collectively ensure that the system operates within the bounds of necessity, minimizes privacy risks, and upholds the VA's commitment to protecting Veteran and beneficiary data.

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
Patient Name	Used to identify patients for appointments, billing, and communication with providers and insurers.	To facilitate the electronic payment of health care claims.
Social Security Number (SSN)	Used as a unique patient identifier to verify eligibility, identity, and benefits with federal agencies.	To facilitate the electronic payment of health care claims.
Date of Birth (DOB)	Used to verify identity, determine age-based eligibility, and for accurate matching across systems.	To facilitate the electronic payment of health care claims.
Date of Death (DOD)	Used to prevent fraudulent claims and ensure proper closure and reconciliation of accounts.	To facilitate the electronic payment of health care claims.
Address	Used for mailing correspondence, determining residency eligibility, and confirming patient identity.	To facilitate the electronic payment of health care claims.
2nd Address	Used for mailing correspondence, determining residency eligibility, and confirming patient identity.	To facilitate the electronic payment of health care claims.
Personal Phone Number(s)	Used to contact patients for claim clarification, eligibility verification, or benefit-related communication.	To facilitate the electronic payment of health care claims.
Personal Email	Used for digital communication related to claims status, documentation requests, and account inquiries.	To facilitate the electronic payment of health care claims.

Member Identification Number	Used to uniquely identify a patient within a specific health plan or benefits system.	To facilitate the electronic payment of health care claims.
Patient Control Number	Internal reference number used to track claims and patient billing activity across systems.	To facilitate the electronic payment of health care claims.
Medications	Used to assess the medical necessity and appropriateness of claims, especially for pharmacy billing and coordination of care.	To facilitate the electronic payment of health care claims.
Medical Records	Used to substantiate services rendered, verify diagnoses, and validate claim accuracy.	To facilitate the electronic payment of health care claims.
Medical Record Identification Number	Links patient medical records to claims and supports audit, tracking, and documentation review.	To facilitate the electronic payment of health care claims.
Health Insurance Numbers	Used to verify a patient's coverage with the health plan to determine claim eligibility.	To facilitate the electronic payment of health care claims.
Coverage Dates	Used to confirm active coverage during service to validate payment responsibility.	To facilitate the electronic payment of health care claims.
Plan Name	Identifies the insurance plan to route and adjudicate the claim correctly.	To facilitate the electronic payment of health care claims.
Current Procedural Terminology	Standardized codes used to describe medical, surgical, and diagnostic services; essential for billing, reimbursement, and ensuring consistency in claims adjudication.	To facilitate the electronic payment of health care claims.
CPT/International Code Designator (ICD)	Used for standardized medical coding to support consistent billing and service evaluation.	To facilitate the electronic payment of health care claims.
Coded Billing Information (Claim Index)	Contains grouped data necessary for systematic claims processing and validation.	To facilitate the electronic payment of health care claims.
Billed Amounts	It reflects the cost of services submitted for payment and is used to determine reimbursement value.	To facilitate the electronic payment of health care claims.

Other Health Insurance Information	Used to coordinate benefits and determine primary vs. secondary payer responsibilities.	To facilitate the electronic payment of health care claims.
Insurance Financial Management System (FMS) Document ID	Tracks financial documents across systems for claim reconciliation and audit purposes.	To facilitate the electronic payment of health care claims.
Financial Information	Includes costs, payment amounts, and financial adjustments necessary for claims adjudication.	To facilitate the electronic payment of health care claims.
Health Insurance Beneficiary Numbers	Links patients to specific benefit programs, such as Medicare/Medicaid, for claim processing.	To facilitate the electronic payment of health care claims.
Paid Amounts	Represents the payment issued for a claim and is used in audits and financial reporting.	To facilitate the electronic payment of health care claims.
Check or Remittance Numbers	Identifies the payment transaction for tracking and reconciliation with provider systems.	To facilitate the electronic payment of health care claims.
Provider Name	Identifies the rendering or billing provider responsible for services.	To facilitate the electronic payment of health care claims.
Provider Phone Number	Used to clarify submitted claims, service details, or follow up on documentation.	To facilitate the electronic payment of health care claims.
Provider Billing Address	Designates where to send payments and related correspondence.	To facilitate the electronic payment of health care claims.
Provider Physical Address	Indicates the service location, used for POS validation and geographic eligibility.	To facilitate the electronic payment of health care claims.
Provider Remit to Address	Specifies the address for remittance of payments and explanation of benefits (EOBs).	To facilitate the electronic payment of health care claims.
Tax Identification Number (TIN)	Used to report payments for tax purposes and to validate provider identity for claims.	To facilitate the electronic payment of health care claims.
Diagnosis Codes	Used to validate the reason for services provided and determine medical necessity.	To facilitate the electronic payment of health care claims.

Treatment Codes	Used to support procedures performed; critical for claim evaluation and billing.	To facilitate the electronic payment of health care claims.
Prescription Numbers	Identifies dispensed medications for payment verification and audit purposes.	To facilitate the electronic payment of health care claims.
National Council for Prescription Drug Programs (NCPDP) Codes	Used to ensure proper drug identification and reimbursement within pharmacy claims.	To facilitate the electronic payment of health care claims.
Date of Service (DOS)	Confirms when services were rendered to validate timeliness and coverage eligibility.	To facilitate the electronic payment of health care claims.
Place of Service (POS)	Identifies the physical location where care was delivered to validate appropriate billing codes.	To facilitate the electronic payment of health care claims.

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?

The ClaimXM system supports the VA by generating operational reports that provide insight into the volume, frequency, and status of processed healthcare claims. These reports assist VA analysts and program managers track claims processing performance, identify trends, and monitor system throughput.

While ClaimXM does not conduct complex analytics such as scoring, pattern recognition, or predictive modeling, it compiles structured data summaries highlighting activity across various claims categories and providers. The system's output helps identify anomalies or potential backlogs that may warrant further investigation by VA personnel.

Processed claims data is ultimately transferred to the Claims Processing and Eligibility (CP&E) Data Warehouse, where more advanced analytical functions can be applied. These downstream analyses may include relational linkages across claim submissions, timeliness assessments, and longitudinal evaluations to support operational planning, compliance oversight, and program improvement initiatives.

2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

The ClaimXM system does not create new or previously unused information about individuals to make determinations or take actions that affect them. While the system generates reports detailing the volume, frequency, and status of processed healthcare claims, these reports are aggregate and intended to support operational oversight, workload tracking, and system performance analysis.

Any claim-related data derived during processing, such as timestamps, routing information, or claim status codes, is stored within existing transaction records and ultimately integrated into the Claims Processing and Eligibility (CP&E) Data Warehouse. This derived data supports administrative processes and system monitoring, not initiating or influencing decisions about individual Veterans or beneficiaries.

No new records are created solely from this derived information, and no direct actions, positive or negative, are taken against individuals based on these reports. Access to any claim-related data, including derived elements, is strictly limited to authorized VA personnel with a defined business need. These users operate under established privacy, security, and role-based access controls to ensure appropriate data handling in compliance with VA policy and federal regulations.

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?

The system uses multiple layers of security to protect sensitive data, including PII and PHI, during storage and transmission.

For Data at Rest: Information is stored on encrypted arrays that comply with the FIPS 140-2. These solutions protect physical and virtual storage media data from unauthorized access, ensuring confidentiality, integrity, and resilience against potential compromise.

For Data in Transit: All data transmitted across internal and external networks is protected using strong encryption protocols, including Transport Layer Security (TLS), to maintain confidentiality and integrity while in transit. These measures help prevent interception, unauthorized access, or data alteration during transfer between systems or external partners.

In both scenarios, encryption controls are implemented according to VA Handbook 6500 and relevant federal cybersecurity guidelines, ensuring the protection of sensitive information throughout its lifecycle.

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).

Yes, the system employs enhanced protections for any Social Security Numbers (SSNs) collected, processed, or retained. All SSNs are treated as highly sensitive data and are subject to strict handling and security requirements in accordance with VA policy and federal regulations.

Data in Transit: SSNs are transmitted using secure, encrypted channels that utilize industry-standard protocols such as Hypertext Transfer Protocol Secure (HTTPS) and Virtual Private Network (VPN) technologies. These protocols ensure end-to-end encryption and safeguard the confidentiality and integrity of SSNs during data transmission.

Data at Rest: Stored SSNs are encrypted in compliance with 140-2 using strong encryption algorithms. This ensures that SSNs remain protected on all storage media, whether primary or backup, and cannot be accessed without proper authorization.

Access and Handling Controls: SSNs are tightly restricted to authorized personnel with a validated business need and enforced through role-based access controls and multi-factor authentication. The system also supports audit logging and monitoring capabilities to detect and respond to unauthorized access attempts.

These additional safeguards are part of a comprehensive data protection strategy designed to minimize the risk of unauthorized exposure, maintain compliance with the Privacy Act, and uphold the VA's commitment to protecting Veteran information.

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

The system implements multiple layers of safeguards to protect PII and PHI in compliance with the requirements outlined in OMB Memorandum M-06-15. This includes preventing unauthorized access, limiting exposure risk, and ensuring accountability in handling sensitive data.

Data Encryption: All PII/PHI is encrypted at rest and in transit using protocols that meet or exceed VA standards and FIPS 140-2 requirements. This ensures that sensitive data remains protected even if accessed outside of authorized use.

Access Control and Authentication: Access to the system is restricted to authorized users operating within the VA network. All users are authenticated through VA-approved two-factor authentication (2FA), including using Personal Identity Verification (PIV) credentials. Elevated access privileges require formal approval and are provisioned through the Electronic Permissions Access System (ePAS) after supervisory and security review.

Session Management: The system enforces a 15-minute automatic timeout and session lock policy to mitigate the risk of unattended sessions. This helps prevent unauthorized viewing or misuse of PII or PHI in shared or unattended environments.

Policy Compliance and Oversight: All users must complete annual VA privacy and cybersecurity training, reinforcing best practices in handling sensitive information. System usage is logged and monitored to detect and respond to unauthorized access attempts, and compliance with OMB and VA policies is reviewed regularly.

