Privacy Impact Assessment for the VA IT System called:

VCIP Source Material Tracking

(VCIP SMTS)

VBA

VBA-Office of Business Integration OBI

eMASS I.D.#: 1313

Date PIA submitted for review:

10/16/2024

System Contacts:

System Contacts

Role	Name	E-mail	Phone Number
Privacy Officer	Marvis Harvey	marvis.harvey@va.gov	(202) 461-8401
Information System Security Officer (ISSO)	Richard Alomar-Loubriel	Richard.Alomar-Loubriel@va.gov	787.696.4091
Information System Owner	John Clark	John.Clark7@va.gov	708.483.5575

Abstract

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

The VCIP Source Material Tracking System (VCIP SMTS) allows users to manage, locate, track, update and report on paper mail artifacts undergoing conversion (digitization, routing and upload) to the Veteran Benefits Management System (VBMS) or Digital Mail Handling System (DMHS) in support of the Veterans Benefit Administrations (VBA) eligibility determination processes. The system is a managed service platform hosted by the vendor on AWS GovCloud (outside of the VAEC) and integrated with the vendor's on-premises document scanning and processing facility. SMTS supports paper mail handlers and support staff as well as VA personnel and their approved representatives. VCIP SMTS was rolled out in 2020. In 2022, VCIP SMTS was extended to include the public, front-facing QuickSubmit capability. To reduce the need to physically transmit and scan paper documents, QuickSubmit allows Veterans, veteran family members, VA employees, and veteran business partners—including Veteran Service Organizations (VSOs), attorneys, and other Veterans' representatives—to directly upload electronic claims and claims-related documents.

Overview

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

1 General Description

A. What is the IT system name and the name of the program office that owns the IT system?

The system name "Veterans Claim Intake Program Source Material Tracking System" (VCIP SMTS) is owned by the Veterans Claims Intake Processing organization of the Veterans Benefit Administration (VBA).

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

VCIP SMTS allows users to manage, locate, track, update and report on Paper Mail artifacts undergoing digital conversion routing and upload to designated Veterans Affairs Administration (VA) downstream systems in support of the VBA's eligibility determination processes.

C. *Who is the owner or control of the IT system or project?*

The system is developed, maintained, and hosted by vendor GovernmentCIO (GovCIO) and used by paper mail handlers and support staff and VA personnel and their approved representatives. To fulfill its source material tracking objective, VCIP SMTS collects one or more of the following fields: Name, Address, Date of Birth, Document Control Number, Participate number and Unique Identifier.

2. Information Collection and Sharing

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

VCIP SMTS will receive and store primary the VA unique identifier file number for tracking mail related to a Veteran. Note that for many Veterans the Veteran File Number matches their Social Security numbers. VCIP SMTS is able to track all data within the system by using the unique identifier file number (all data is stored in an encrypted data repository). Data is managed in accordance with the Health Insurance Portability and Accountability Act (HIPAA) requirements for tracking PII/PHI
information within the Source Mailing Tracking System.

The non-sensitive data element that will be transmitted will be a Universal Unique Identifier linked to existing Veteran Claim documents that were not able to be processed by the VA due to missing Veteran information (the Universal Unique Identifier is tied to a Veteran claim package that is not able to be verified with a Veteran or a Veteran ID Number.

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

The public-facing QuickSubmit intake user interface collects one or more of the following fields: Name, Address, Email Address, Phone number (for SMS/text notification only) and Veteran File Number.

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

VCIP SMTS is hosted in AWS FedRAMP compliant (Non-VAEC) AWS GovCloud and inherits associated FedRAMP security controls.

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

External access to the system is controlled via (and in compliance with) VA's designated single sign on (SSO) interface, which facilitates two factor authentications. Internal factory users of the system access via local two factor authentication within the factory firewalls.

3. Legal Authority and SORN

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

The authorization for operation of VCIP is VA Contract No. VA118-16-D-1003 Purchase Order 36C10B20N1003008, with Federal authorization to collect information under: "Title 38, U.S.C. Chapter 3, Section 210 (c) (1), Title 38 U.S.C. 7301, 5 U.S.C. 552a.and Executive order 9397.

The Table below identifies the SORNS that align with VCIP-SMTS business purpose.

SORN Number	SORN Title	SORN Link
54VA10NB3 / 80 FR 11527	Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files-VA	https://www.govinfo.gov/content/pkg/FR-2015-03-03/pdf/2015-04312.pdf
58VA21/22/28 / 86 FR 61858	Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA	https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf
147VA10 / 86 FR 46090	Enrollment and Eligibility Records-VA	https://www.govinfo.gov/content/pkg/FR-2021-08-17/pdf/2021-17528.pdf
192VA30/88 FR 72820	Veterans Affairs Profile-VA	https://www.govinfo.gov/content/pkg/FR-2023-10-23/pdf/2023-23327.pdf
08VA05 / 88 FR 4885	Employee Medical File System Records (Title 38)-VA	https://www.govinfo.gov/content/pkg/FR-2023-01-25/pdf/2023-01438.pdf

I. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?
Yes, the SORNs in the table above covers the systems to which VCIP-SMTS connect and operates with Veteran Data collection, processing, and is the same as the AWS FedRAMP High gov cloud storage, data management, data retrieval/archive and access referenced in 192VA30/88 FR 72820.

1. *will the SORN require amendment or revision and approval?*

No

4. System Changes

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

No

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

No

Section 1. Characterization of the Information

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

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

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

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

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
- ☒ Social Security Number
- ☒ Date of Birth
- ☐ Mother's Maiden Name
- ☒ Personal Mailing Address
- ☒ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☒ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☐ Financial Information
- ☐ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers[1]
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☐ Medications
- ☐ Medical Records
- ☐ Race/Ethnicity

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

☐ Tax Identification Number
☐ Medical Record Number
☐ Gender
☒ Integrated Control Number (ICN)

☐Military History/Service Connection
☐ Next of Kin
☒ Other Data Elements (list below)
- Document Control Number
- Participant number,

Other PII/PHI data elements: <<Add Additional Information Collected but Not Listed Above Here (For Example, A Personal Phone Number That Is Used as A Business Number)>>

PII Mapping of Components (Servers/Database)

VCIP Source Material Tracking System (VCIP SMTS) consists of **two** 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 **VCIP Source Material Tracking System (VCIP SMTS)** 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 3.9 in the PTA should be used to answer this question.

