Privacy Impact Assessment for the VA IT System called:

Beneficiary Travel Self-Service System (BTSS)

VHA Members Services, Health Eligibility Center

Veteran Transportation Program (VTP)

Date PIA submitted for review:

October 20, 2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Shirley Hobson	Shirley.Hobson@va.gov	404-828-5337
Information System Security Officer (ISSO)	Terry Dziadik	Terry.Dziadik@va.gov	412-822-3211
Information System Owner	Tony Sines	Tony.Sines@va.gov	316-2498510

Abstract

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

The Beneficiary Travel Self Service System (BTSSS) is a modern alternative to the current Travel Vista Claim package. The BTSSS system, hosted on Microsoft Government cloud infrastructure, automates a majority of the manual decisions and processes under the legacy system required to approve and pay a travel claim for Veterans, Caregivers and eventually Vendors. The BTSSS system leverages patient and appointment information currently stored in VA systems of record (SORs) to validate the claimant information and verify eligibility for payment. The system provides a single point of access by the claimant through DS Logon, AccessVA, ID.me, LOGIN.GOV and My HealtheVet (MHV) to submit and monitor the claim status using their own device such as PC, phone or tablet. The system stores only the Personal Identifiable Information (PII) necessary to process and audit the processing of travel claims.

Overview

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

1 General Description

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

Beneficiary Travel Self-Service System (BTSSS) and Veteran Transportation Program (VTP)

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

The Beneficiary Travel Self Service System (BTSSS) is a cloud hosted solution owned by VHA, Veteran Transportation Program (VTP) for processing Veteran travel related benefits in compliance with requirements found in 38 CFR Part 70, Beneficiary Travel under 38 U.S.C. 111. BTSSS is expected to store the information of approximately 1.6M clients within its record system which will be housed on the Microsoft Government Cloud. The physical servers are located in Virginia and Iowa. VA owns all the data within the Microsoft Government Cloud.

All BTSSS records at VA sites are protected from unauthorized access by systems and include external security, access control, and identification procedures. The BTSSS system will be hosted on Microsoft Government cloud infrastructure. Microsoft GovCloud (US) is an isolated region designed to host sensitive workloads in the cloud, ensuring that this work meets the US government's regulatory and compliance requirements. The Microsoft GovCloud (US) region adheres to United States International Traffic in Arms Regulations (ITAR) as well as Federal Risk and Authorization Management Program (FedRAMP) requirements. Microsoft GovCloud (US) is available to US government agencies, government contractors, private and public commercial entities, educational institutions, nonprofits and research organizations that meet GovCloud (US) requirements for access. Microsoft GovCloud (US) has received an Agency Authorization to Operate (ATO) from the US Department of Veterans Affairs. Therefore, the BTSSS Hosted Solution will utilize FedRAMP Department of Veterans Affairs ATO and implement shared security controls for BTSSS ATO.

The typical client is the Veteran on whom the travel claims or request for travel assistance is processed. This is a national program used by all VA medical centers to process travel for Veterans. Information within the system is primarily payment history but it does have claimant identifiable information used to process the claim as part of the payment record. The system generates ad hoc reports on demand for analysis of payment demographics to determine trends and forecast costs for budgeting purposes. The system interfaces with several systems of records to support the processing of a claim or travel request but it only shares claim related data with the Financial Management System (FMS) to facilitate the Veterans reimbursement and will eventually interface with the Corporate Data Warehouse (CDW) for storage of historical records and analytics. Systems include: Identity Access Management (IAM) for internal and external single sign-on, Master Veterans Index (MVI) for correlated Identifications, Enrollment Services (ES) for eligibility and enrollment data, VistA Integration Adapter (VIA) for

appointment data, Financial Management System (FMS) via Financial Services Center (FSC) for obligation and payment data, and in the future the Corporate Data Warehouse (CDW) for storage of historical records.

Within VA, the legal authority to gather and use the SSN to verify veteran information is outlined in VA Handbook 6507.1 Section 2 subsection a(8).

The collection, processing, and dissemination of health information must follow the rules and regulations established by the:

- Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191 (Aug. 21, 1996), (codified in scattered sections of title 42 U.S. Code) (full-text); 45 C.F.R. parts 160 and 164 (HIPAA Privacy and Security Rules).
- Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5, 123 Stat. 226 (Feb. 17, 2009), *codified at* 42 U.S.C. §§300jj *et seq.*; §§17901 *et seq.*

Additionally, the collection, processing, and dissemination of Beneficiary Travel must follow the rules and regulations established by the:

- Title 38 United States Code (U.S.C.), Section 111
- Title 38 Code of Federal Regulations (CFR) Sections 70.1, 70.2, 70.3, 70.4, 70.10, 70.20, 70.21, 70.30, 70.31, 70.32, 70.40, 70.41, 70.42, 70.50

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

VA Controlled / non-VA Owned and Operated

2. Information Collection and Sharing

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

Over 9 million or 60% of the eligible veterans are believed to be utilizing the BTSSS for reimbursement for travel to and from their VA medical appointments.

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

Basic contact information (name, contact info, SS#, income and banking info, veteran related info., Claim information, Appointment information, VA and associated facility information, and payment history information is all pulled directly from FMS and displayed within the BTSSS system. This information is used to identify claimants and to process payments.