These controls collectively ensure that the system aligns with the objectives of OMB M-06-15, which mandates the protection of PII through encryption, strict access control, and continuous oversight.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

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

2.4a How is access to the PII determined?

Access to PII within PED is determined through a structured, role-based access control process, consistent with VA policy and federal information security standards. Only users with a validated business need and defined roles are granted access. Authentication is enforced through VA-approved two-factor authentication, including Personal Identity Verification (PIV) credentials and Active Directory (AD) validation. Access requests must be submitted via the Electronic Permissions Access System (ePAS) and the e9957 process, specifying the required role and justification.

Each request undergoes approval from supervisory and designated authorization officials and must be initiated by someone with a higher level of authority than the requestor to ensure proper oversight. The Office of Information Technology (OIT) approves final access and provision. AD group membership enforces access permissions, automatically enabling or denying system entry based on role assignments.

To protect PII and uphold the privacy principles of transparency and use limitation, while aligning with privacy controls, the system incorporates:

CA-02 (Control Assessments): Regular reviews and audits to verify appropriate access control implementation.

AT-01 (Security Awareness and Training): Mandatory annual privacy and security training for all users with access to PII.

IR-08 (Incident Response – Privacy): Established incident response procedures to address unauthorized access, including revocation of access rights and notification protocols.

These measures ensure that access is granted appropriately, monitored continuously, and promptly revoked when it is no longer necessary or in the event of misuse.

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?

Yes, the criteria, procedures, controls, and responsibilities governing access to the system are formally documented and maintained in accordance with VA policy. These requirements are outlined in official VA policies, Standard Operating Procedures (SOPs), and mandatory training programs that define the user access lifecycle, from request and approval to revocation and re-certification.

All VA employees, contractors, and affiliates with access to systems containing Veterans' information must complete annual training on the VA Rules of Behavior and Privacy and Security Awareness training. These trainings detail individual responsibilities for safeguarding sensitive information and outline the consequences of non-compliance, which may include administrative action or termination.

Access management procedures, which include role-based access assignments, approvals, modifications, and de-provisioning, are documented within VA SOPs and carried out through systems such as the Electronic Permissions Access System (ePAS). These controls are regularly reviewed and updated to align with applicable security frameworks.

All documentation is centrally stored in the official VA policy repositories and the organization's SOP libraries, and it is accessible to authorized personnel through VA's internal knowledge management platforms. These documents support compliance with access control policies, audit readiness, and ongoing security governance.

2.4c Does access require manager approval?

Yes, access to the system requires documented approval from a user's supervisor as part of a formal access control process. All access requests are submitted and processed through the Electronic Permissions Access System (ePAS) and the e9957 procedure. Before granting access, each request must be reviewed and explicitly approved by the user's direct supervisor and a designated authorization official to ensure oversight and alignment with role-based access principles.

This approval process ensures access is granted only to individuals with a verified business need and aligns with their job responsibilities, following VA security policy and access control standards.

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

Yes, access to PII within the system is continuously monitored, tracked, and recorded to ensure compliance with VA policies and identify any unauthorized activity. All-access provisioning is documented through the Electronic Permissions Access System (ePAS) and e9957 workflows, which feature comprehensive audit trails of approval processes.

Once access is granted, user authentication is managed through Active Directory (AD), and all user activities, especially those involving access to PII, are subject to ongoing logging and automated monitoring. These logs capture access events, user actions, and system interactions and are routinely reviewed by security personnel to identify anomalies or policy violations.

These monitoring activities align with VA's broader cybersecurity and privacy governance framework, promoting accountability, transparency, and prompt incident response.

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

All users with access to the system are responsible for protecting Personally Identifiable Information (PII) by adhering to established privacy and security safeguards. Nonetheless, the primary accountability for ensuring these safeguards are effectively implemented and maintained rests with the system manager, as documented in the Enterprise Mission Assurance Support Service (eMASS).

The system manager is responsible for assigning access roles in accordance with the principle of least privilege, overseeing user authorization processes, and ensuring that technical, administrative, and physical controls align with the system's privacy and security requirements. This involves verifying that the safeguards outlined in the system's security documentation and technical design are applied in practice and remain effective throughout the system's lifecycle.

These responsibilities ensure compliance with federal mandates and VA policies designed to protect sensitive information and maintain the integrity of system operations.

Section 3. Retention of Information

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

*Identify and list all information collected from question 1.1 that is **retained** by the system. This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal*

Patient Identification and Communication:

- **Patient Name -** Used to identify patients for appointments, billing, and communication with providers and insurers.
- **Social Security Number (SSN) -** Used as a unique patient identifier to verify eligibility, identity, and benefits with federal agencies.
- **Date of Birth (DOB) -** Used to verify identity, determine age-based eligibility, and for accurate matching across systems.
- **Date of Death (DOD) -** Used to prevent fraudulent claims and ensure proper closure and reconciliation of accounts.
- **Address/2nd Address -** Used for mailing correspondence, determining residency eligibility, and confirming patient identity.
- **Personal Phone Number(s) -** Used to contact patients for claim clarification, eligibility verification, or benefit-related communication.
- **Personal Email -** Used for digital communication related to claims status, documentation requests, and account inquiries.

Member and Claim Tracking:

- **Member Identification Number -** Used to uniquely identify a patient within a specific health plan or benefits system.
- **Patient Control Number -** Internal reference number used to track claims and patient billing activity across systems.

Clinical Information and Evaluation:

- **Medications -** Used to assess the medical necessity and appropriateness of claims, especially for pharmacy billing and coordination of care.
- **Medical Records -** Used to substantiate services rendered, verify diagnoses, and validate claim accuracy.
- **Medical Record Identification Number -** Links patient medical records to claims and supports audit, tracking, and documentation review.
- **Diagnosis Codes -** Used to validate the reason for services provided and determine medical necessity.
- **Treatment Codes -** Used to support procedures performed, critical for claim evaluation and billing.
- **Prescription Numbers -** Identifies dispensed medications for payment verification and audit purposes.
- **National Council for Prescription Drug Programs (NCPDP) Codes -** Used to ensure proper drug identification and reimbursement within pharmacy claims.
- **Current Procedural Terminology (CPT) -** Standardized codes used to describe medical, surgical, and diagnostic services; essential for billing, reimbursement, and ensuring consistency in claims adjudication.

Insurance and Coverage Information:

- **Health Insurance Numbers -** Used to verify a patient's coverage with the health plan to determine claim eligibility.
- **Coverage Dates -** Used to confirm active coverage during service to validate payment responsibility.
- **Plan Name -** Identifies the insurance plan to route and adjudicate the claim correctly.
- **Other Health Insurance Information**
  Used to coordinate benefits and determine primary vs. secondary payer responsibilities.
- **Health Insurance Beneficiary Numbers -** Links patients to specific benefit programs, such as Medicare/Medicaid, for claim processing.

Billing, Payment, and Reconciliation:

- **CPT/International Code Designator (ICD) -** Used for standardized medical coding to support consistent billing and service evaluation.
- **Coded Billing Information (Claim Index) -** Contains grouped data necessary for systematic claims processing and validation.
- **Billed Amounts -** It reflects the cost of services submitted for payment and is used to determine reimbursement value.
- **Insurance Financial Management System (FMS) Document ID -** Tracks financial documents across systems for claim reconciliation and audit purposes.
- **Financial Information -** Includes costs, payment amounts, and financial adjustments necessary for claims adjudication.
- **Paid Amounts -** Represents the payment issued for a claim and is used in audits and financial reporting.

- **Check or Remittance Numbers -** Identifies the payment transaction for tracking and reconciliation with provider systems.

Provider Details and Claim Routing:

- **Provider Name -** Identifies the rendering or billing provider responsible for services.
- **Provider Phone Number -** Used to clarify submitted claims, service details, or follow up on documentation.
- **Provider Billing Address -** Designates where to send payments and related correspondence.
- **Provider Physical Address -** Indicates the service location, used for POS validation and geographic eligibility.
- **Provider Remit to Address -** Specifies the address for remittance of payments and explanation of benefits (EOBs).
- **Tax Identification Number (TIN) -** Used to report payments for tax purposes and to validate provider identity for claims.

Service Validation:

- **Date of Service (DOS) -** Confirms when services were rendered to validate timeliness and coverage eligibility.
- **Place of Service (POS) -** Identifies the physical location where care was delivered to validate appropriate billing codes.

3.2 How long is information retained?

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

SORN 23VA10NB3 – Retention and Disposal of Records:

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.

VHA RCS 10-1, Item 6000.2.b., Electronic Health Record (EHR) – Electronic Final Version of Health Record. **Disposition Instruction: Temporary.** Destroy/delete 75 years after the last episode of care. **Disposition Authority:** N1-15-02-3, item 3.

SORN 24VA10A7 – Retention and Disposal of Records:

In accordance with the records disposition authority approved by the Archivist of the United States, paper records and information stored on electronic storage media are maintained for seventy-five (75) years after the last episode of patient care and then destroyed/or deleted. VHA Records Control Schedule (RCS 10–1), Chapter 6, 6000.1d (N1–15–91–6, Item 1d) and 6000.2b (N1–15–02–3, Item 3).

VHA RCS 10-1, Item 6000.1.d., Inactive Health Record. **Disposition Instruction:** Retire annually to the records storage facility. If not recalled by the accessioning facility for reactivation, destroy by WITNESS DIPOSAL 72 years after retirement (75 after the last episode of care). **Disposition Authority:** N1-15-91-6, item 1d.

VHA RCS 10-1, Item 6000.2.b., Electronic Health Record (EHR) – Electronic Final Version of Health Record. **Disposition Instruction: Temporary.** Destroy/delete 75 years after the last episode of care. **Disposition Authority:** N1-15-02-3, item 3.

SORN 54VA10NB3 – Retention and Disposal of Records:

Record Control Schedule (RCS) 10–1 item XXXVIII Civilian Health and Medical care (CHMC) Records. NARA job number N1–015–3–1Item 1–8b. (Master file) item 3, Destroy 6 years after all individuals in the record become ineligible for program benefits.