Internal Components Table

Components of the information system (servers) collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
VCIP SMTS	Yes	Yes	Name, SSN, DOB, phone number, email, Document Control Number, Participant number, Veteran File Numbers (Social Security Number), Integration Control Number (ICN)	VCIP SMTS will be able to track all data within the system by using the unique identifier file number (stored in a secure encrypted data repository).	Personal Identity Verification (PIV) controlled access / two factor authentication for users authorizing for VA personnel to gain access. VA IAM also allows use of ID.me and login.gov Credential Service

					providers (MFA also required).
QuickSubmit	Yes	Yes	Name, SSN, DOB, phone number (SMS Texts), email, Document Control Number, Participant number, Veteran File Numbers (Social Security Number), Integration Control Number (ICN)	Identifiers are required for intake of claims when we send them to PMCMS DMHS and VBMS.	Same as above.
Claim Evidence	Yes	Yes	Name, Address, Social Security Numbers (including Social Security Number), Email Address, SMS (text) phone numbers. ICN File Numbers	Identifiers are required for intake of claims when we send them to PMCMS DMHS and VBMS., the use of Unique Identifiers anonymizes the unverified packet from the veteran	Same as above
Printing of Unidentified Records	Yes	Yes	Name, Address, Social Security Numbers (including Social Security Number), Email Address, SMS (text) phone numbers. ICN File Numbers Universal Unique Identifier (UUID)	The Identifiers are required to validate the veteran and the claim package or generate the UUID when unidentified and printed as a mail pack back to the submitter.	Same as above

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

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

In support of VCIP SMTS primary mission of making Veteran's information gathering and processing more efficient and timelier, Team GovCIO receives source materials directly from the Post Office, mail couriers (e.g. United Parcel Service), VBA Regional Offices (Ros), Veterans Service Organizations (VSOs) and third parties providing evidence in support of a claim.

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.

In addition to VCIP SMTS paper mail intake, the VCIP SMTS QuickSubmit frontend allows Veterans, Veteran family members, VA employees, and Veteran business partners—including Veteran Service Organizations (VSOs), attorneys, and other Veterans' representatives—to directly upload electronic claims and claims-related documents.

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

Claims processing and Claims status reports for performance metrics

1.3 How is the information collected?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

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

Paper Mail artifacts come into the vendor factory from the Post Office, United Parcel Service and other mail couriers designated and engaged by the VA. The factory intakes that mail and the VCIP SMTS is provided tracking information from the factory's internal data systems via a secure Virtual Private Network (VPN) connection as mail goes through the factory conversion process.

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?

There are many forms and mail processing automation that is part of the Digital upload for Veteran Claim Processing.

1.4 How will the information be checked for accuracy? How often will it be checked?

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

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

Information is collected in VCIP SMTS to track and report on the intake, processing, rescanning and delivery of artifacts submitted to Team GovCIO under the terms of the Veterans Intake, Conversion, and Communications Services (VICCS) Veterans Benefits Administration (VBA) Mail Management Services (MMS) contract. It is also needed to transmit claims to both DMHS and VBMS, and to track the status of the claims and related artifacts as they are being processed by DMHS and VBMS.

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?

SMTS has built-in field validation and Team GovCIO's Quality Team performs regular sampling audits of the system by reviewing reports. The VA also has independent auditors contracted and their personnel are stationed onsite at the Team GovCIO processing factory. The six personnel perform regular and ongoing audits of all materials processed by our factory systems and provide regular reports to the VA Contracting Officer Representative (COR) and Program Manager (PM) for the MMS contract. Finally, VCIP Administrators are the administrators of the VCIP SMTS application and review the system's accuracy on an ongoing basis via canned reports and ad hoc queries.

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

The authorization for operation of VCIP is VA Contract No. VA118-16-D-1003 Purchase Order 36C10B20N1003008, with Federal authorization to collect information under: "Title 38, U.S.C. Chapter 3, Section 210 (c) (1), Title 38 U.S.C. 7301, 5 U.S.C. 552a.and Executive order 9397."

SORN Number	SORN Title	SORN Link

54VA10NB3 / 80 FR 11527	Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files-VA	https://www.govinfo.gov/content/pkg/FR-2015-03-03/pdf/2015-04312.pdf
58VA21/22/28 / 86 FR 61858	Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA	https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf
147VA10 / 86 FR 46090	Enrollment and Eligibility Records-VA	https://www.govinfo.gov/content/pkg/FR-2021-08-17/pdf/2021-17528.pdf
192VA30/88 FR 72820	Veterans Affairs Profile-VA	https://www.govinfo.gov/content/pkg/FR-2023-10-23/pdf/2023-23327.pdf
08VA05 / 88 FR 4885	Employee Medical File System Records (Title 38)-VA	https://www.govinfo.gov/content/pkg/FR-2023-01-25/pdf/2023-01438.pdf

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

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?

This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

Privacy Risk: There is risk that the information may be accessed by unauthorized individual

Mitigation: PIV access is utilized VCIP SMTS uses the latest encryption and integrity algorithms for all point of communication to ensure the privacy of the PII data (such as AES256, SHA1, SHA2- 256, ikev1 and ikev2), and is, under this contract, enhancing security with the implementation of the VA's Single Sign On capability which enforces multifactor authentication.

Section 2. Uses of the Information

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

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

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

PII/PHI Data Element	Internal Use	External Use
Name	File Identification purposes	Not used
Document Control Number	File Identification purposes	Not used
Social Security Number	Personal Information Verification	Not used
Date of Birth	Personal Information verification	Not used
Personal phone number	Personal Information verification	Used for SMS notifications OPT IN only
Personal email	Personal Information verification	Not used
Integrated Control Number	personal identifier and records ID	Not used

Since 2020, the VA's VBA organization has used the SMTS system to track materials that have been provided to Team GovCIO for conversion and rescans so that they can better understand where veteran records are in the conversion

process. Reports in VCIP SMTS allow VCIP SMTS users, supervisors and VCIP Administrators to what elements of the veteran record have been processed and delivered to downstream VA systems. As of 2023, the QuickSubmit frontend intake application's user base is mostly Veterans and Veteran Service Organizations (VSOs) who directly upload claims and claims-related documents. This direct user experience supports VBA's mission to serve more Veterans with a faster turnaround time than with traditional paper.