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

Information is transmitted between several systems. VistA and Cerner Millennium are VA SORs that transmit VistA and EHRM appointment data to BTSSS. VIA or VDIF serve as adapter interfaces for VistA interface.

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

BTSSS leverages Microsoft Dynamics 365 SaaS as the application framework. BTSSS serves multiple sites but since Microsoft Dynamics 365 is a centralized SaaS, by definition, all data is consistent.

3. Legal Authority and SORN
A citation of the legal authority to operate the IT system.

Within VA, the legal authority to gather and use the social security number (SSN) to verify veteran information is outlined in VA Handbook 6507.1 Section 2 subsection a(8).

2001 Privacy Act, VA Federal Register Privacy Act Systems of Records Notices, Index to VA System of Records: https://vaww.va.gov/privacy/SystemsOfRecords/2001_Privacy_Act_GPO_SOR_compilation.pdf , e.g., 79VA19 System name: Veterans Health Information Systems and Technology Architecture (VistA) Records-VA., and 13VA047 System name: Individuals Submitting Invoices/Vouchers For Payment-VA.

The collection, processing, and dissemination of Beneficiary Travel health information must follow the rules and regulations established by the:

Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191 (Aug. 21, 1996), (codified in scattered sections of title 42 U.S. Code) (full-text); 45 C.F.R. parts 160 and 164 (HIPAA Privacy and Security Rules).

Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5, 123 Stat. 226 (Feb. 17, 2009), *codified at* 42 U.S.C. §§300jj *et seq.*; §§17901 *et seq.*

Additionally, the collection, processing, and dissemination of Beneficiary Travel health information must follow the rules and regulations established by the:

Title 38 United States Code (U.S.C.), Section 111
Title 38 Code of Federal Regulations (CFR) Sections 70.1, 70.2, 70.3, 70.4, 70.10, 70.20, 70.21, 70.30, 70.31, 70.32, 70.40, 70.41, 70.42, 70.50

The BTSSS terms and conditions to be read and acknowledged by the Veteran in registering for BTSSS, contains a Privacy Act “Routine Uses” section describing how the information will be used.

H. 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?

N/A

D. System Changes

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

N/A

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

N/A

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.

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

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

- For Veterans, Dependents, or Caregivers the following information is collected: First and Last name, Email address, Integrated Control Number (ICN) Electronic Data Interchange Personal Identifier (EDIPI), Correlated IDs, Address, Date of Birth, Eligibility and Enrollment Data (such as service-connected percentages), Appointment Data (such as appointment date, appointment status and facility location), Vendor ID, Dollar Amount, and Claims related data.

For VA employees their first and last name along with their email address is collected.

For VA Contractors their first and last name along with their email address is collected.

*Specify type of Certificate or License Number (e.g. Occupational, Education, Medical) N/A

PII Mapping of Components (Servers/Database)

Beneficiary Travel Self-Service System consists of 2 key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **Beneficiary Travel Self-Service System** and the reasons for the collection of the PII are in the table below.

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

Internal Database Connections

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
Dynamics365	Yes	Yes	Demographics, SSN	Identify the claimant, process payments	stored encrypted in the database, transmitted encrypted via HTTPS, secured by SSOe/SSOi and role-based security, only accessible on VA
Dynamics365 Portals	Yes	Yes	Demographics, SSN	Identify the claimant, process payments	stored encrypted in the database, transmitted encrypted via HTTPS, secured by

					SSOe/SSOi and role-based security

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?

Some verifying information is collected from the Veteran such as the location and date time of the appointment on which the travel claim is based. Information from systems of records such as MVI is also used to confirm the individual accessing the systems identity and residential information for calculating mileage traveled. All information sources other than those from the claimant are retrieved from or provide interface with VA internal systems for the purposes of processing Veteran requests for Travel assistance or payment: MVI, VIA/VistA, ESR, FSC/FMS, and BTSSS. Additionally, payment history is stored within closed VA systems; BTSSS sends payment approval electronically to FMS and in the future will send payment history to CDW for storage.

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.

Beneficiary Travel is a regulatory benefit for which Veterans must apply to receive mileage reimbursement. BTSSS is a new system that allows electronic interaction between the claimant and VHA staff processing claims or requesting services. The overall processing of a claim will be automated as much as possible aimed at reducing the time from request to payment of a claim and the administrative burden on the number of personnel needed to manually process a claim. BTSSS once in service will replace the current highly manual and paper dependent, Vista Beneficiary Travel Dashboard and the Data Group Beneficiary Travel (DGBT) claim system. Once a claim is completed it is a record of payment transaction and the information supporting the claim must be stored or easily retrieved to satisfy audits.

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

Some verifying information is collected from the Veteran such as the location and date time of the appointment on which the travel claim is based. Information from systems of records such as MVI is also used to confirm the individual accessing the systems identity and residential information for calculating mileage traveled. All information sources other than those from the claimant are retrieved from or provide interface with VA internal systems for the purposes of processing Veteran requests for Travel assistance or payment: MVI, VIA/VistA, ESR, FSC/FMS, and BTSSS. Additionally,

payment history is stored within closed VA systems; BTSSS sends payment approval electronically to FMS and in the future will send payment history to CDW for storage.