VHA RCS 10-1, Item 1260.1.c., Electronic Records (Master Files). **Disposition Instruction: Temporary.** Destroy 6 years after all individuals in the record become ineligible for program benefits. **Disposition Authority:** N1-15-03-1, item 3.

SORN 58VA21/22/28 – Retention and Disposal of Records:

All claims' files folders for Compensation and Pension claims are electronically imaged and uploaded into the VBMS eFolder. Once a file is electronically imaged and established by VA as the official record, its paper contents (with the exception of documents that are on hold due to pending litigation, and service treatment records and other documents that are the property of DoD), are reclassified as duplicate—non record keeping—copies of the official record, and will be destroyed in accordance with Records Control Schedule VB–1, Part 1 Section XIII, Item 13–052.100 as authorized by NARA. All paper documentation that is not the property of VA (e.g., DoD-owned documentation) is currently stored by VA after scanning, pending a policy determination as to its final disposition. All documentation being held pursuant to active litigation is held in its native format during the pendency of the litigation. All VBMS eFolder's are stored on a secure VA server, pending permanent transfer to NARA where they will be maintained.

SORN 79VA10 – Retention and Disposal of Records:

VHA RCS 10-1, Item 2000.2., Information Technology Operations and Maintenance Records. **Disposition Instruction: Temporary**. Destroy 3 years after agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated or superseded, but longer retention is authorized if required for business use. **Disposition Authority:** DAA-GRS-2013-0005-0004, item 020.

VHA RCS 10-1, Item 2100.3., System Access Records / Systems requiring special accountability for access. **Disposition Instruction: Temporary**. Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use. **Disposition Authority:** DAA-GRS-2013-0006-0004, item 31.

SORN 147VA – Retention and Disposal of Records:

Per Records Control Schedule (RCS) 10–1 January 2020; use Health Eligibility Center disposition schedules 1250.1, 1250.2 and 1250.3. For 1250.1, destroy 7 years after the income year for which the means test verification was conducted, when all phases of Veteran's appeal rights have ended. If an appeal is filed, retain record until all phases of the appeal have ended; 1250.2, destroy 30 days after the data has been validated as being a true copy of the original data; and 1250.3, destroy when no longer needed.

VHA RCS 10-1, Item 1250.1., Health Eligibility Center (HEC) Records. **Disposition Instruction: Temporary**. Destroy 7 years after the income year for which the means test verification was conducted, when all phases of veteran's appeal rights have ended. If an appeal is filed, retain record until all phases of the appeal have ended. **Disposition Authority:** DAA-0015-2018-0001, item 0001.

VHA RCS 10-1, Item 1250.2., Tapes received from Social Security Administration (SSA) and Internal Revenue Service (IRS). **Disposition Instruction: Temporary.** Destroy 30 days after the data has been validated as being a true copy of the original data. **Disposition Authority:** DAA-0015-2018-0001, item 0002.

VHA RCS 10-1, Item 1250.3., Summary Reports and Other Output Records. **Disposition Instruction: Temporary.** Destroy when no longer needed. **Disposition Authority:** DAA-0015-2018-0001, item 0003.

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?

SORN 23VA10NB3 – Retention and Disposal of Records:

VHA RCS 10-1, Item 6000.2.b., Electronic Health Record (EHR) – Electronic Final Version of Health Record. **Disposition Instruction: Temporary.** Destroy/delete 75 years after the last episode of care. **Disposition Authority:** N1-15-02-3, item 3.

SORN 24VA10A7 – Retention and Disposal of Records:

In accordance with the records disposition authority approved by the Archivist of the United States, paper records and information stored on electronic storage media are maintained for seventy-five (75) years after the last episode of patient care and then destroyed/or deleted. VHA Records Control Schedule (RCS 10–1), Chapter 6, 6000.1d (N1–15–91–6, Item 1d) and 6000.2b (N1–15–02–3, Item 3).

VHA RCS 10-1, Item 6000.1.d., Inactive Health Record. **Disposition Instruction:** Retire annually to the records storage facility. If not recalled by the accessioning facility for

reactivation, destroy by WITNESS DIPOSAL 72 year after retirement (75 after the last episode of care). **Disposition Authority:** N1-15-91-6, item 1d.

VHA RCS 10-1, Item 6000.2.b., Electronic Health Record (EHR) – Electronic Final Version of Health Record. **Disposition Instruction: Temporary.** Destroy/delete 75 years after the last episode of care. **Disposition Authority:** N1-15-02-3, item 3.

SORN 54VA10NB3 – Retention and Disposal of Records

VHA RCS 10-1, Item 1260.1.c., Electronic Records (Master Files). **Disposition Instruction: Temporary.** Destroy 6 years after all individuals in the record become ineligible for program benefits. **Disposition Authority:** N1-15-03-1, item 3.

SORN 58VA21/22/28 – Retention and Disposal of Records

All claims' files folders for Compensation and Pension claims are electronically imaged and uploaded into the VBMS eFolder. Once a file is electronically imaged and established by VA as the official record, its paper contents (with the exception of documents that are on hold due to pending litigation, and service treatment records and other documents that are the property of DoD), are reclassified as duplicate—non record keeping—copies of the official record, and will be destroyed in accordance with Records Control Schedule VB–1, Part 1 Section XIII, Item 13–052.100 as authorized by NARA. All paper documentation that is not the property of VA (e.g., DoD-owned documentation) is currently stored by VA after scanning, pending a policy determination as to its final disposition. All documentation being held pursuant to active litigation is held in its native format during the pendency of the litigation. All VBMS eFolder's are stored on a secure VA server, pending permanent transfer to NARA where they will be maintained.

SORN 79VA10 – Retention and Disposal of Records

VHA RCS 10-1, Item 2000.2., Information Technology Operations and Maintenance Records. **Disposition Instruction: Temporary**. Destroy 3 years after agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated or superseded, but longer retention is authorized if required for business use. **Disposition Authority:** DAA-GRS-2013-0005-0004, item 020

VHA RCS 10-1, Item 2100.3., System Access Records / Systems requiring special accountability for access. **Disposition Instruction: Temporary**. Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use. **Disposition Authority:** DAA-GRS-2013-0006-0004, item 31.

SORN 147VA – Retention and Disposal of Records

VHA RCS 10-1, Item 1250.1., Health Eligibility Center (HEC) Records. **Disposition Instruction: Temporary**. Destroy 7 years after the income year for which the means test verification was conducted, when all phases of veteran's appeal rights have ended. If an appeal is filed, retain record until all phases of the appeal have ended. **Disposition Authority:** DAA-0015-2018-0001, item 0001.

VHA RCS 10-1, Item 1250.2., Tapes received from Social Security Administration (SSA) and Internal Revenue Service (IRS). **Disposition Instruction: Temporary.** Destroy 30 days after the data has been validated as being a true copy of the original data. **Disposition Authority:** DAA-0015-2018-0001, item 0002.

VHA RCS 10-1, Item 1250.3., Summary Reports and Other Output Records. **Disposition Instruction: Temporary.** Destroy when no longer needed. **Disposition Authority:** DAA-0015-2018-0001, item 0003.

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.

After the approved retention period, all Sensitive Personal Information (SPI), including PII and PHI, maintained within PED is securely destroyed or, where applicable, transferred to the National Archives and Records Administration (NARA) under federal records management requirements.

Electronic Records Destruction: For electronically stored information, data is permanently deleted from the system using VA-approved sanitization methods that render it irretrievable. These methods comply with VA Handbook 6500.1, Electronic Media Sanitization, which follows NIST Special Publication 800-88 Revision 1 guidelines. Deletion procedures include overwriting data, cryptographic erasure, and physically destroying storage media when necessary. Magnetic and digital media, such as hard drives and SSDs, are either physically shredded or sent to an authorized destruction vendor that provides a Certificate of Destruction.

Paper Records Destruction: For any physical records associated with claims processing, documents are destroyed on-site using cross-cut shredders to an unreadable state or are transferred to a secure third-party shredding service under contract with the VA. The destruction is accompanied by documented verification, including a Certificate of Destruction, in compliance with VA Directive 6371.

Transfer to NARA: Data is transferred following NARA-approved formats and procedures for permanent records, as identified under an approved NARA disposition authority. This includes converting records to acceptable archival formats, validating data integrity, and submitting transfer documentation through NARA's electronic Records Archives (ERA) system in coordination with the VA Records Officer.

Oversight and Documentation: All destruction and transfer processes are governed by Field Security Service (FSS) guidance, including FSS Bulletin #176 and SOP MP-6 Electronic Media Sanitization, which outline secure handling procedures and accountability measures. System owners and designated records management personnel ensure all activities are documented, auditable, and compliant with VA and federal records management policies.

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 establishes controls and procedural safeguards to minimize privacy risks related to the use of Personally Identifiable Information (PII) in non-operational environments, such as pre-production testing. When production data is necessary for validating system functionality, strict measures are implemented to protect the confidentiality and integrity of the data.

Copies of production data used for pre-production testing are limited to the minimum necessary to meet validation objectives. Access to this environment is restricted to a small, designated group of business analysts and fewer than five Independent Verification and Validation (IV&V) personnel. Role-based access controls are enforced, and user activity is logged to ensure accountability.

All personnel involved in testing must complete privacy and security training specific to handling sensitive data in test environments. The Training Office keeps training records to demonstrate compliance and awareness of the risks and responsibilities associated with using PII for testing.

Following internal policy, the Enterprise Security External Change Council (ESECC) must authorize all pre-production testing involving PII in advance. Policies and standard operating procedures (SOPs) have also been developed to ensure that, where feasible, de-identified or masked data is used instead of live PII to reduce exposure risk further.

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 in 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: PED collects and retains PII and PHI related to Veterans and their beneficiaries. If this information is kept longer than necessary or beyond its approved records disposition schedule, it increases the risk of unauthorized access, data breaches, or inadvertent disclosures. Extended retention also places a greater burden on the system to ensure continuous protection, accuracy, and integrity of sensitive information.