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

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

The data stored in VCIP SMTS is limited to the information necessary to track artifacts that have been processed under the MMS contract. The VCIP SMTS users can track artifacts that are converted from analog to digital, structured data and they are able to view reports indicating the time taken to process provided artifacts from the point of intake to the point of delivery to downstream VA applications. VCIP tooling is oriented to determine the efficiency of the Team GovCIO factory processes for conversion.

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 information for veterans is maintained with in the veteran's profile so the system will redirect the veteran to their profile system using the veteran's login within the current session via an IFCAMP OIDC compliant authorization to update their record and provide a SMS notification with email confirmation.

2.3 How is the information in the system secured?
These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

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

All data collected, processed, transmitted, and stored in VCIP SMTS is treated as Sensitive. The AWS Gov Cloud provides Relational Database Services RDS with encrypted data backend and encrypted storage files. The hosts use SSL/TLS certificates via VA Venafy certificate management tied to the domain for trusted, and encrypted transmission between the VCIP-SMTS Cloud and VA services.

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

The Use of Unique Identifiers verses SSNs is in place, there are reports and audits with automated notifications when data mismatch is identified as in a user has more than one UID as there can be only one UID. When these happen the VCIP-SMTS Administration engages the IAM team and facilitates conversations with the appropriate Identity management entity Id.ME, Login.gov, to assist the user in realigning their account information. Once the veteran's account is properly configured, and the identity verified the queued package is reconfigured and restarted under the proper identity to prevent any loss of transaction data.

All Data is encrypted at rest and in transit following NIST 800-53, VA NARA and data protections. FIPS 140-2 and FIPS140-3 compliant modules. FIPS 140-3 certificate number of GovCIO, LLC's cryptographic module for connecting to the VA Business Partner Extranet (Connection ID #314) is FIPS #4631. FIPS compliance will be validated by VA.

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

The vendor team runs regular scans required by the VA and the reports are both reviewed internally and provided to government oversight teams for review. POAMs are executed to track and resolve findings in compliance with the MMS contract.

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?

All persons associated with operating the system receive training (initial, annual refresher and ad hoc) on Privacy Act, Health Insurance Portability and Accountability Act (HIPAA), system data security and VA Rules of Behavior (ROB). The VCIP SMTS access control system includes role-based access control (RBAC) based on the following:

- SSO multi-factor authentication for factory system operators.
- SSO multi-factor authentication for VA employees, contractors and designated operators.
- SSO multi-factor authentication for Veterans, Veteran Family Members, and VA Business Partners (including Veteran Service Organizations).
- Authorization for Basic User Access.
- Authorization for Quality Assurance Access.
- Authorization for Supervisor Access.
- Authorization for VCIP Administrator Access.
- Authorization for System Administration Access.

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

The vendor team runs regular scans required by the VA and the reports are both reviewed internally and provided to government oversight teams for review. POAMs are executed to track and resolve findings in compliance with the MMS contract.

2.4c Does access require manager approval?

yes

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

User requests are reviewed and approved by both supervisors and administrators in the User Account Management module of VCIP. All account management actions are logged. All access to and update of records is logged. The vendor team,

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

VA Supervisors and VCIP Administrators are all responsible for reviewing access to and use of VCIP SMTS.

Roles	Responsibilities

Director/Chief Executive Officer (CEO)	» Ensure the Standard Operating Procedures set forth in this document are followed by the individuals under their responsibility. » Allocate sufficient resources (budget, staff, etc.) to implement and operate the system-wide privacy program.
Information System Owner (ISO)	» Work with the Information System Security Officer (ISSO) and Privacy Officer (PO) to complete the annual Privacy Threshold Analysis (PTA) and the Privacy Impact Assessment (PIA). » Work with information owners and Director of Records Management to publish initial System of Records Notices (SORN) and update all System of Records Notices as dictated by law or VA policy. » Assure that all proper measures are taken to ensure confidentiality of PII on all systems for which they are responsible. » Identify Databases that contain PII/PHI. » Maintain/Secure data and hardware to include Litigation Holds.
Information System Security Officer (ISSO)	» Review the Contract Security Checklist 6500.6 along with the Statement of Work (SOW)/Performance Work Statement (PWS). If PII/PHI will be involved in the contract, the ISSO will provide the security language that should be added to the contract. » Work with the Privacy Officer and System Owner to complete the annual Privacy Threshold Analysis (PTA) and the Privacy Impact Assessment (PIA). » Verifies the site sanitization process and disposition program complies with VA policy annually and maintains the audit documentation. » Review the Governance, Risk and Compliance (GRC) tool for control completeness, evidence is uploaded, and Plan of Action and Milestones (POA&M) are created for non-compliance. » Reports/Documents incidents involving compromise or loss of data in accordance with the GOVCIO VCIP-SMTS Security team, Follows the procedures outlined in the IRP, IR SOP and align with VA Security Operations (VSO) Incident Response Training and Testing SOP. » Ensure that the data is secured for transit.