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?

Information is collected electronically from the Veteran when entering payment request into the BTSSS claimant portal. Information is transmitted electronically from MVI, ESR to the BTSSS for the purpose of processing the claim and to FMS and in the future to CDW for the purpose of authorizing payment and storing payment history. Veteran may also use VA form 10-3542 to submit a written request for payment. Information that comes from the Veteran that is required for a claim submission is stored with the claim record in Microsoft Dynamics. This includes attachments submitted by the Veteran.

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

Information is collected electronically from the Veteran when entering payment request into the BTSSS claimant portal. Information is transmitted electronically from MVI, ESR to the BTSSS for the purpose of processing the claim and to FMS and in the future to CDW for the purpose of authorizing payment and storing payment history. Veteran may also use VA form 10-3542 to submit a written request for payment. Information that comes from the Veteran that is required for a claim submission is stored with the claim record in Microsoft Dynamics. This includes attachments submitted by the Veteran

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.

BTSSS will not store data controlled by other systems of record unless it specifically relates to the claim being submitted and processed. Once a claim is submitted and processed, it is stored in

Microsoft Dynamics. BTSSS will access each system of record to pull relevant information each time a decision is being made on that information. For any data that is stored as part of BTSSS, when the call is made to the system of record, this data will be updated within BTSSS and stored in Microsoft Dynamics. All the Data will be checked at the source end.

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

BTSSS will not store data controlled by other systems of record unless it specifically relates to the claim being submitted and processed. Once a claim is submitted and processed, it is stored in Microsoft Dynamics. BTSSS will access each system of record to pull relevant information each time a decision is being made on that information. For any data that is stored as part of BTSSS, when the call is made to the system of record, this data will be updated within BTSSS and stored in Microsoft Dynamics. All the Data will be checked at the source end.

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

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

Within VA, the legal authority to gather and use the social security number (SSN) to verify veteran information is outlined in VA Handbook 6507.1 Section 2 subsection a(8).

Additionally, the collection, processing, and dissemination of health information must follow the rules and regulations established by the:

> Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191 (Aug. 21, 1996), (codified in scattered sections of title 42 U.S. Code) (full-text); 45 C.F.R. parts 160 and 164 (HIPAA Privacy and Security Rules).
> Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5, 123 Stat. 226 (Feb. 17, 2009), *codified at* 42 U.S.C. §§300jj *et seq.*; §§17901 *et seq.*

The BTSSS terms and conditions to be read and acknowledged by the Veteran in registering for BTSSS, contains a Privacy Act "Routine Uses" section describing how the information will be used.

Additionally, the collection, processing, and dissemination of Beneficiary Travel must follow the rules and regulations established by the:

> Title 38 United States Code (U.S.C.), Section 111
> Title 38 Code of Federal Regulations (CFR) Sections 70.1, 70.2, 70.3, 70.4, 70.10, 70.20, 70.21, 70.30, 70.31, 70.32, 70.40, 70.41, 70.42, 70.50

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: Unauthorized users accessing BTSSS and gaining access to PII/PHI

Mitigation:

1. Because BTSSS is an online cloud solution in the Microsoft Government cloud, there are already numerous security controls in place that are inherited as part of the FedRAMP ATO issued for this platform.
2. BTSSS utilizes VA-approved authentication through IAM with Single Sign On internal (SSOi) for internal users and Single Sign On external (SSOe) for external users.
3. Once users are authenticated, BTSSS uses role-based security (security roles) and row-level security (teams) to authorize a user to only view data for their assigned facility/VISN/region/national level of access.

Section 2. Uses of the Information

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

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

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

External: The information gathered from the claimant is used to confirm the claimant's identity and eligibility for payment and to calculate the amount of payment if eligible or to notify the claimant of denial and procedures for appeal of claim for payment. The claimant also receives notification of each claim's status throughout the process. Internal: BT staff and automated rules engine use the information to review and process the claim for accuracy and payment approval or denial. Both the rules engine and travel clerk actions are recorded at the row level showing how each claim passes or fails each business rule, including the data supporting the disposition. This ensures that a complete audit trail for the adjudication of the claim is recorded and available for reporting and analytics. Approved claims are transmitted to FMS for payment. Payment history is used for auditing by all levels from facility to program office and external parties as directed by Congress such as Improper Payment Elimination Recovery Act (IPERA). Name - confirm identity of claimant SSN - confirm identity of claimant Personal Phone Number(s) - to contact claimant if necessary Personal Email Address - to contact claimant if necessary Financial Account - to make payment to claimant Personal Mailing Address - to contact claimant by mail, if necessary, Zip Code - to contact claimant by mail if necessary Previous Medical Records - to identify appointment for reimbursement

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.

For new claims data, new records will be created and associated to the claimant’s contact record. For updated information within a claim or a contact record, the system will record the new value and audit trails will show who updated the record and when. This new information will be used by the system and its users to approve or deny claims. BTSSS will also include standard pre-formatted reports for real-time transactional analysis, as well as adhoc reporting capabilities through the Advanced Find Customer Relationship Management (CRM) feature for dynamic reporting. Reports may contain PII listed in Section 1.1, depending upon report parameters. The reports are developed, shared, maintained and/or discarded by the discretion of the Veteran Transportation Program office and rules of behavior (ROB) policy. In the future, more advanced analytics and historical analysis will be available through CDW. These various tools for analytics and reporting, coupled with the audit capabilities within Dynamics365, will assist the VA in fighting fraud, waste, and abuse.