Mitigation: To mitigate this risk, the PED system follows a formally approved records retention schedule created with the VA Records Officer and the National Archives and Records Administration (NARA). Data is retained only as long as legally required to fulfill the system's mission, under the Principle of Minimization and the Federal Records Act. Retention schedules and procedures are outlined in VA Handbook 6300.1 and VA Directive 6300, ensuring that records are regularly reviewed and purged when no longer necessary.

The system is hosted in a FISMA-Moderate environment under the Office of Information and Technology (OIT) security guidelines. All retained data is encrypted during transit and at rest, in compliance with FIPS 140-2 standards, and is protected by documented Backup and Restore Plans within the AWS infrastructure. These plans ensure recoverability while facilitating controlled lifecycle management.

Business Associate Agreements (BAAs) are also established for contractors accessing PHI or PII, reinforcing third-party accountability. Designated supervisors review and verify access rights annually to ensure they align with operational roles.

All personnel with access to the system must complete mandatory annual privacy and security training through the VA's Talent Management System (TMS), which includes:

- **VA 10176** – VA Privacy and Information Security Awareness and Rules of Behavior
- **VA 10203** – Privacy and HIPAA Training

These controls collectively minimize the retention risk, ensure the relevance and integrity of retained data, and uphold VA's privacy commitments.

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 PED EDI TAS consists of 4 key components (servers/databases/instances/applications/software/application programming interfaces (API)). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **Payer EDI TAS** 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
Aurora Postgres (AWS Service)	Yes	Yes	Coverage Dates, Plan Name, Current Procedural Terminology, International Code Designator (ICD), Coded Billing Information (Claim Index), Billed Amounts, Other Health Insurance Information, Insurance FMS Document ID, Paid Amounts, Check or Remittance Numbers, Provider Name, Provider Phone Number, Provider Billing Address, Provider Physical Address, Provider Remit to Address), Tax Identification Number, Diagnosis Codes, Treatment Codes, Prescription Numbers, NCPDP Codes, Date of Service (DOS), Place of Service (POS), Patient Name, Social Security Number (SSN), Date of Birth (DOB), Data of Death (DOD), Address, 2nd Address, Email, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Numbers, Health Insurance Numbers (Policy Number)	Data is utilized to track, store, and process Veterans' healthcare claims.	Data is encrypted both at rest and during transit.
S3 Bucket (AWS Service)	Yes	Yes	Coverage Dates, Plan Name, Current Procedural Terminology, International Code Designator (ICD), Coded Billing Information (Claim Index), Billed	Data is utilized to track, store, and process Veterans' healthcare claims	Data is encrypted both at rest and during transit.

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
			Amounts, Other Health Insurance Information, Insurance FMS Document ID, Paid Amounts, Check or Remittance Numbers, Provider Name, Provider Phone Number, Provider Billing Address, Provider Physical Address, Provider Remit to Address), Tax Identification Number, Diagnosis Codes, Treatment Codes, Prescription Numbers, NCPDP Codes, Date of Service (DOS), Place of Service (POS), Patient Name, Social Security Number (SSN), Date of Birth (DOB), Data of Death (DOD), Address, 2nd Address, Email, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Numbers, Health Insurance Numbers (Policy Number). (SSN), Date of Birth (DOB), Data of Death (DOD), Address, 2nd Address, Email, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Numbers, Health Insurance Numbers (Policy Number).		
Payer EDI TAS SQL Server Database	Yes	Yes	Name, Social Security Number (SSN), Date of Birth (DOB), Data of Death (DOD), Street	Data is utilized to track, store, and process Veterans' healthcare claims	Data is encrypted both at rest

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
			Address, City, Zip Code, Country, Email, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Number, Plan/Policy Number, Member Identification, Plan Name, Coverage Effective Dates, Coverage Limits, Co-Pays, International Code Designator (ICD), Coded Billing Information (Claim Index), Billed Amounts, Other Health Insurance Information, Other Health Insurance FMS Document ID, Tax Identification Number (TIN), Phone Number, Place of Service (POS) Name, Place of Service Address (Street, City, Zip, Country),Date of Service, Charge Amount, Paid Amount, Diagnosis Codes, Treatment Codes, Prescription Number, NCPDP Codes, (National Council For Prescription Drug Programs)		and during transit.
Claims Database	Yes	Yes	Coverage Dates, Plan Name, Current Procedural Terminology, International Code Designator (ICD), Coded Billing Information (Claim Index), Billed Amounts, Other Health Insurance Information, Insurance FMS Document ID, Paid Amounts, Check	Data is utilized to track, store, and process Veterans' healthcare claims	Data is encrypted both at rest and during transit.

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
			or Remittance Numbers, Provider Name, Provider Phone Number, Provider Billing Address, Provider Physical Address, Provider Remit to Address), Tax Identification Number, Diagnosis Codes, Treatment Codes, Prescription Numbers, NCPDP Codes, Date of Service (DOS), Place of Service (POS), Patient Name, Social Security Number (SSN), Date of Birth (DOB), Data of Death (DOD), Address, 2nd Address, Email, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Numbers, Health Insurance Numbers (Policy Number)		

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 Administration (VHA) / Claim Processing & Eligibility System (CP&E)	Veteran beneficiary healthcare claim data, which includes all PII and related PHI values, is exchanged to support claim adjudication.	Coverage Dates, Plan Name, Current Procedural Terminology, International Code Designator (ICD), Coded Billing Information (Claim Index), Billed Amounts, Other Health Insurance Information, Insurance FMS Document ID, Paid Amounts, Check or Remittance Numbers, Provider Name, Provider Phone Number, Provider Billing Address, Provider Physical Address, Provider Remit to Address), Tax Identification Number, Diagnosis Codes, Treatment Codes, Prescription Numbers, NCPDP Codes, Date of Service (DOS), Place of Service (POS), Patient Name, Social Security Number (SSN), Date of Birth (DOB), Data of Death (DOD), Address, 2nd Address, Email, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Numbers, Health Insurance Numbers (Policy Number).	SFTP
Veterans Health Administration (VHA) / Financial Management System (FMS)	Veteran and beneficiary healthcare claim data, which includes PII and minimal PHI values, is exchanged to support claim payments and subsequent reconciliation between adjudicated claims and those that have been paid or not paid.	Coverage Dates, Plan Name, Current Procedural Terminology, International Code Designator (ICD), Coded Billing Information (Claim Index), Billed Amounts, Other Health Insurance Information, Insurance FMS Document ID, Paid Amounts, Check or Remittance Numbers, Provider Name, Provider Phone Number, Provider Billing Address, Provider Physical Address, Provider Remit to Address), Tax Identification Number, Diagnosis Codes, Treatment Codes, Prescription Numbers, NCPDP Codes, Date of Service (DOS), Place of Service (POS), Patient Name, Social Security Number (SSN), Date of Birth (DOB), Data of Death (DOD), Address, 2nd Address, Email, Member	FTPS