Privacy Officer (PO)/ Freedom of Information Act (FOIA) Officer	» Provide guidance to staff regarding the use/disclosure of PII/PHI as needed. » Determine when human data can be released to an affiliate institution or other entity. » Work with the ISSO, and System Owner to complete the annual Privacy Threshold Analysis (PTA) and the Privacy Impact Assessment (PIA). » Conduct Privacy and Heath Insurance Portability and Accountability Act of 1996 (HIPAA) training for the New Employee Orientation (NEO) and will monitor Talent Management System (TMS) for Privacy and HIPAA training compliance annually. » Audit the Accounting of Disclosures (AOD) on a quarterly basis. » Responds to Accounting of Disclosure (AOD)/Release of Information (ROI)/ Freedom of Information Act (FOIA) requests. » Review the Contract Security Checklist 6500.6 along with the Statement of Work (SOW)/Performance Work Statement (PWS). If PII/PHI will be involved in the contract, the PO will provide the privacy language that should be added to the contract and will determine if a Business Associate Agreement (BAA) is required. » Conduct reviews of contracts and equipment purchases to identify new or renewal of systems/services that may utilize System owned data. » Engages with VA Privacy Services, in OMB Federal Privacy Council activities and listservs in order to monitor changes in federal privacy laws and OMB guidance affecting privacy requirements. » Reports/Documents incidents involving compromise or loss of data in accordance with the VA Security Operations (VSO) Incident Response Training and Testing SOP. » Collaborate with local Record Officers or Records Liaison Officers to implement processes to facilitate proper retention and disposal of records. » Respond appropriately to all privacy complaints under their purview of responsibility as stipulated in Directive 6502, VA Enterprise Privacy Program.
Department Head / Supervisors	» Assign Functional Category to users and review annually

	» Assure users complete the privacy training annually

Section 3. Retention of Information

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

3.1 What information is retained?

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

The Data elements Retained are:

Name, SSN, DOB, phone number, email for internal system use.

During the first 120 calendar days following the initiation of Mail Management Services operations, or until directed otherwise by the Government, the Contractor shall retain paper mail for 60 calendar days following confirmation of successful upload to a Government image repository. Storage of source materials beyond the required 60 calendar days shall be at the Contractor's expense. At the conclusion of the required 60 calendar day retention period, the Contractor shall ship source materials to VA's Records Management Services vendor in accordance with After the required retention period in the Post-Conversion Retention, the Contractor shall ship paper mail materials to the Government's Records Management Services Vendor for storage awaiting disposition unless otherwise defined in the DCRs.

3.2 How long is information retained?

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

- Seven years unless otherwise specified by the VBA.
- VCIP SMTS Scanning Facility: 90 days. The SOR for claims is VBMS eFolders, so scanning facility purges temp images after 90 days.

- VCIP SMTS QuickSubmit: “indefinite” as specified by the VBA in the Business Requirement Document (BRD) for QuickSubmit.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)?

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

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

The system data retention schedule is in accordance with the Department of Veterans Affairs Records Control Schedule 10-1 [https://vaww.va.gov/vhapublications/rcs10/rcs10-1.pdf] specified and compliant with the base contract, and any changes specified in the Interconnection Security Agreement (ISA)/Memorandum of Understanding (MOU). Information contained in the system is restricted to minimum required to meet system objectives.

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

See Veterans Affairs Records Control Schedule 10-1 Chapter 6- Healthcare Records for details on type series, and disposition authority related to Veteran Claims processing and Source Material Tracking Services. [https://vaww.va.gov/vhapublications/rcs10/rcs10-1.pdf]

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

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

No Veteran’s records are destroyed by the VCIP SMTS system. Factory systems data is flushed every 90 days on a rolling basis as de-prepared mail packets are assembled and shipped to long term storage (LTS) per contract requirements. In the event the Government directed Team GovCIO to destroy paper mail artifacts, the artifacts would be destroyed in accordance with the requirements of NIST SP 800-88, Media Sanitization.” system.

The raw (unofficial) electronic documents uploaded through the VCIP SMTS

QuickSubmit frontend are kept indefinitely in encrypted AWS S3 buckets. After 90 days they transition in-place from standard to archive class, but the infrequently accessed archives are still available instantly, per VBA customer requirements in the Business Requirements Document (BRD). The official copies of claims are maintained downstream in VBMS.

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.

Not applicable no live data for PII/PHI will be used for testing, training, and research.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

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

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

Follow the format below:

Privacy Risk: VCIP SMTS is not a system of record for Veteran claims. Data sent and held by VCIP SMTS is sent to VBMS, where the official copy of the claims are kept; however, per VBA customer retention requirements in the Business Requirements Document (BRD) for QuickSubmit, the raw unofficial electronic copies of documents are to be retained indefinitely. The artifacts sent to the system's scanning facility (Data Dimensions) will be retained for the required

time for the Privacy Act.

Mitigation: Veteran PII/SPI is encrypted during transmission and storage. Data is only retained in compliance with the MMS contract requirements and is purged programmatically when retention period is reached. Factory systems data is flushed every 90 days on a rolling basis as de-prepared mail packets are assembled and shipped to long term storage (LTS) per contract requirements. Only authorized and trained personnel can access VCIP SMTS.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared / received with the specified program office or IT system***	***List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT system***	***Describe the method of transmittal***

MOU ISA Component 1 - VA Master Patient Index (MPI): Master Person Index (aka Master Patient Index) is the VA Enterprise service for Veteran and user identity traits. VA IAM identity traits come from MPI, but MPI also has APIs that can be directly called by applications.	For VCIP SMTS's QuickSubmit feature: to send users SMS/text notification when an upload packet status is "complete". We use MPI in order to match a user more accurately than just IAM alone—also helps avoid use of SSN, also helps us match to Veteran's communication settings in VA Profile.	**First Name, Middle Name, Last Name, VA Profile ID,** and **Participant Id**. (VA Profile Id and Veteran identifier and disambiguates Veteran identifier data	HTTPS 443 over VA BPE (Extranet). VA Site Code 0496: CID 311 (production), CID 312 (staging), CID 313 (dev). The tunnel encrypts REST API calls to MPI.
MOU ISA Component 2 – *VA Profile*: VA Enterprise service for Veteran contact information and communication preferences.	For VCIP SMTS's QuickSubmit feature: to send users SMS/text notification when an upload packet status is "complete". VA Profile allows us to centrally manage the communication settings rather than storing the settings locally.	We read/write a user's centralized Email Address and Phone Number so that they can be used by the VA Notify service. We also allow the user to directly opt in or out of our communication channel, which is a way to enable/disable email/phone notifications.	HTTPS 443 over VA BPE (Extranet). VA Site Code 0496: CID 311 (production), CID 312 (staging), CID 313 (dev). The tunnel encrypts REST API calls to VA profile.
MOU ISA Component 3 – *VA Notify*: VA Enterprise API service for sending email and text.	For VCIP SMTS's QuickSubmit feature: to send users email notifications such as receipt of upload or upload status (success, failure).	We read/write/use Email Address to manage and send email receipts and notifications. We read/write/use Phone Number to manage and send text notifications.	HTTPS 443 over VA BPE (Extranet). VA Site Code 0496: CID 311 (production), CID 312 (staging), CID 313 (dev). The tunnel encrypts REST API calls to VA Notify
MOU ISA Component 5 Claims Evidence / *VA Enterprise File Storage: Veteran Enterprise File Storage is a replacement for the legacy eFolder Web Service and user interface*	extracts the logical elements of the legacy service and restructures them as a standalone application for use both in updated Veterans Benefit Management System capabilities as well as new capabilities requiring access to files providing evidence for claims.	Non-sensitive data will be transmitted. Success/fail notifications with transaction ID IDs (which is a universally unique identifier specific to the problem/action and not to an individual) will be transmitted.	HTTPS 443 over VA BPE (Extranet). VA Site Code 0496: CID 311 (production), CID 312 (staging), CID 313 (dev). The tunnel encrypts REST API calls to the VBMS and Enterprise File Storage Service