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.

For new claims data, new records will be created and associated to the claimant's contact record. For updated information within a claim or a contact record, the system will record the new value and audit trails will show who updated the record and when. This new information will be used by the system and its users to approve or deny claims.

BTSSS will also include standard pre-formatted reports for real-time transactional analysis, as well as adhoc reporting capabilities through the Advanced Find Customer Relationship Management (CRM) feature for dynamic reporting. Reports may contain PII listed in Section 1.1, depending upon report parameters. The reports are developed, shared, maintained and/or discarded by the discretion of the Veteran Transportation Program office and rules of behavior (ROB) policy. In the future, more advanced analytics and historical analysis will be available through CDW.

These various tools for analytics and reporting, coupled with the audit capabilities within Dynamics365, will assist the VA in fighting fraud, waste, and abuse.

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?

PII within BTSSS is segregated by federal employees' duties and security controls within the system using a role-based framework.

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

System access is restricted. Permission for access is granted to only VA staff and contractors with the need to know. In other words, SSNs are masked (hidden) by default, and only available to privileged users, and only in partial form (the last 4).

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

Because BTSSS is an online cloud solution in the Microsoft Government cloud, there are already numerous security controls in place as part of that platform. BTSSS uses mock data for development and testing that comes from VA systems of record that BTSSS is integrated with. No real data is used during research, testing or training.

BTSSS utilizes VA-approved authentication through IAM with SSOe for external users. Once users are authenticated, external users can only see their own claims and related appointment and profile data. BTSSS does not share any information externally.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

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

2.4a How is access to the PII determined?

Access to PII within BTSSS is segregated by federal employees' duties and security controls within the system by a role-based framework.

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

Yes

2.4c Does access require manager approval?

Yes, upon initial hire manager approval is required before PII can be accessed.

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

Access to PII within BTSSS is segregated by federal employees' duties and security controls within the system by a role-based framework.

2.4e Who is responsible for assuring safeguards for the PII?
Everyone who uses the BTSSS program.

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*

BTSSS collects information listed in question 1.1 from other VA systems of record for the purpose of processing claims but does not retain this information. Once a claim is submitted and processed it is stored in Microsoft Dynamics. Any information that came from the Veteran that is required for a claim submission is stored with the claim record in Microsoft Dynamics, including attachments submitted by the Veteran. Any attachments created and uploaded by the Travel Clerk are stored with the contact record in Microsoft Dynamics. Contact Entity: First Name Last Name Street 1 Street 2 Street 3 City State/Providence Zip/Postal Code Country/Region Phone Number Email SSN Net Income Income Effective Income Modified By Income Modified On Bank Name Bank Account # Bank Routing Number Full Name SSN Appointment Entity: Name Date & Time Facility Name Completed Claim Entity: Claimant First Name Middle Name Last Name Address Line 1 Address Line 2 City State/Providence Zip/Postal Code Caregiver Caregiver First Name Caregiver Middle Name Caregiver Last Name Caregiver Address Line 1 Caregiver Address Line 2 Caregiver City Caregiver State/Providence Caregiver Zip/Postal Code Facility Appointment Appointment Date Appointment Completed Mileage Expense Entity: Address From Line 2 State Zip/Postal Code Address To Line 2 City State Zip/Postal Code Cost

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.*

This document specifies how long records will be retained by the VA (6 years in the case of BTSSS finance records), if/when they will be transferred to a national records storage location, and the length of time the records will be stored at the national level. For greater details related to records retention at the Veterans' Health Administration, please review RCS10-1. https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf BTSSS database information will be retained for the life of the project, and the server logs will be rotated on a periodic basis. In BTSSS, even

when you delete information, that information is just flagged as deleted and blocked from general viewing and is not actually deleted from the database. A system administrator will be responsible for writing and executing a database script to permanently delete any data based on guidance from the Veterans Transportation Service (VTS) staff.

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?

When managing and maintaining VA data and records, BTSSS will follow the guidelines established in pursuant to NARA General Records Schedules GRS 3.2, item 030 and item 031.
https://www.archives.gov/records-mgmt/grs.html

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

This document specifies how long records will be retained by the VA (6 years in the case of BTSSS finance records), if/when they will be transferred to a national records storage location, and the length of time the records will be stored at the national level. For greater details related to records retention at the Veterans' Health Administration, please review RCS10-1.
https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

BTSSS database information will be retained for the life of the project, and the server logs will be rotated on a periodic basis. In BTSSS, even when you delete information, that information is just flagged as deleted and blocked from general viewing and is not actually deleted from the database. A system administrator will be responsible for writing and executing a database script to permanently delete any data based on guidance from the Veterans Transportation Service (VTS) staff.

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.