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*
		Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Numbers, Health Insurance Numbers (Policy Number)	
Veterans Health Administration (VHA) / Program Integrity Tool (PIT)	Veteran and beneficiary healthcare claim data, which includes all PII and numerous PHI values.	Coverage Dates, Plan Name, Current Procedural Terminology, International Code Designator (ICD), Coded Billing Information (Claim Index), Billed Amounts, Other Health Insurance Information, Insurance FMS Document ID, Paid Amounts, Check or Remittance Numbers, Provider Name, Provider Phone Number, Provider Billing Address, Provider Physical Address, Provider Remit to Address), Tax Identification Number, Diagnosis Codes, Treatment Codes, Prescription Numbers, NCPDP Codes, Date of Service (DOS), Place of Service (POS), Patient Name, Social Security Number (SSN), Date of Birth (DOB), Data of Death (DOD), Address, 2nd Address, Email, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Numbers, Health Insurance Numbers (Policy Number)	SFTP
Veterans Health Administration (VHA) / Integrated Veterans Care Centralized Data Repository (CDR)	Ingests data from multiple community care sources and stores it in an organized manner, allowing for easy access for reporting and analytical purposes.	Coverage Dates, Plan Name, Current Procedural Terminology, International Code Designator (ICD), Coded Billing Information (Claim Index), Billed Amounts, Other Health Insurance Information, Insurance FMS Document ID, Paid Amounts, Check or Remittance Numbers, Provider Name, Provider Phone Number, Provider Billing Address, Provider Physical Address, Provider Remit to Address), Tax Identification Number, Diagnosis Codes, Treatment Codes, Prescription Numbers, NCPDP Codes, Date of Service (DOS), Place of Service (POS), Patient Name, Social Security Number (SSN), Date of Birth (DOB), Data of Death (DOD), Address, 2nd Address, Email, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Numbers, Health Insurance Numbers (Policy Number)	SFTP
Veterans Health Administration	Provide the dataset to be consolidated with other	Coverage Dates, Plan Name, Current Procedural Terminology, International	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*
(VHA) / Community Care Reporting System (CCRS)	Integrated Veterans Care datasets into a single repository. These datasets are used for analytical and business improvement purposes.	Code Designator (ICD), Coded Billing Information (Claim Index), Billed Amounts, Other Health Insurance Information, Insurance FMS Document ID, Paid Amounts, Check or Remittance Numbers, Provider Name, Provider Phone Number, Provider Billing Address, Provider Physical Address, Provider Remit to Address), Tax Identification Number, Diagnosis Codes, Treatment Codes, Prescription Numbers, NCPDP Codes, Date of Service (DOS), Place of Service (POS), Patient Name, Social Security Number (SSN), Date of Birth (DOB), Data of Death (DOD), Address, 2nd Address, Email, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Numbers, Health Insurance Numbers (Policy Number)	
Veterans Health Administration (VHA) / Community Care Non-Network Claims	Provide the dataset to be consolidated with other Integrated Veterans Care datasets into a single repository. These datasets are used for analytical and business improvement purposes.	Coverage Dates, Plan Name, Current Procedural Terminology, International Code Designator (ICD), Coded Billing Information (Claim Index), Billed Amounts, Other Health Insurance Information, Insurance FMS Document ID, Paid Amounts, Check or Remittance Numbers, Provider Name, Provider Phone Number, Provider Billing Address, Provider Physical Address, Provider Remit to Address), Tax Identification Number, Diagnosis Codes, Treatment Codes, Prescription Numbers, NCPDP Codes, Date of Service (DOS), Place of Service (POS), Patient Name, Social Security Number (SSN), Date of Birth (DOB), Data of Death (DOD), Address, 2nd Address, Email, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Numbers, Health Insurance Numbers (Policy Number)	SFTP
Veterans Health Administration (VHA) / Veterans Enrollment System (VES)	The authoritative source for Veteran healthcare eligibility and benefits, derived from client enrollment applications, Military Service Information, rating decisions, financial	Coverage Dates, Plan Name, Patient Name, Social Security Number (SSN), Date of Birth (DOB), Data of Death (DOD), Address, 2nd Address, Email, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record	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, and other sources.	Numbers, Health Insurance Numbers (Policy Number).	
Veterans Health Administration (VHA) / Document Management Program	A claim processing component that documents the rationale for denied claims.	Coverage Dates, Plan Name, Patient Name, Social Security Number (SSN), Date of Birth (DOB), Data of Death (DOD), Address, 2nd Address, Email, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Numbers, Health Insurance Numbers (Policy Number).	Lambda IAM Transfer
Veterans Health Administration (VHA) / Medical Care Collections Fund Electronic Data Interchange Transactions Application Suite (MCCF EDI TAS)	The system facilitates electronic data exchange to and from VistA systems.	Coverage Dates, Plan Name, Patient Name, Social Security Number (SSN), Date of Birth (DOB), Data of Death (DOD), Address, 2nd Address, Email, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Numbers, Health Insurance Numbers (Policy Number).	SFTP
Veterans Health Administration (VHA) / Attachment Retrieval System (ARS) EDI Web Viewer (EWV)N	Veteran healthcare claim data includes all Personally Identifiable Information (PII) and all related Protected Health Information (PHI) necessary to support claim adjudication.	Coverage Dates, Plan Name, Current Procedural Terminology, International Code Designator (ICD), Coded Billing Information (Claim Index), Billed Amounts, Other Health Insurance Information, Insurance FMS Document ID, Paid Amounts, Check or Remittance Numbers, Provider Name, Provider Phone Number, Provider Billing Address, Provider Physical Address, Provider Remit to Address), Tax Identification Number, Diagnosis Codes, Treatment Codes, Prescription Numbers, NCPDP Codes, Date of Service (DOS), Place of Service (POS), Patient Name, Social Security Number (SSN), Date of Birth (DOB), Data of Death (DOD), Address, 2nd Address, Email, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Numbers, Health Insurance Numbers (Policy Number)	Batch access TCP. System in internal to the VA. Only approved employees and contractors have access to the system.
Veterans Health Administration (VHA) / Fee Payment Processing System (FPPS)	Veteran healthcare claim data includes all Personally Identifiable Information (PII) and all related Protected Health Information (PHI) necessary to support claim adjudication.	Coverage Dates, Plan Name, Current Procedural Terminology, International Code Designator (ICD), Coded Billing Information (Claim Index), Billed Amounts, Other Health Insurance Information, Insurance FMS Document ID, Paid Amounts, Check or Remittance Numbers, Provider Name, Provider Phone	Batch access TCP. System in internal to the VA. Only approved employees and contractors

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*
		Number, Provider Billing Address, Provider Physical Address, Provider Remit to Address), Tax Identification Number, Diagnosis Codes, Treatment Codes, Prescription Numbers, NCPDP Codes, Date of Service (DOS), Place of Service (POS), Patient Name, Social Security Number (SSN), Date of Birth (DOB), Data of Death (DOD), Address, 2nd Address, Email, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Numbers, Health Insurance Numbers (Policy Number)	have access to the system.
Veterans Health Administration (VHA) / Healthcare Informatics Veterans Data Integration and Federation Enterprise Platform (VDIF-EP)	To facilitate the sharing of procurement and vendor information between the VA and other business entities.	Coverage Dates, Plan Name, Current Procedural Terminology, International Code Designator (ICD), Coded Billing Information (Claim Index), Billed Amounts, Other Health Insurance Information, Insurance FMS Document ID, Paid Amounts, Check or Remittance Numbers, Provider Name, Provider Phone Number, Provider Billing Address, Provider Physical Address, Provider Remit to Address), Tax Identification Number, Diagnosis Codes, Treatment Codes, Prescription Numbers, NCPDP Codes, Date of Service (DOS), Place of Service (POS), Patient Name, Social Security Number (SSN), Date of Birth (DOB), Data of Death (DOD), Address, 2nd Address, Email, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Numbers, Health Insurance Numbers (Policy Number)	Batch access TCP. 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 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: PED shares data internally with other authorized VA systems and programs to support adjudication and benefit coordination of healthcare claims. However, there is an inherent risk that PII or PHI could be inadvertently accessed or disclosed to unauthorized VA systems, programs, or personnel. Such unauthorized internal sharing may compromise sensitive data, undermine data minimization principles, and lead to privacy violations or misuse.

Mitigation: To mitigate this risk, the Office of Information and Technology (OIT) enforces comprehensive access control policies and procedures that align with VA Handbook 6500 and NIST SP 800-53 Rev. 5 standards. These policies define internal data access's purpose, scope, and responsibilities and are reviewed and updated annually to reflect evolving operational and security needs.

Access to PII and PHI within the TAS system is governed by strict role-based access controls (RBAC) and is limited to authorized VA personnel with a documented business need. All internal data exchanges are authenticated and encrypted using FIPS 140-2 compliant protocols, ensuring confidentiality and integrity during transmission. Integration points with other VA systems are reviewed and approved through formal configuration management processes, with connections vetted by the Enterprise Security External Change Council (ESECC).

Additionally, system access logs and audit trails are continuously monitored to detect and investigate unauthorized or anomalous activity. Personnel with access to sensitive data must complete annual VA privacy and security training, reinforcing proper data-handling practices and their responsibilities under the Privacy Act and HIPAA.

These layered controls guarantee that data shared within the VA network is managed securely, stays within its intended boundaries, and adheres to the principle of the least privilege and data minimization.

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***
Trizetto Facets Claim (CXM) (Signature Performance	Veteran and beneficiary PII and PHI related to claim data are exchanged to support the adjudication of professional, institutional, dental, and pharmacy claims.	Coverage Dates, Plan Name, Current Procedural Terminology, International Code Designator (ICD), Coded Billing Information (Claim Index), Billed Amounts, Other Health Insurance Information, Insurance FMS Document ID, Paid Amounts, Check or Remittance Numbers, Provider Name, Provider Phone Number, Provider Billing Address, Provider Physical Address, Provider Remit to Address), Tax Identification Number, Diagnosis Codes, Treatment Codes, Prescription Numbers, NCPDP Codes, Date of Service (DOS), Place of Service (POS), Patient Name, Social Security Number (SSN), Date of Birth (DOB), Data of Death (DOD), Address, 2nd Address, Email, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Numbers, Health Insurance Numbers (Policy Number).	ISA/MOU	Site-to-Site (S2S) VPN Tunnel: Files are exchanged via SFTP.
Intelligent Medical Network	An industry provider	Coverage Dates, Plan Name, Current Procedural Terminology,	ISA/MOU	Site-to-Site (S2S) VPN

(IMN) (Change Healthcare)	gateway that offers real-time VA Veteran and Family Member healthcare eligibility and benefits approvals and authorizations.	International Code Designator (ICD), Coded Billing Information (Claim Index), Billed Amounts, Other Health Insurance Information, Insurance FMS Document ID, Paid Amounts, Check or Remittance Numbers, Provider Name, Provider Phone Number, Provider Billing Address, Provider Physical Address, Provider Remit to Address), Tax Identification Number, Diagnosis Codes, Treatment Codes, Prescription Numbers, NCPDP Codes, Date of Service (DOS), Place of Service (POS), Patient Name, Social Security Number (SSN), Date of Birth (DOB), Data of Death (DOD), Address, 2nd Address, Email, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Numbers, Health Insurance Numbers (Policy Number).		Tunnel: Files are exchanged via SFTP.
RxClaim (Optum)	Veteran and beneficiary PII and PHI claim-related data are exchanged to support the entire pharmacy claims process, from the initial receipt of pharmacy claims from Optum to the final disposition of payments back to Optum.	Coverage Dates, Plan Name, Current Procedural Terminology, International Code Designator (ICD), Coded Billing Information (Claim Index), Billed Amounts, Other Health Insurance Information, Insurance FMS Document ID, Paid Amounts, Check or Remittance Numbers, Provider Name, Provider Phone Number, Provider Billing Address, Provider Physical Address, Provider Remit to Address), Tax Identification Number, Diagnosis Codes, Treatment Codes, Prescription Numbers, NCPDP Codes, Date of Service (DOS), Place of Service (POS), Patient Name, Social Security Number (SSN), Date of Birth (DOB), Data of Death (DOD), Address, 2nd Address, Email, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Numbers, Health Insurance Numbers (Policy Number).	ISA/MOU	External Firewall

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 system shares PII and PHI with external entities, such as healthcare clearinghouses and industry partners, to support claims processing and care coordination for Veterans. Once this information leaves the VA's direct control, there is a risk that it could be inadvertently accessed, misused, or disclosed to unauthorized third parties. Such an incident could compromise individual privacy, expose sensitive health and financial data, and damage public trust in the VA

Mitigation: Data shared externally is governed by legally binding agreements, including Memoranda of Understanding (MOUs), Business Associate Agreements (BAAs), and Interconnection Security Agreements (ISAs), which outline each party's scope, purpose, and security responsibilities. These agreements require external partners to adhere to HIPAA Privacy Rule standards and VA policies, including implementing the principle of minimum necessary use.