MOU ISA Component 6 Printing of Unidentified Records: The Printing of Unidentified Records (PUR) application exists to help reconcile Veteran mail that is unable to be associated with a specific Veteran	Ingest Veteran Physical and Digital Mail claims packets the print and mail out new mail packets, and provides functionality that reunites these mail packets to the Veteran's Veteran Benefit Management System's eFolder where enough information exists to do so	Non sensitive Data will be transmitted	HTTPS 443 over VA BPE (Extranet). VA Site Code 0496: CID 311 (production), CID 312 (staging), CID 313 (dev). The tunnel encrypts REST API calls to VA Printing of Unidentified Records

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: Users of VCIP SMTS could share their screens or reports that are exported from the web application.

Mitigation: All VA employees and contractor are required to complete training for managing PI/PII/SPI in the course of performing their jobs. The VCIP SMTS System also logs access to the application and additionally logs updates and deletes and report downloads to allow VCIP SMTS Administrators to monitor access and use of VCIP SMTS. In the QuickSubmit data entry user interface, Veteran File Numbers (which may be SSNs) are hidden until the field is in focus, actively needed for read or edit.

Section 5. External Sharing/Receiving and Disclosure

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

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

Is the sharing of information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal

mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.

NOTE: Question 3.10 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 External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
N/A				

Privacy Risk: Veterans Claim Intake Processing - Source Material Tracking System does not share any data that is being held in the system. Therefore, no
privacy risks are associated with sharing information outside of the VA.

Mitigation: There is no information being shared externally and no privacy risks associated with data sharing; therefore, the mitigation strategy is not applicable.

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: N/A No information is being shared. VCIP SMTS will request authority to proceed PIV confirmation through SAML transmitted through the Application Program Interface (API) There is a small risk that information may be shared with an external organization or agency.

Mitigation: N/A Safeguards are implemented to ensure data is not shared with unauthorized organizations, including employee security and privacy training, and required reporting of suspicious activity. Personal Identification Verification (PIV) cards are required to gain access. All measures that are utilized for the system. Interconnection Security Agreement (ISA) and Memorandum of Understanding (MOU) are kept current and monitored closely to ensure protection of information.

Section 6. Notice

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

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

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

6.1a This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

Notice is provided by VBA-Compensation, Pension, Education, and Vocational Rehab and Employment Records. VBA Systems of Records Notice (SORN) # 58VA21, 58VA22, and 58VA28
Please see Appendix A 6.1 Privacy Statement

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

N/A

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

VBA Systems of Records Notice (SORN) # 58VA21, 58VA22, and 58VA28

https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

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.

Veterans have the right to refuse to disclose their SSNs to VBA. The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VBA an SSN (please refer to the 38 Code of Federal

Regulations CFR 1.575(a)).

Because we use VA IAM to identify users, when Veterans log into the system their Veteran File Numbers are already known by the system (these are often the same as SSN).

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.

All requests must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VBA address outlined within the SORN.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

Principle of Transparency: Has sufficient notice been provided to the individual?

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

Privacy Risk: Originally N/A. VCIP SMTS dealt with the status of the package during the digitization and archiving process, but not end users (not Veterans or the general public). The data is not meant for public consumption.

Mitigation:
The current notices are displayed to the end users:
1. VCIP SMTS: "WARNING: This U.S government system is intended to be used by [authorized VA network users] for viewing and retrieving information only, except as otherwise explicitly authorized. VA information resides on and transmits through computer systems and networks funded by VA. All use is considered to be with an understanding and acceptance that there is no reasonable expectation of privacy for any data or transmissions on Government intranet or Extranet (non-public) networks or systems. All transactions that occur on this system and all data transmitted through this system are subject to review and action including (but not limited to) monitoring,

recording, retrieving, copying, auditing, inspecting, investigating, restricting access, blocking, tracking, disclosing to authorized personnel, or any other authorized actions by all authorized VA and law enforcement personnel. All use of this system constitutes understanding and unconditional acceptance of these terms. Unauthorized attempts or acts to either (1) access, upload, change, or delete information on this system, (2) modify this system, (3) deny access to this system, or (4) accrue resources for unauthorized use on this system are strictly prohibited. Such attempts or acts are subject to action that may result in criminal, civil, or administrative penalties."

2. VCIP SMTS QuickSubmit: during the Single Sign On process, all users are presented with AccessVA's Privacy and FOIA links (https://department.va.gov/privacy/ and https://department.va.gov/foia/)

VCIP SMTS was originally not a public facing application; however, the QuickSubmit frontend feature may need a display a Limited Privacy Policy notice in a future release, since end users may want to know what PII the application is using.

Section 7. Access, Redress, and Correction

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

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

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

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. ***For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.***

Veterans may request access to Privacy Act records maintained by requesting a copy in writing. All requests to review must be received by direct mail, fax, in person, or by mail referral from another agency or VA office. All requests for access must be delivered to and reviewed by the System Manager for the concerned VBA system of records, the facility Privacy Officer, or their designee. Each request must be date stamped and reviewed to determine whether the request for access should be granted.