Paper documents are destroyed to an unreadable state in accordance with the Department of Veterans' Affairs VA Directive 6371, (April 8, 2014), http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=742&FType=2

Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and VA Handbook 6500.1 Electronic Media Sanitization. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destruction. https://www.va.gov/vapubs/search_action.cfm?dType=1

All BTSSS SPI is stored in the Microsoft Government Cloud database. Information from the application is never deleted by users, but rather marked to be disabled by setting a flag. If the request came from the VA requiring data to be deleted, Liberty (VA contractor) can write and execute a database script to do so. Upon request from VA, Liberty will securely delete all digital data

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.

BTSSS uses mock data for development and testing that comes from VA systems of record that BTSSS is integrated with. No real data is used during research, testing or training. All Testing is completed in the lower environment using "fake" or "made up" data.

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: There is a risk that the information contained in the BTSSS System will be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached.

Mitigation: In addition to collecting and retaining only information necessary for fulfilling the VA mission, the disposition of data housed is based on standards developed by the National Archives Records Administration (NARA). This ensures that data is held for only as long as necessary.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?

This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Veterans' Health Administration (VHA)	Master Person Index (MPI)	First name, Last name, email, ICN, Correlated ID	Electronically via secure web https service calls, Information is retrieved (shared) each time a user profile is accessed, and when a claim is processed.
Identity Access Management (IAM)	Authentication (Single Sign On Internal - SSOi) and Authentication (Single Sign On External - SSOe)	First Name, Last Name, email, ICN, Address, Date of Birth	Electronically via secure web https services. Security Assertion Markup Language (SAML) token is encrypted using certificates.
Veterans' Health Administration (VHA)	Eligibility and Enrollment System (ES)	Eligibility and enrollment data such as service-connected percentage	Electronically via secure web service https calls, information is retrieved (shared) each time a user profile is accessed, and when a claim is processed.
Veterans' Health Administration (VHA)	Veterans' Health Information System and Technology Architecture (VistA), VistA Integration Adapter (VIA)	Appointment Data such as appointment date, appointment status and facility location	Electronically via secure web service https calls: information is retrieved (shared) each time a user's appointment list is

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
			viewed, and when a claim is processed.
Financial Services Center (FSC)	Financial Management System (FMS)	Obligation code, Vendor ID, Dollar Amount	Electronically via secure web service calls, information is transmitted (shared) each time a claim is processed and requires payment.
VHA/Office Electronic Health Record Modernization	Oracle/Cerner Millennium EHR	EDIPI, ICN, Appointment Data such as appointment date, appointment status and facility location	Application Programming Interface (API), through Fast Healthcare Interoperability Resources (FHIR), responds with the internal Cerner Millennium Patient Identifier (ID).
Veterans' Health Administration (VHA)	VetRide	ICN, Appointment Data such as appointment date, appointment status and facility location	Electronically via secure web service https calls, information is retrieved (shared) each time a user's appointment list is viewed, and when a travel was provided by VHA's VetRide services.
Veterans' Health Administration (VHA)	Caregiver Record Management Application (CARMA)	EDIPI, ICN, Caregiver relationship information: Start/Benefit End date, Status, status date, Caregiver type	Salesforce Application Programming Interface (API)/ Mulesoft Government Cloud.

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: Unauthorized users accessing BTSSS and gaining access to PII/PHI

Mitigation:

1. Because BTSSS is an online cloud solution in the Microsoft Government cloud, there are already numerous security controls in place that are inherited as part of the FedRAMP ATO issued for this platform.
2. BTSSS utilizes VA-approved authentication through IAM with SSOi for internal users.
3. Once users are authenticated, BTSSS uses role-based security (security roles) and row-level security (teams) to authorize a user to only view data for their assigned facility/Veterans Integrated Service Networks (VISN)/region/national level of access.

Section 5. External Sharing/Receiving and Disclosure

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

5.1 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				

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

Follow the format below:

Privacy Risk: N/A

Mitigation: N/A

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.