All outbound data transmissions are encrypted using methods compliant with FIPS 140-2 to ensure confidentiality during transfer. Access controls are enforced on both sides of the data exchange, restricting data use to authorized individuals only. Additionally, the VA routinely monitors and reviews audit logs to confirm appropriate use and to detect any anomalies in data access or handling by external entities.

These safeguards ensure that sharing external information remains aligned with the original purpose of data collection: the secure and efficient processing of healthcare claims, while protecting Veteran data from unauthorized disclosure or misuse.

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.

The Payer Electronic Data Interchange Transactions Application Suite (TAS) provides notice to individuals regarding the collection and use of their information through multiple channels, consistent with the requirements of the Privacy Act of 1974 (5 U.S.C. § 552a), 38 U.S.C., and the eGovernment Act of 2002, Pub. L. 107–347, §208.

1. **Privacy Impact Assessment (PIA):** This PIA serves as an official notice to the public. According to the eGovernment Act, the completed PIA will be made publicly available on the Department of Veterans Affairs' website to inform individuals about the nature, purpose, and use of Personally Identifiable Information (PII) collected by the system.
2. **Notice of Privacy Practices (NOPP):** Upon enrolling in VA healthcare programs, veterans and beneficiaries receive a Notice of Privacy Practices (NOPP). This notice outlines how health and personal information may be used or disclosed and describes individuals' privacy rights under HIPAA and VA policy. A version of this notice is also published in the CHAMPVA Guide and is available at all VA medical facilities.
3. **Point-of-Service Notices:** At VA medical centers and points of care, individuals receive additional privacy notices following Veterans Health Administration (VHA) Handbook 1605.04, "Notice of Privacy Practices," ensuring in-person and situational awareness of how their data is utilized and protected.
4. **VA Privacy Website:** Comprehensive privacy notices, including published System of Records Notices (SORNs), are available on the VA Privacy Service website: https://www.oprm.va.gov/privacy/systems_of_records.aspx. These notices clarify data handling, record management, and sharing protocols.
5. **System of Records Notice (SORN):** The system is covered under VA SORN 168VA10P2, "Health Care Provider Credentialing and Privileging Records–VA," along with other applicable SORNs based on the nature of the records processed. These notices are published in the Federal Register and provide legal authority and procedural transparency for data collection and management.
6. **Social Security Number Disclosure Statement:** When applicable, individuals are informed that providing a Social Security Number (SSN) is voluntary and requested under the authority of 38 U.S.C. The SSN is used solely for identity verification and benefit administration, in compliance with the Privacy Act.

Appendix A of this PIA includes a copy of the most current VA Notice of Privacy Practices (NOPP) and references additional links to relevant notices and SORNs.

6.1b If notice was not provided, explain why.

PED does not collect information directly from Veterans, beneficiaries, or members of the public. Instead, PED receives structured data submissions from external entities, such as healthcare providers and clearinghouses, which initiate claims transactions on behalf of Veterans.

As the original data collectors, these entities are responsible for providing appropriate notice to individuals at the point of collecting, including the required disclosures under the Privacy Act of 1974 and HIPAA, where applicable. Therefore, PED does not issue a Privacy Act Notice independently at the time of collection.

Nonetheless, the VA ensures that the data received by PED is managed according to applicable privacy laws and covered under relevant System of Records Notices (SORNs) and the publicly available Privacy Impact Assessment (PIA), which together meet the transparency and notification requirements for downstream data processing.

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

Privacy notices provided during the information collection process align directly with PED's operational purpose: to process and route healthcare claims submitted on behalf of veterans and their beneficiaries.

Although the PED system does not gather data directly from individuals, privacy notices are provided to Veterans and beneficiaries at the initial point of enrollment and at the time of service by the VA or its community care partners. These notices, including the VA Notice of Privacy Practices (NOPP) outlined in VHA Handbook 1605.04, inform individuals how their information may be used and disclosed. This encompasses purposes such as claim processing, coordination of benefits, and healthcare payment activities, all core functions supported by the PED.

Additionally, the Privacy Impact Assessment (PIA) serves as public notice in compliance with the eGovernment Act of 2002, transparently outlining the types of data collected, the methods of collection, the authorized uses, and the privacy protections implemented. Including this PIA in the agency's public-facing repositories ensures that individuals know how their data may be utilized once transmitted to backend processing systems like PED.

Where applicable, Social Security Numbers (SSNs) are addressed explicitly in privacy notices and authorized under 38 U.S.C. for administering Veterans' benefits and managing records. The collection and subsequent processing of this data through PED is thus consistent with both the individual notice provided and the statutory purpose of the system.

All referenced notices, including the NOPP, SORN listings, and supporting documentation, are available in Appendix A and on the VA Privacy website: https://www.oprm.va.gov/privacy/systems_of_records.aspx.

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.

The Payer Electronic Data Interchange Transactions Application Suite (TAS) does not directly collect information from Veterans, beneficiaries, or members of the public. Instead, the system processes claims and related healthcare data originating from external sources, such as community healthcare providers and clearinghouses, which collect the information on behalf of the VA.

As such, the opportunity to decline providing information is offered at the initial point of collection, typically during enrollment in VA healthcare programs or when receiving care from a VA or community provider. At that time, individuals receive a Notice of Privacy Practices (NOPP), which informs them of their privacy rights, including the option to withhold certain information.

However, individuals should be advised that choosing not to provide specific Personally Identifiable Information (PII), such as Social Security Numbers (SSNs) or other necessary identifiers, may lead to limitations or denial of certain VA services or benefits, as this information is often essential for verifying eligibility, processing claims, and coordinating care.

In summary, while PED does not directly provide the option to decline data provision, the original data collection process accommodates individual rights under the Privacy Act and HIPAA, and any related implications for refusal are addressed at that point of service.

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.

Individuals, including veterans and their beneficiaries, can request restrictions on how the Department of Veterans Affairs (VA) uses or discloses their PII and PHI. These rights are outlined in the VA Notice of Privacy Practices (NOPP) and are governed by the Health Insurance Portability and Accountability Act (HIPAA) and relevant federal regulations under 45 CFR §164.522.

While the initial collection and general use of information for healthcare operations, treatment, and payment are authorized without specific consent, individuals may request further limitations on how their information is utilized or shared. To exercise this right, a Veteran must submit a written request specifying:

- The information to be restricted,
- The specific use or disclosure is to be limited,
- The party or entity to which the restriction applies.

Requests may be submitted at the local VA medical center or by following the procedures outlined in the NOPP. While the VA is not obligated to accept all restrictions, it evaluates each

request and will honor those it approves, especially when mandated by law or under exceptional circumstances.

It is important to note that although Veterans may choose to limit the use or disclosure of their information, such restrictions may impact the VA's ability to process claims, coordinate care, or provide specific services. The NOPP included in Appendix A of this PIA offers complete guidance on individual consent rights and procedures.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that veterans and their beneficiaries may not fully understand that the Payer Electronic Data Interchange Transactions Application Suite (TAS) collects, maintains, and processes their Personally Identifiable Information (PII) and Protected Health Information (PHI) as part of backend claims management. Suppose sufficient notice is not provided during initial data collection or is not easily accessible. In that case, individuals may be unaware of how their data is used or disclosed, which could undermine trust and transparency and potentially lead to perceived or actual misuse of personal information.

Mitigation: To mitigate this risk, the Department of Veterans Affairs provides several layers of notice consistent with the Principle of Transparency. Veterans receive a Notice of Privacy Practices (NOPP) upon enrollment and at the point of service, as required by VHA Handbook 1605.04. This notice outlines how their data will be used for treatment, payment, and healthcare operations, including systems like PED that support claims processing functions.

The Privacy Impact Assessment (PIA) for PED is publicly available in accordance with the eGovernment Act of 2002. It further enhances transparency by detailing how the system collects, uses, shares, and protects PII and PHI. These notices adhere to the Principle of Use Limitation, ensuring that data is utilized solely for disclosed and authorized purposes.

Additionally, the VA Privacy Office retains records of notice distribution to ensure compliance with disclosure requirements. All System of Records Notices (SORNs) related to PED are published in the Federal Register and the VA Privacy Service website. These measures

collectively ensure that individuals are adequately informed, and that the system's use of personal information remains within the stated purpose's scope.

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.***

Individuals have the right to access their personal information maintained by the Department of Veterans Affairs (VA) in accordance with the Privacy Act of 1974, 5 U.S.C. § 552a, and VA regulations under 38 CFR Part 1, Subpart B. Access to information is provided through various established channels, including:

- **Privacy Act and FOIA Requests:** Individuals can submit a request for privacy or the Freedom of Information Act (FOIA) through the VA Public Access Link (PAL) at the VA Public Access Link - Home. This portal enables Veterans and other requesters to submit and track requests for personal data access.
- **VHA Facility Requests**: Veterans may submit written requests to review or obtain a copy of their health information directly to the Privacy Officer at the Veterans Health Administration (VHA) healthcare facility that provided or paid for their care. Contact information for each facility's Privacy Officer is available through local VA medical centers.
- **VHA Notice of Privacy Practices:** Veterans are informed of their rights to access their health information through the VHA's Notice of Privacy Practices, which outlines the procedures for reviewing and obtaining copies of medical records. This notice is provided upon enrollment and is available at all VA medical centers. It can also be accessed online at the VA Notice of Privacy Practices.
- **Records Maintained Outside VHA:** Individuals should contact the National Personnel Records Center at (314) 801-0800 or visit the Veterans' Service Records website for previous military service health records.
- **Customer Support:** Individuals can also contact the VA's customer service representatives or local Records Officers to obtain their records.

According to the Federal Information Privacy Principles (FIPPs), these procedures promote transparency and individual access rights. The relevant System of Records Notices

(SORNs) governing data access include, but are not limited to: 3VA10NB3, 24VA10A7, 54VA10NB3, 58VA21, and 79VA10. All referenced notices are provided in Appendix A of the PIA.

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)?

The PED is subject to the access provisions of the Privacy Act of 1974. However, the system does not collect information directly from individuals. Instead, it receives data from healthcare providers and clearinghouses on behalf of Veterans and beneficiaries.