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)?

N/A

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?

N/A

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.

Veterans have the right to amend their records by submitting their request in writing. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VBA that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager or designee for the concerned VBA system of records, and the facility Privacy Officer or designee, and needs to be date stamped; and filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579.

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.

No direct feedback from Veterans. All information collect was given by Veteran. The Veterans provide their information directly either by mail, or a form they will submit their information in a paper form and will be digital conversion routing and upload to designated Veterans Affairs Administration (VA) downstream systems in support of the VBA's eligibility determination processes. This process is done prior to VCIP SMTS receiving the digitalized record. SMTS will not correct any information received digitally, so VCIP SMTS would not be aware if the information received is being inaccurate information.

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.

Formal redress is provided. All information correction must be taken via the Amendment process.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that the paper mail that is received and undergoes conversion under the MMS contract will enter provided information and that it will be incorrect and there is the risk that the provided data is correct but incorrectly transposed into VCIP SMTS.

Mitigation: The data entered into the source tracking system is a subset of the data processed for delivery to VA downstream systems. When the affected source material is entered into the Veterans Benefits Management System (VBMS) and associated with a Veterans case(s), the team will be able to correct incorrect data.

Additionally, the Team GovCIO factory has extensive controls and processes in place to track and audit the processing of all Veteran paper mail processed under the MMS contract.

Section 8. Technical Access and Security

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

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

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

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

Access control is maintained in accordance with FIPS Publication 199 *Moderate* information system control standards. Team GovCIO follows the Principle of Least Privilege when approving access to any system and/or data. System users and administrators are given only the minimum access necessary to perform their function(s). Standard minimum access profiles are maintained via roles defined for the VCIP SMTS application. Role-based access requests and revocations are processed within the application. The Team GovCIO System Administrator verifies requests are made from valid VA accounts and then the requests are processed by a VBA Station Supervisor and final approval is granted by the VCIP Administrators.

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?

The Access to the system is in the form of read access based on the access request provided reviewed and approved by the system Owner or delegates. Team GovCIO follows the Principle of Least Privilege when approving access to any system and/or data. System users and administrators are given only the minimum access necessary to perform their function(s). Standard minimum access profiles are maintained via roles defined for the VCIP SMTS application. Role-based access requests and revocations are processed within the application.

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

Team GovCIO follows the Principle of Least Privilege when approving access to any system and/or data. System users and administrators are given only the minimum access necessary to perform their function(s). Standard minimum access profiles are maintained via roles defined for the VCIP SMTS application. Role-based access requests and revocations are processed within the application.

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

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access

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

VCIP SMTS is a contractor-furnished and maintained system. At the end of the previous PMCMS contract the applications were transitioned, system shut down, access terminated. Per current Performance Work Statement (PWS) for VCIP VBA Mail Management System (MMS), the terms stated in attachment 44, "VA 6500.6, Contract Security, Appendix C.pdf" applies to the current MMS contract. In addition to VA 6500.6, the following terms apply to our contract (all contractors are required to acknowledge):

- No work shall be performed OCONUS.
- Access to AWS GovCloud requires the completion of an active public trust background investigation with the VA.
- Access to production applications require multi-factor authentication via VA IAM. For VA employees and the designees (which includes our contractors), multifactor authentication leveraging SSO with a PIV card is enforced. PIV cards are terminated at contract end.

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 persons associated with VCIP SMTS development, operation, and maintenance receive initial entry, annual refresher, and ad hoc training on privacy, including the Privacy Act, HIPAA, system and data security, and the VA Rules of Behavior (ROB)

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Complete
2. *The System Security Plan Status Date:* 30-Oct-2023
3. *The Authorization Status:* Authorization to Operate (ATO)
4. *The Authorization Date:* 11/21/2023
5. *The Authorization Termination Date:* 21-Nov-2025
6. *The Risk Review Completion Date:* 20-Nov-2023
7. *The FIPS 199 classification of the system (LOW/**MODERATE**/HIGH):* **Moderate**

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

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

The enhanced implementation of VCIP SMTS with SSO enabled, improved performance and enhanced reporting capabilities was released to production August 9, 2020.

The FIPS 199 classification for VCIP SMTS is a Moderate system. 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.

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1*. (Refer to question 3.3.1 of the PTA)*

The Cloud Model implemented is Amazon Web Service FedRamp High Government Cloud leveraging the AWS hosted PaaS services for:

1. Cloud Front
2. Relational databases
3. Elastic Containers
4. Fargate with lambda functions
5. Elastic Beanstalk

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

A Statement of Work (SOW) or Performance Work Statement (PWS) will be written to establish privacy roles and responsibilities for contractors if they are required to have access to PHI/PII. The program uses VA T1SOR with ROB, Training, and compliance audits for contractors.

The authorization for operation of VCIP is:

- VA Contract No. VA118-16-D-1003
- Purchase Order 36C10B20N1003008, with Federal authorization to collect information under: "Title 38, U.S.C. Chapter 3, Section 210 (c) (1), Title 38 U.S.C. 7301, 5 U.S.C. 552a.and Executive order 9397."

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.

The CSP does not collect any ancillary data related to the VCIP-SMTS system or its' users. The Program VCIP-SMTS is in control of the ancillary data. The program leverages the VA T1SOR for compliance and the PWS contract for further compliance to Privacy Standards requirements.

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.

VA issues guidelines verifying and maximizing the quality, utility, objectivity, and integrity of disseminated Privacy Act information in VA Handbook and Directive 0009: Ensuring Quality of Information Disseminated by VA.

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).

N/A

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**

ID	Privacy Controls
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.

MARVIS HARVEY

Digitally signed by MARVIS HARVEY
Date: 2024.10.30 11:37:19 -05'00'

Privacy Officer, Marvis Harvey

RICHARD ALOMAR-LOUBRIEL

Digitally signed by RICHARD ALOMAR-LOUBRIEL
Date: 2024.11.18 15:48:54 -04'00'

Information System Security Officer, Richard Alomar-Loubriel

JOHN CLARK

Digitally signed by JOHN CLARK
Date: 2024.11.19 21:14:47 -06'00'

Information System Owner, John Clark

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).