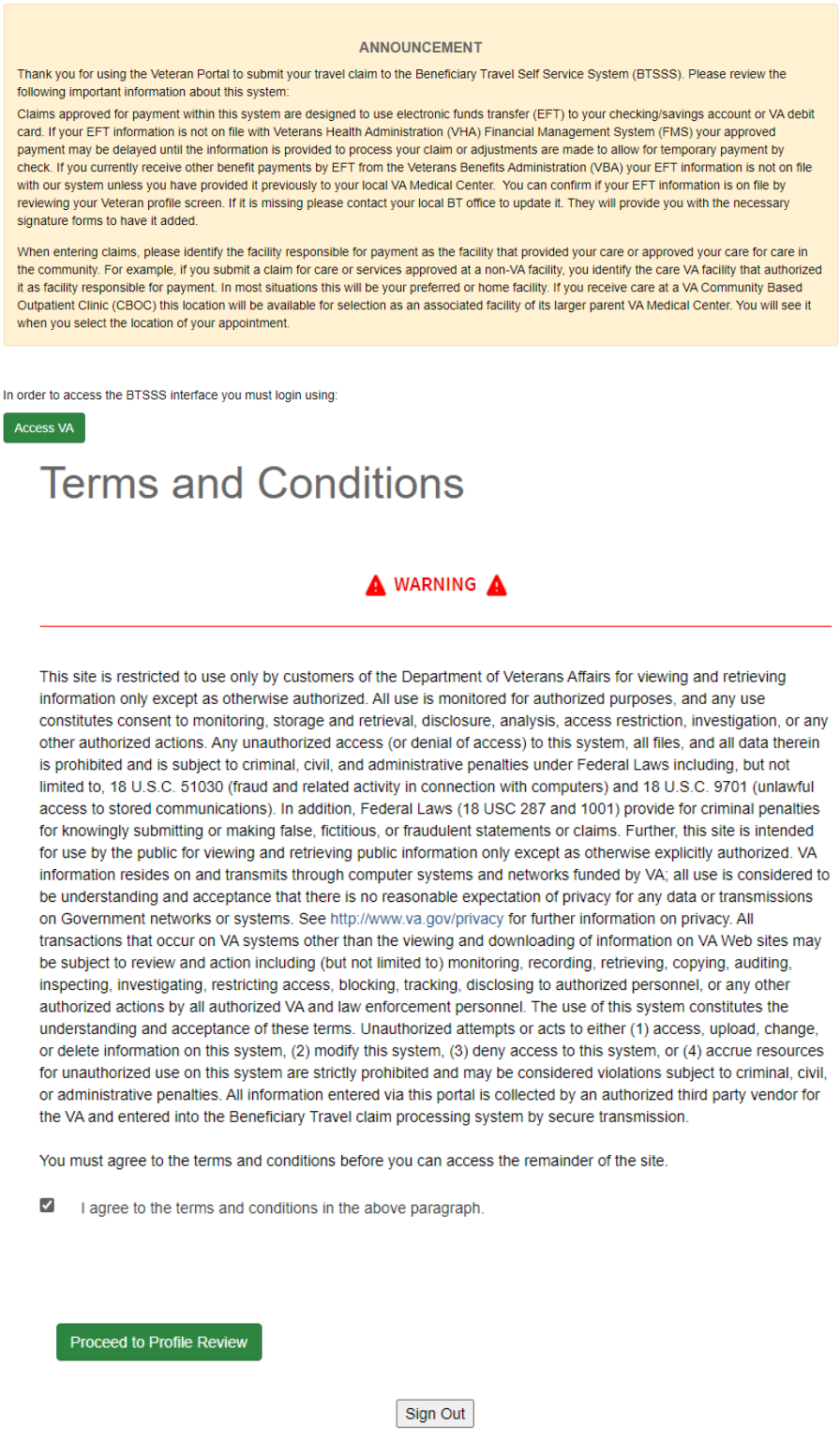
6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an Appendix-A 6.1 on the last page of the document. Also provide notice given to individuals by the source system (A notice may include a posted privacy policy, a Privacy Act 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 to all BTSSS users when they log into the system (see APPENDIX A). Veterans must acknowledge they have read and understood the BTSSS terms and conditions (see APPENDIX A) every time they make a BT Request in BTSSS. Veteran's accounts that are moved over from existing VA systems to BTSSS are not automatically notified. VTS Staff must notify Veterans via a call or email of the VTS BT system changes. Finally, this Privacy Impact Assessment (PIA) also serves as notice of the BTSSS system. As required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means." A notice was published in the Federal Register, Vol. 77, No. 211, Wednesday, October 31, 2012. for

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



ANNOUNCEMENT

Thank you for using the Veteran Portal to submit your travel claim to the Beneficiary Travel Self Service System (BTSSS). Please review the following important information about this system:

Claims approved for payment within this system are designed to use electronic funds transfer (EFT) to your checking/savings account or VA debit card. If your EFT information is not on file with Veterans Health Administration (VHA) Financial Management System (FMS) your approved payment may be delayed until the information is provided to process your claim or adjustments are made to allow for temporary payment by check. If you currently receive other benefit payments by EFT from the Veterans Benefits Administration (VBA) your EFT information is not on file with our system unless you have provided it previously to your local VA Medical Center. You can confirm if your EFT information is on file by reviewing your Veteran profile screen. If it is missing please contact your local BT office to update it. They will provide you with the necessary signature forms to have it added.

When entering claims, please identify the facility responsible for payment as the facility that provided your care or approved your care for care in the community. For example, if you submit a claim for care or services approved at a non-VA facility, you identify the care VA facility that authorized it as facility responsible for payment. In most situations this will be your preferred or home facility. If you receive care at a VA Community Based Outpatient Clinic (CBOC) this location will be available for selection as an associated facility of its larger parent VA Medical Center. You will see it when you select the location of your appointment.