Individuals whose data resides in VA systems supporting PED have the right to access their records under the Privacy Act. To exercise this right, individuals may submit VHA Form 10-5345, "Request for and Authorization to Release Medical Records or Health Information," to the Privacy Officer at their respective VA medical facility. This process aligns with VA Handbook 1605.1 and ensures individuals can review and obtain copies of their protected health information (PHI) and personally identifiable information (PII).

Currently, this system does not claim any exemptions under the Privacy Act. If any exemptions apply in the future, they will be formally published in the Federal Register and codified in the Code of Federal Regulations (CFR), in accordance with 5 U.S.C. § 552a(j) or (k).

For a complete list of applicable System of Records Notices (SORNs), individuals may refer to Appendix A of this Privacy Impact Assessment (PIA) or visit the VA SORN website.

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?

Although the Payer Electronic Data Interchange Transactions Application Suite (Payer EDI TAS) is not a direct Privacy Act system that collects information from individuals, it supports other VA systems of records that do maintain Personally Identifiable Information (PII) and Protected Health Information (PHI) under the Privacy Act of 1974. Information in Payer EDI TAS comes from industry clearinghouses and healthcare providers and is used by the Department of Veterans Affairs (VA) for claims processing and related administrative functions.

Individuals wishing to access their records can do so through the procedures outlined by the Veterans Health Administration (VHA). Specifically, requests for access to PHI and PII may be submitted by completing VHA Form 10-5345, "Request for and Authorization to Release Medical Records or Health Information," and sending it to the Privacy Officer at the VA medical facility that provided or funded the care.

These procedures are governed by VA Handbook 1605.1, the Privacy Act of 1974 (5 U.S.C. § 552a), and HIPAA Privacy Rule regulations (45 CFR Parts 160 and 164). While Payer EDI TAS does not interface directly with individuals, it is connected to record systems under these legal frameworks.

Appendix A of this Privacy Impact Assessment (PIA) and the VA Privacy Service Systems of Records page provide more information on applicable Systems of Records Notices (SORNs).

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 have the right to request corrections to their health information if they believe it is incomplete, inaccurate, outdated, or unrelated to their care. This right is outlined in all VA medical centers' Notice of Privacy Practices. To initiate a correction, individuals must submit a written request specifying the nature of the amendment and providing supporting rationale to the Privacy Officer at the VA healthcare facility that maintains the relevant records. If the request is denied, the individual will receive written notice of the denial and may respond by filing an appeal, submitting a formal "Statement of Disagreement," or requesting that the original amendment request be included with any future disclosures of the disputed information. Contact information for the appropriate facility's Privacy Officer can be found by visiting the VA's Privacy website at https://www.va.gov/privacy or contacting the VHA healthcare facility directly.

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

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Individuals are informed about procedures for correcting their personal and health information through various channels, including the VA's Notice of Privacy Practices (NOPP), which is distributed at enrollment, available at all VA medical facilities, and accessible online at the VA Privacy Service website. The NOPP clearly outlines the right to request amendments to records and the process for doing so. Additionally, guidance is provided in person at the point of care and through official VA publications such as the CHAMPVA Guide. These notices ensure that Veterans and beneficiaries understand their rights and the means available to maintain the accuracy and integrity of their records.

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.

The PED system does not provide a formal process for individuals to address issues with their personal information. Therefore, if someone wishes to access, correct, or update their personal data, they must contact the original source from which PED collects this information. This approach aligns with standard data collection practices and ensures that any changes are

made at the authoritative level of the source system. The use of personal information within the PED system is governed by the Privacy Act of 1974 (5 USC 552a) and relevant provisions of Title 38 of the United States Code, which outline the principles for managing and protecting personal data. While PED lacks an internal mechanism for making changes directly, individuals are encouraged to collaborate with the source system to ensure their information is accurate and complete.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department's access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. ***For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals involved might change their behavior.*** *(Work with your Privacy Officer (PO) to complete all Privacy Risk questions in this section).*

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

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

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

Follow the format below:

Privacy Risk: Individuals may be unaware of their right to access, review, and request corrections to their PII or PHI, which could lead to outdated or inaccurate data remaining unchallenged in the system. This situation may adversely affect benefit eligibility determinations or care coordination and diminish individual trust in the Department's data stewardship.

Mitigation: The Department of Veterans Affairs mitigates this risk through clear, documented procedures that support individual participation and data accuracy. Individuals are informed of their rights via the VA's Notice of Privacy Practices, which outlines the steps to request access or submit amendments to their records. Correction requests must be submitted in writing to the Privacy Officer at the relevant VHA facility, who reviews and responds in accordance with VA policies and HIPAA guidelines. Individuals receive written justification if a request is denied and may appeal the decision or submit a Statement of Disagreement. These processes ensure transparency, uphold the integrity of the data, and reinforce the VA's commitment to protecting the rights of Veterans and beneficiaries.

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?

VA's access control policies strictly govern access to the PED system, adhering to a role-based, need-to-know authorization model. Only VA employees and contractors who have completed the mandatory privacy and cybersecurity training, including VA Privacy and Information Security Awareness and Rules of Behavior, can request system access.

The access request process consists of the following steps:

1. **Submission of Access Request:** Users must submit a request through the Electronic Permissions Access System (ePAS), specifying the required role and providing justification for access. A designated sponsor or supervisor needs to initiate this request.
2. **Managerial and Security Approval:** The access request is reviewed and approved by the individual's supervisor and the designated Authorizing Official (AO). Approval verifies that access is essential for the user's job responsibilities.
3. **Clearance Verification:** Before system credentials are issued, all users must complete a VA personnel security screening and receive clearance to the appropriate level.
4. **Access Provisioning:** Active Directory (AD) credentials are issued upon approval and clearance. These credentials are set up to enforce read-only, view-only access within the system, in accordance with the user's assigned role.
5. **Role Assignments and Auditability:** User access is restricted by role to reduce data exposure, and roles undergo periodic reviews for compliance. Access logs are kept and monitored to identify any unauthorized activity.

This thorough multi-step process ensures that only personnel who are properly cleared and trained can access the PED, strengthening the VA's commitment to protecting sensitive data.

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?

No external agencies or non-VA personnel are permitted to access the PED system. Access is restricted exclusively to authorized VA employees and contractors who satisfy the established security, privacy, and training requirements.

All criteria for using and potentially sharing PII within the VA are established and governed by the VA's Office of Information and Technology (OIT), in coordination with the Privacy Service and compliance with applicable federal laws, including the Privacy Act of 1974, HIPAA, and VA-specific policies such as VA Handbook 6500.

If data sharing with another federal agency becomes permissible in the future, access would depend on:

- The establishment of a formal inter-agency agreement or Memorandum of Understanding (MOU).
- Role-based access is clearly defined in the agreement.
- Adherence to data minimization principles ensures that only the necessary data elements are shared.
- Oversight by the VA Privacy Officer and Data Governance Board to ensure compliance with all relevant statutory and regulatory obligations.

However, under the current operational configuration, all access to the VA network is internal and regulated by strict internal policies to ensure the integrity and confidentiality of PII and other sensitive information.

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.

Access to the Payer EDI TAS system is strictly role-based and governed by the principle of least privilege, ensuring that users only access the information necessary to fulfill their official responsibilities. The roles are defined in general terms as follows:

- **Read-Only Users**: These individuals, typically business analysts, auditors, or support staff, have restricted access to view data within the system. They cannot modify, delete, or export data and are limited to pre-defined query and report functions necessary for their role.
- **System Administrators** are responsible for system maintenance and configuration. Their access includes managing user accounts, troubleshooting technical issues, and performing system updates. They do not have direct access to sensitive PII or PHI unless required for system operations and explicitly authorized.
- **Data Managers**: These users may have limited write-access privileges to perform specific data correction, validation, or reconciliation functions. Their actions are governed by strict audit logging and require supervisory approval.
- **Information Security Officers (ISOs)**: Tasked with monitoring access control compliance, ISOs have oversight capabilities to audit user activity and ensure alignment with VA security standards.
- **Program Managers and Supervisors**: These roles include review and approval authority for access requests. They ensure that requested access levels align with the user's job responsibilities and maintain compliance with internal governance.

Access requests are initiated and documented through the Electronic Permissions Access System (ePAS). Each request undergoes review and must be approved by the requester's supervisor and validated by the Office of Information and Technology (OIT). This layered approval process ensures proper access control and safeguards the confidentiality and integrity of data within the system.

8.2. Contractor signed Non-Disclosure Agreement (NDA), Business Associate Agreement (BAA) etc. in place.

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.

8.2a Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

Yes, contractors supporting the PED system must sign Non-Disclosure Agreements (NDAs) as a condition of their engagement. These NDAs ensure that all contractors formally acknowledge their responsibility to protect the confidentiality and integrity of any Personally Identifiable Information (PII) or other sensitive data they may encounter during work.

The Office of Community Care (OCC) ensures that all contractors working on OCC-managed projects, including the PED system, have signed NDAs before being granted access. These agreements are kept as part of the contractor's personnel records and are reviewed in accordance with contract renewals or assignment changes.

Contractor access is strictly role-based and limited to functions necessary for fulfilling defined operational or technical support requirements. All access is governed by the principle of least privilege, ensuring that contractors have access only to the data essential for their duties.

By enforcing the NDA requirement and limiting access through structured role assignments, the VA reduces the risk of unauthorized disclosure or misuse of sensitive information by contractor personnel.

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

Yes, VA contractors may be granted access to the PED system and to Personally Identifiable Information (PII), but such access is strictly governed by established VA security and privacy protocols. Contractors are required to sign Non-Disclosure Agreements (NDAs) before any access is granted. These NDAs emphasize the contractor’s legal and ethical responsibility to protect all sensitive information encountered during their duties.

Access is granted only to contractors deemed essential for the system's operation, maintenance, or support. The Contracting Officer Representative (COR) oversees the compliance process, ensuring that each contractor has signed an NDA and meets all contractual and security requirements for system access.