QuickSubmit Privacy Policy

Thank you for visiting the Department of Veterans Affairs (VA) QuickSubmit site and reviewing our Limited Privacy Policy (aka "Local Privacy Policy"). The VA applies leading privacy practices
and adheres to data stewardship principles in securely managing our user data on the Web. The data stewardship principles guiding our efforts include the following goals: protection of user privacy; maintaining the confidentiality of user data; and ensuring appropriate levels of security for user data.

Privacy Act Rights

The VA follows the requirements of the Privacy Act, which protects your personal information that VA maintains in "systems of records." A system of records is a file, database, or program from which personal information is retrieved by name or another personal identifier. The Privacy Act provides several protections for your personal information. These typically include how information is collected, used, disclosed, stored, and disposed of. VA System of Records Notices (SORN) are available at: Department of Veterans Affairs Privacy Act Systems of Records.
QuickSubmit is a system that uses your data from VA Systems of Record or submits data to a VA
Systems of Record.
QuickSubmit is a "Department of Veterans Affairs computer system" (aka, "VA System") controlled by the Department of Veterans Affairs and operated by GovCIO, LLC., an authorized VA contractor. QuickSubmit is hosted within the Continental United States (CONUS) with a federal Authority to Operate (ATO). All data that passes through QuickSubmit is considered VA-sensitive data. This system, including all related equipment, networks, and network devices (specifically including Internet access) are provided only for authorized uses. VA systems may be monitored for all lawful purposes, including ensuring that their use is authorized, managing the system, protecting against unauthorized access, and verifying security procedures, survivability, and operational security. During monitoring, information may be examined, recorded, copied, and used for authorized purposes.
QuickSubmit will not disclose your personal information to third parties outside VA without your consent, except to facilitate the transaction, to act on your behalf at your request, or as

authorized by law. When QuickSubmit does collect personal information from you online, we will tell you in advance in our Limited Privacy Policy. QuickSubmit will use your information to process requests for VA services or information. When QuickSubmit collects information from you, we will reference the relevant authority in our Limited Privacy Policy. Providing the information is voluntary, but if it is not provided, we may not be able to process your request and provide you with electronic services. When information is required to process your request, we will advise you of this fact in the appropriate Limited Privacy Policy. Any decision you make not to provide information will not have any effect on any benefits to which you may be entitled.

VA General Privacy Policy

The VA maintains a General Privacy Policy which applies to all public VA Web pages and sites: https://www.va.gov/privacy/index.htm. Some VA Web sites may provide additional policy guidance on privacy practices compatible with the General Privacy Policy. These additional privacy policies are called "Limited Privacy Policies."

QuickSubmit Limited Privacy Policy

This Limited Privacy Policy describes how the VA handles the following personal information you provide to the VA via QuickSubmit:

• Personally Identifiable Information (PII) for QuickSubmit includes your name, email address, zip code, phone number.
• Sensitive Personal Information (SPI) includes your Veteran File Number, which could also be your Social Security Number (SSN).
• Depending on the details contained in the documents you upload to QuickSubmit, additional information may include:
o Personally Identifiable Information (PII) such as home address, date of birth, and other identification numbers or documents such as driver's license, birth certificates, marriage certificates, etc. Government-issued documents or certificates and legal documents are likely to contain PII.
o Personal Health Information (PHI) related to medical conditions.

The information you have submitted to QuickSubmit is considered VA sensitive data.
The operator of QuickSubmit, GovCIO, LLC., will not use your email, mailing address, or phone number to send promotional messages and newsletters via email, or otherwise alert you to products or services we think might be of interest to you. QuickSubmit will never sell, rent, or trade your personal information to outside parties. QuickSubmit will not disclose your personal information to third parties outside the VA without your consent, except to facilitate the transaction, to act on your behalf at your request, or as authorized by law.

QuickSubmit will use your information to process requests for VA services or information. QuickSubmit has the federal authorization to collect information under Title 38, U.S.C. Chapter 3, Section 210 (c) (1), Title 38 U.S.C. 7301, 5 U.S.C. 552a, and Executive order 9397. Providing the information is voluntary, but if it is not provided, we may not be able to process your request and provide you with electronic services. Any decision you make not to provide information will not have any effect on any benefits to which you may be entitled.
This limited privacy policy applies to VA claimants (veterans, veteran beneficiaries) and appointed agents acting on their behalf with a VA Form 21-22 (Veteran Service Organizations) and VA Form 21-22a (Individual as Claimant's Representative).

Information Collected and Stored Automatically

We automatically collect certain information about your visit to the QuickSubmit application for the authorized purpose of tracking when a document was submitted, by whom, and for what purpose. We automatically collect and store the following information about your visit to the QuickSubmit website:

- General log information. Examples of general log information include but are not limited to: Internet domain; Internet Protocol (IP) address; operating system; the browser used to access our website; the date and time you accessed our site; and the parts of the online site that you visited.
- Referral and statistical information where we have links to or from the site you visited. Such data may include aggregate data such as the number of logins within a period, the number of documents uploaded or downloaded, or the size of documents uploaded or downloaded. It may also include specific data, such as the identity of the site which you visited immediately before or after our site. We do not use such data to identify you personally.

We use the general log information to help us make QuickSubmit sites more useful to end users. We use it to learn about how the features on our site are being used, what information is of most and least interest, and how we can enhance ease of use by ensuring our sites can interface with the types of technology our visitors use. We also use such statistics to tell us of any site performance problems or suspicious activity. Except for oversight, law enforcement investigations, or protection of the VA information technology infrastructure as authorized by law, no other attempts are made to identify you or your usage habits.
General logs are used for no other purposes than the purposes described above and are scheduled for regular destruction in accordance with General Records Schedules published by the National Archives and Records Administration (NARA) and agency record control schedule requirements.

Use of Cookies and Tracking Technologies

When you visit certain websites, they send a small piece of information called a "cookie" to your web browser along with the web page. This is also true of QuickSubmit. For the purposes of this privacy policy, there are two kinds of tracking cookies to consider.