In order to access the BTSSS interface you must login using:

Access VA

Terms and Conditions

WARNING

This site is restricted to use only by customers of the Department of Veterans Affairs for viewing and retrieving information only except as otherwise authorized. All use is monitored for authorized purposes, and any use constitutes consent to monitoring, storage and retrieval, disclosure, analysis, access restriction, investigation, or any other authorized actions. Any unauthorized access (or denial of access) to this system, all files, and all data therein is prohibited and is subject to criminal, civil, and administrative penalties under Federal Laws including, but not limited to, 18 U.S.C. 51030 (fraud and related activity in connection with computers) and 18 U.S.C. 9701 (unlawful access to stored communications). In addition, Federal Laws (18 USC 287 and 1001) provide for criminal penalties for knowingly submitting or making false, fictitious, or fraudulent statements or claims. Further, this site is intended for use by the public for viewing and retrieving public 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 understanding and acceptance that there is no reasonable expectation of privacy for any data or transmissions on Government networks or systems. See http://www.va.gov/privacy for further information on privacy. All transactions that occur on VA systems other than the viewing and downloading of information on VA Web sites may be 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. The use of this system constitutes the understanding and 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 and may be considered violations subject to criminal, civil, or administrative penalties. All information entered via this portal is collected by an authorized third party vendor for the VA and entered into the Beneficiary Travel claim processing system by secure transmission.

You must agree to the terms and conditions before you can access the remainder of the site.

I agree to the terms and conditions in the above paragraph.

Proceed to Profile Review

Sign Out

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.

Notice is provided to all BTSSS users when they log into the system (see APPENDIX A). Veterans must acknowledge they have read and understood the BTSSS terms and conditions (see APPENDIX A) every time they make a BT Request in BTSSS.

Veteran's accounts that are moved over from existing VA systems to BTSSS are not automatically notified. VTS Staff must notify Veterans via a call or email of the VTS BT system changes.

Finally, this Privacy Impact Assessment (PIA) also serves as notice of the BTSSS system. As required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means."

A notice was published in the Federal Register, Vol. 77, No. 211, Wednesday, October 31, 2012, for the
Veterans Health Information Systems and Technology Architecture (VistA) (79VA10), Privacy Act System of Records. Also, a notice was published prior to 1995 for the Individuals Submitting InvoicesVouchers For Payment-VA (13VA047).

https://www.oprm.va.gov/docs/SORN/Current_SORN_List_09_19_2022.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.

Individuals cannot opt out from providing information because system does not function without that information. If individuals opt out, the system will not provide them service. The Veterans Health Administration (VHA) as well as the BTSSS system request only information necessary to provide transportation services to Veterans and other potential beneficiaries. While an individual may choose not to provide information to BTSSS, this will prevent them from obtaining the necessary Beneficiary Travel (BT) services. Employees and VA contractors are also required to provide requested information to maintain employment or their contract with the VA.

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.

Providing BTSSS requested information is a voluntary act and by reading and acknowledging the terms and conditions, individuals consent to the use of the requested information for the sole purpose of BT services. Individuals cannot consent to only a portion of required data since all required data is needed to properly process BT claims. The information is not used for any other purpose.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

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

Privacy Risk: There is a risk that an individual may not receive notice that their information is being collected, maintained, processed, or disseminated by the BTSSS system prior to providing the requested information.

Mitigation: This risk is mitigated by providing the terms and conditions when Veterans submit a BT claim request. Employees and contractors are required to review, sign and abide by the National Rules of Behavior on a yearly basis as required by VA Handbook 6500 as well as complete annual mandatory Information Security and Privacy Awareness training.

Additional mitigation is provided by making the System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) available for review online, as discussed in question 6.1.

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.***

There are several ways a Veteran or other beneficiary may access information about them. The Department of Veterans' Affairs has created the MyHealthEVet program to allow online access to their medical records. More information on this program and how to sign up to participate can be found online at https://www.myhealth.va.gov/index.html. Veterans and other individuals may also request copies of their medical records and other records containing personal data from the medical facility's Release of Information (ROI) office. Employees should contact their immediate supervisor and Human Resources to obtain information. Contractors should contact their Contract Officer Representative to obtain information.

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).

There are several ways a Veteran or other beneficiary may access information about them. The Department of Veterans' Affairs has created the MyHealthEVet program to allow online access to their medical records. More information on this program and how to sign up to participate can be found online at https://www.myhealth.va.gov/index.html. Veterans and other individuals may also request copies of their medical records and other records containing personal data from the medical facility's Release of Information (ROI) office.

Employees should contact their immediate supervisor and Human Resources to obtain information. Contractors should contact their Contract Officer Representative to obtain information.

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.

Veteran: There are several ways a Veteran or other beneficiary may access information about them. The Department of Veterans' Affairs has created the MyHealthEVet program to allow online access to their medical records. More information on this program and how to sign up to participate can be found online at https://www.myhealth.va.gov/index.html. Veterans and other individuals may also request copies of their medical records and other records containing personal data from the medical facility's Release of Information (ROI) office.

Employees should contact their immediate supervisor and Human Resources to obtain information. Contractors should contact their Contract Officer Representative to obtain information.

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.

A Claimant can submit a request to a travel clerk to update profile information. Travel clerks are assigned tasks by the system to go to the system of record and make the requested modification(s). For updates to existing claims that have not been processed, the claimant can make those changes directly in BTSSS. For updates to existing claims that have been processed, claimants can work with a travel clerk directly to submit a corrective claim associated with the original, incorrect claim.

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.