Contractors’ access is role-based and follows the principle of least privilege. Role definitions are set to restrict access based on job function, and system permissions are configured to ensure that contractors can only view or interact with data necessary for their assigned responsibilities. These roles are regularly monitored and reviewed to prevent unauthorized access or privilege creep.

All contractor access must comply with VA policy, including adherence to the requirements outlined in VA Handbook 6500, the Federal Information Security Modernization Act (FISMA), and OMB Memorandum M-17-12. Contractors must also complete annual VA privacy and security training to ensure ongoing awareness of data protection responsibilities.

Through these layered safeguards, contractual, technical, and procedural, the VA mitigates risks associated with contractor access while ensuring operational continuity and compliance with federal privacy regulations.

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

Contractors supporting the Payer EDI TAS system are involved in its design and ongoing maintenance. These individuals fulfill critical roles such as software developers, systems engineers, cybersecurity specialists, and infrastructure support personnel. Their access is strictly limited to the scope needed to perform assigned tasks, and all contractors must sign Non-Disclosure Agreements (NDAs) before accessing the system.

Contractor responsibilities may include designing new system features, applying software patches and updates, ensuring compliance with security configurations, conducting vulnerability scans, and maintaining operational continuity. Each contractor's access is governed by documented privacy roles and responsibilities that enforce role-based access controls (RBAC), limiting permissions to only what is necessary for job performance.

The Contracting Officer Representative (COR) ensures all contractor engagements comply with applicable VA policies, including the Federal Acquisition Regulation (FAR), VA Handbook 6500, and current OMB guidance. All contracts undergo regular reviews as part of VA's acquisition management and oversight processes, with updates made as necessary to reflect system changes or evolving policy requirements.

By closely managing contractor participation and access rights, and ensuring strict oversight and adherence to NDA obligations, the VA reduces risks to Veterans' sensitive data while leveraging contractor expertise to maintain secure and effective system operations.

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 individuals requiring access to the Payer EDI TAS system, including VA employees and contractors, must complete mandatory privacy and security training to handle Personally Identifiable Information (PII) and Protected Health Information (PHI) properly. Before gaining system access, users must review and electronically acknowledge the VA Information Security Rules of Behavior (RoB), affirming their understanding and commitment to safeguarding sensitive data. The VA Talent Management System (TMS) manages and tracks this acknowledgment.

Annual completion of the following core TMS courses is mandatory:

1. **VA 10176** – *VA Privacy and Information Security Awareness and Rules of Behavior*
2. **VA 10203** – *Privacy and HIPAA Training*
3. **VA 3812493** – *Annual Government Ethics Training*

In addition to the foundational training, role-based training is offered according to the user's specific responsibilities within the system. This ensures users know what is relevant to their access levels and duties. Role-based training includes, but is not limited to, the following courses:

- **VA 1016925** – Information Assurance for Software Developers
- **VA 3193** – Information Security for Executives, CIOs, and Senior Leaders
- **VA 1357084** – Role-Based Training for Data Managers
- **VA 64899** – Role-Based Training for IT Project Managers
- **VA 3197** – Role-Based Training for IT Specialists
- **VA 1357083** – Role-Based Training for Network Administrators
- **VA 1357076** – Role-Based Training for System Administrators
- **VA 3867207** – Role-Based Training for System Owners

These training requirements align with VA Handbook 6500 and NIST SP 800-53 Rev. 5 guidelines. The curriculum is designed to reinforce best practices in data protection, raise awareness of evolving cyber threats, and support compliance with federal privacy regulations.

By requiring comprehensive, role-specific training and strengthening accountability through regular reviews and recognition, the VA ensures a workforce fully equipped to handle sensitive information responsibly and securely.

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

8.4a If completed, provide:

1. *The Security Plan Status:* **Approved**
2. *The System Security Plan Status Date:* **October 28, 2024**
3. *The Authorization Status:* **Authorization to Operate (ATO)**
4. *The Authorization Date:* **January 17, 2025**
5. *The Authorization Termination Date:* **January 17, 2027**
6. *The Risk Review Completion Date:* **December 23, 2025**
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* **Moderate**

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

*8.4b If not completed or In Process, provide your **Initial Operating Capability (IOC) date.***

<<ADD ANSWER HERE>>

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)***

VA Enterprise Cloud (VAEC) - Amazon Web Services (AWS)
FedRAMP package #: F1603047866, VA Enterprise Cloud Amazon Web Services GovCloud High.
Yes, the system is FedRAMP approve.

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

The Department of Veterans Affairs (VA) maintains complete ownership and custodial responsibility for all data, including Personally Identifiable Information (PII) and Protected Health Information (PHI), that is processed and stored within the VA Enterprise Cloud (VAEC) hosted on Amazon Web Services (AWS) GovCloud. This ownership is established in the contractual agreements between VA and AWS, ensuring that all data remains under VA control and is managed according to federal privacy regulations and VA policies.

The contractual framework aligns with the National Institute of Standards and Technology (NIST) Special Publication 800-144, which emphasizes that federal agencies are ultimately accountable for the security and privacy of data held by cloud service providers on their behalf. Therefore, the VA is responsible for implementing and maintaining appropriate security and privacy controls for all data within the VAEC-AWS environment.

FedRAMP package number F1603047866 identifies the specific contract governing this arrangement, which pertains to the VA Enterprise Cloud Amazon Web Services GovCloud High authorization. This contract outlines the roles and responsibilities of both VA and AWS, ensuring compliance with relevant laws, regulations, and data ownership and protection standards.

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.

Ancillary Data Collection:

In alignment with NIST Special Publication 800-144, cloud service providers (CSPs) like Amazon Web Services (AWS) may collect ancillary data while operating their cloud services. This ancillary data consists of metadata such as system logs, audit trails, and usage metrics, which are crucial for service monitoring, billing, and ensuring the security and performance of the cloud environment.

Ownership of Ancillary Data:

The Department of Veterans Affairs (VA) retains full ownership and custodial responsibility for all data, including any ancillary data generated within the VA Enterprise Cloud (VAEC) hosted on AWS GovCloud. This ownership is explicitly defined in the contractual agreements between the VA and AWS, ensuring that all data remains under VA control and is managed in compliance with federal privacy regulations and VA policies.

The contractual framework aligns with the National Institute of Standards and Technology (NIST) Special Publication 800-144, which emphasizes that federal agencies are ultimately accountable for the security and privacy of data held by cloud service providers on their behalf. Consequently, the VA is responsible for implementing and maintaining appropriate security and privacy controls for all data within the VAEC-AWS environment.

FedRAMP package number F1603047866 identifies the specific contract governing this arrangement, which pertains to the VA Enterprise Cloud Amazon Web Services GovCloud High authorization. This contract clearly outlines the roles and responsibilities of both the VA and AWS, ensuring compliance with applicable laws, regulations, and data ownership and protection standards.

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.

Contractual Framework and Data Ownership:

The VA's contractual arrangements with AWS, identified by FedRAMP package number F1603047866, clearly establish the VA as the sole owner of all data, including Personally Identifiable Information (PII) and Protected Health Information (PHI), stored within the VAEC environment. These contracts outline the responsibilities of both parties, ensuring that AWS delivers the necessary infrastructure and security controls. Meanwhile, the VA maintains full authority over data governance and compliance with federal privacy regulations.

Roles and Responsibilities:

- **VA Responsibilities:**
  - Implement and manage application-level security controls.
  - Ensure compliance with federal data protection laws and VA policies.
  - Oversee data governance, including access controls and incident response.
- **AWS Responsibilities:**
  - Maintain physical and environmental security of the cloud infrastructure.
  - Provide secure network and storage services in accordance with FedRAMP High baseline requirements.
  - Support the VA in meeting its compliance obligations through shared responsibility models.

This division of responsibilities ensures that, while AWS manages the underlying infrastructure, the VA retains control over data usage, access, and compliance. This approach adheres to the accountability principle outlined in NIST 800-144.

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

Robotic Process Automation is the use of software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. For example, will the automation move or touch PII/PHI information. RPA may also be referred to as "Bots" or Artificial Intelligence (AI).

The PED system does not use Robotic Process Automation (RPA), including bots or Artificial Intelligence (AI), to process or manage data. All system functions and data interactions are carried out through controlled, human-initiated operations. Therefore, no automated scripts or processes exist that access, move, or manipulate PII or PHI.

This ensures that all sensitive data handling stays within the scope of human oversight and aligns with existing VA data governance policies and privacy safeguards. If RPA capabilities are considered for future system enhancements, a thorough privacy impact assessment and policy review will be conducted according to VA standards and NIST guidelines.

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.

ELLER PAMINTUAN

Digitally signed by ELLER PAMINTUAN
Date: 2025.06.05 10:43:13 -06'00'

Privacy Officer, Eller Pamintuan

PAUL BARTHOLOMEW

Digitally signed by PAUL BARTHOLOMEW
Date: 2025.06.05 11:53:37 -05'00'

Information System Security Officer, Paul Bartholomew

DENA LISTON

Digitally signed by DENA LISTON
Date: 2025.06.09 11:05:41 -04'00'

Information System 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; screen shot of a website collection privacy notice).

Veterans Health Administration NOTICE OF PRIVACY PRACTICES Effective Date: September 30, 2013. For further details, please visit: https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946.

1. 23VA10NB3, Non-VA Care (Fee) Records -VA (7/30/2015), 2015-18646.pdf (govinfo.gov)
2. 24VA10A7, Patient Medical Records -VA (10/2/2020), 2020-21426.pdf (govinfo.gov)
3. 54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry, and Payment Files -VA (3/3/2015), 2015-04312.pdf (govinfo.gov)
4. 58VA21, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records -VA (11/8/2021), 2021-24372 (govinfo.gov)
5. 79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records –VA (12/23/2020), 2020-28340 (govinfo.gov)
6. Title 38, United States Code, Section 7301(a).

HELPFUL LINKS:

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 Notice of Privacy Practices
VHA Handbook 1605.04: Notice of Privacy Practices