▪ A Persistent Cookie is a line of text that is saved to a local file used by your web browser that is called up the next time you visit that website. This lets the site remember information about your previous visits and use of the website. Persistent Cookies are

not used by the VA or other federal government websites, unless there is a compelling and authorized reason for their use. If any VA web page uses a Persistent Cookie, then the Limited Privacy Policy for that web page will clearly state the purpose and legal authority for such use.

QuickSubmit does not use Persistent Cookies.

▪ A Session Cookie is a text line stored temporarily in your computer's random-access memory (RAM). A Session Cookie is destroyed as soon as you close your browser.

QuickSubmit uses Session Cookies in the following manner:

▪ Since QuickSubmit requires all users to be logged in, registered, and authenticated by the VA, we use session cookies with both the Secure (HTTPS/TLS required) and Http Only (read only) flags set to true. They help enable us to authorize you as a specific user authenticated by the VA.

▪ During the QuickSubmit login process, AccessVA and AccessVA Sign-In Partners may require the use of other Session Cookies for end users to authenticate with the VA prior to being authorized by QuickSubmit. For more information about AccessVA, see the AccessVA FAQ: https://eauth.va.gov/accessva/about.

Log In and Registration

QuickSubmit requires all authorized users to be logged in. We do not support the concept of visitors or unauthenticated users. During the login process, users must first be authenticated by the VA. When you go the QuickSubmit public URL (Uniform Resource Locator), https://digitization.gcio.com/va/upload/, you will be redirected to the VA's authentication URL for QuickSubmit (https://eauth.va.gov/accessva/?cspSelectFor=quicksubmit) to authenticate with a government approved AccessVA Sign-In Partner. After authentication, if you are not yet a registered user, QuickSubmit requires you to register with our application to be an authorized user. Registration is a quick, one-time, one-step process.

Password Protection

When you register for a QuickSubmit account, access to your personal information will be protected by multifactor authentication, which typically includes an email address, a password, and at least one other authentication factor such as a mobile phone that can receive security codes via text message or virtual multifactor authentication (MFA) application such as but not limited to Google Authenticator or Authy. We strongly recommend that you do not divulge your

password to anyone, do not reuse it with another site, change it when needed, and do not share the device used for your additional authentication factor.

Many Internet browsers allow users to save user information, including passwords. When prompted by a browser to save your AccessVA Sign-In Partner's authentication credentials such as your email address and password, you should decline this option. Saving this information could potentially allow persons who gain access to a shared device to access their personal information. You are protected in this scenario by the VA requirement for multifactor authentication before accessing your personal information.

For information on details such as password length/complexity, reset/recovery, and VA account or multifactor authentication (MFA) setup, please visit the appropriate Sign-In Partner recognized in AccessVA for QuickSubmit and refer to their specific password and security recommendations: https://eauth.va.gov/accessva/?cspSelectFor=quicksubmit

Logging Out

Please remember to log out when you are finished using QuickSubmit. Logging out prevents someone else from accessing your personal information if you leave, share, or use a public computer (located, for example, in a library or an Internet cafe) and your session has not automatically "timed out" or shut down. As a last resort, if you forget to log out or 30 minutes of non-activity pass, the session will automatically time out.

Information Sharing

We do not sell, rent, or otherwise provide your personal information to outside marketers. Information collected via QuickSubmit may be shared with VA employees, contractors, and other service providers as necessary to respond to a request, provide a service, or as otherwise authorized by law. If appropriate, additional information regarding the use and disclosure of information collected on specific web pages will be posted in the appropriate Limited Privacy Policy for QuickSubmit.

Security

In those instances where we secure your personal information in transit to us over the Internet, and upon our receipt, QuickSubmit uses industry-standard encryption, including Transport Layer Security (TLS), formerly known as Secure Socket Layer (SSL). The connection icon area on

your browser will change to “HTTPS” instead of “HTTP” when this security feature is invoked. Your browser may also display a lock symbol on the task bar at the bottom of your screen to indicate this secure transmission is in place. You should refer to the instructions for your Internet browser software to determine how to examine the security certificate from our website to verify the connection's security.

For site security purposes and to ensure that QuickSubmit remains available to all users, QuickSubmit monitors network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage. Except for oversight or authorized law enforcement investigations, no other attempts are made to identify individual users or their usage habits other than those uses identified in this policy.

Unauthorized attempts or acts to (1) access, upload, change, or delete information on this system, (2) modify this system, (3) deny access to this system, or (4) accrue resources for unauthorized use on this system, are prohibited and may be considered violations subject to criminal, civil, or administrative penalties.

The VA and QuickSubmit take the security of all personally identifiable information we receive very seriously. We implement various measures to protect the security and confidentiality of personally identifiable information. Such measures include access controls designed to limit access to personally identifiable information to the extent necessary to accomplish our mission. We also employ various security technologies to protect personally identifiable information stored on our systems. We test our security measures periodically to ensure that they remain operational.

Links to External Sites

QuickSubmit provides access to other websites outside our control and jurisdiction. When you click on a link to these websites, you leave our application, so your communications are no longer protected by our privacy policies. If the link is to another VA website, the QuickSubmit Limited Privacy Policy no longer applies but the VA General Privacy Policy still applies; however,

if the link is to a non-VA website, neither QuickSubmit nor the VA is responsible for the privacy practices or the content of those non-VA websites. We encourage you to review the privacy policy or terms and conditions of those sites to fully understand what information is collected

and how it is used.

Contact the VA Privacy Service

Please let us know if you have any questions or concerns regarding our privacy policy or use of your information. You can get more information at the VA Privacy Service online, and you can email your question or concern directly to privacyservice@va.gov, or send a letter to Department of Veterans Affairs, Privacy Service, 810 Vermont Avenue, N.W. (005R1A) Washington, DC 20420.

Your inquiry will be treated confidentially and will not be shared with third parties, except as necessary to respond to your inquiry and for other purposes as authorized by the Privacy Act and other relevant legal authority.

The VA Privacy Service works to minimize the impact on Veterans' privacy, particularly Veterans' personal information and dignity, while achieving the mission of the Department of Veteran Affairs.

Last reviewed on October 31, 2023

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