Veterans are informed of the amendment process by many resources to include the terms and conditions which states: Right to Request Amendment of BT Information. You have the right to request an amendment (correction) to your BT information if you believe it is incomplete, inaccurate, untimely, or unrelated to your VA transportation needs. You must submit your request in writing, specify the information that you want corrected, and provide a reason to support your request for amendment. All amendment requests should be submitted to the facility Mobility Manager/BT Staff at the VHA health care facility that maintains your information. If your request for amendment is denied, you will be notified of this decision in writing and provided appeal rights. In response, you may do any of the following: • File an appeal •File a "Statement of Disagreement" • Ask that your initial request for amendment accompany all future disclosures of the disputed health information. Information can also be obtained by contacting the facility ROI office.

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.

N/A. Claimants when accessing the system view their information received from the system of record and used to process the claim. If the information is not correct, they are provided instructions for updating the information with the source record. BTSSS reads from systems of record but does not update to a system of record.

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 a Veteran may not be familiar with how to obtain access to their records or how to request corrections to their records

Mitigation: As discussed in question 7.3, the terms and conditions, which every Veteran reads and acknowledges prior to receiving BT claim services, discusses the process for requesting an amendment to one's records. The VHA staffs Release of Information (ROI) offices at facilities to assist Veterans with obtaining access to their medical records and other records containing personal information.

Section 8. Technical Access and Security

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

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

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

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

System Security Plan (SSP) outlines detailed access control requirements for the BTSSS system. Access to BTSSS working and storage areas is restricted to VA employees and contractors who must complete both the HIPAA, Information Security training, and Privacy Training. Specified access is granted based on the employee's functional category. Role based training is required for individuals with significant information security responsibilities to include but not limited to Information Security Officer (ISO), System Administrators, Network Administrators, Database Managers, Users of VA Information Systems or VA Sensitive Information. BTSSS access is requested using a VA Form 9957. This form will be completed and signed by the requester and their supervisor. Once signed it will be forwarded to a BT supervisor who will confirm the information provided in the form. After all the information, has been confirmed, BT supervisor will then grant, per the VA Form 9957, access to the specific facility's database.

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 only role that may fall outside of the VA is the Beneficiary Travel Claimants. That role can either be the veteran themselves, their caregiver or a VA employee that enters a claim on the Veteran's behalf

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.

The following table is a list of user roles, responsibilities, and access levels.

.

User Level	Role	Responsibilities	BTSSS Capabilities Access Level
Primary	Beneficiary Travel Claimants – Public User or VA representative	Represents a Veteran, Caregiver, or other party that is requesting Beneficiary Travel reimbursement.	– Enter/View/Edit profile; – Enter/View/Edit claims (reimbursement requests)

Primary	Travel Clerk - VA	Represents the person(s) responsible for assisting the Beneficiary Travel Claimant with issues with their claim. May need to process the claim manually in some cases when exceptions or special situations are encountered.	– Enter/View/Edit profile; – Enter/View/Edit claims (reimbursement requests); – Approve and deny reimbursement requests; – Trigger/Send notifications.
Primary	Business User - VA	Represents the person who utilizes the BTSSS data for business intelligence and reporting analysis.	- Run/View reports
Secondary	Application Super User	Represents the person who is engaged in report design/customization, workflow design/modification, and parameters configuration setup/modification.	– Enter/View/Edit profile; – Enter/View/Edit claims (reimbursement requests); – Approve and deny reimbursement requests; – Trigger/Send notifications. – Design/Edit Reports; – Design/Edit Workflow; – Enter/Edit Configurable parameters.
Secondary	System Administrator	Represents the person who has full control on the system.	Full control.

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.

Contracts are reviewed (annually) based on the contract guidelines by the appropriate contract authority (i.e., COR, Contracting Officer, Contract Review Committee). Per specific contract guidelines, contractors can have access to the BTSSS system only after completing mandatory information security and privacy training, VHA HIPAA training as well as the appropriate background investigation to include fingerprinting. Certification that this training has been completed by all contractors must be provided to the VHA employee who is responsible for the contract in question. In addition, all contracts by which contractors might access sensitive patient information must include a Business Associate Agreement which clarifies the mandatory nature of the training and the potential penalties for violating patient privacy.

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

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

All individuals and VA employees handling Veteran information will complete "Privacy and HIPAA Training" and "VA Privacy and Information Security Awareness and Rules of Behavior" TMS trainings. Individuals must also have a personal identification verification (PIV) badge reflecting they have a favorably adjudicated Security Agreement Check (SAC) and either a scheduled or favorably adjudicated background investigation at least at the National Agency Check with Inquiries (NACI)/Tier 1.

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

8.4a If Yes, provide: Yes, a conditional ATO was granted on December 3, 2020 and expires December 3, 2023. The FIPS 200 classification is Moderate

1. *The Security Plan Status:* APPROVED
2. *The System Security Plan Status Date:* 10/22/2022 It expired on DEC 16, 2021
3. *The Authorization Status:* APPROVED
4. *The Authorization Date:* 03 DEC 2020
5. *The Authorization Termination Date:* 03 DEC 2023
6. *The Risk Review Completion Date:* 13 NOV 2020
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.***

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)*

Microsoft Azure Government (MAG) VAEC

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.*

Details can be found in 150811-005R-Acceptance_of_FEDRAMP_Authorizations.pdf

According to Circular a130, anything that VA creates, collects, processes, maintains, disseminates, or disposes of by or for the federal government is considered federal information (VA data).

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.

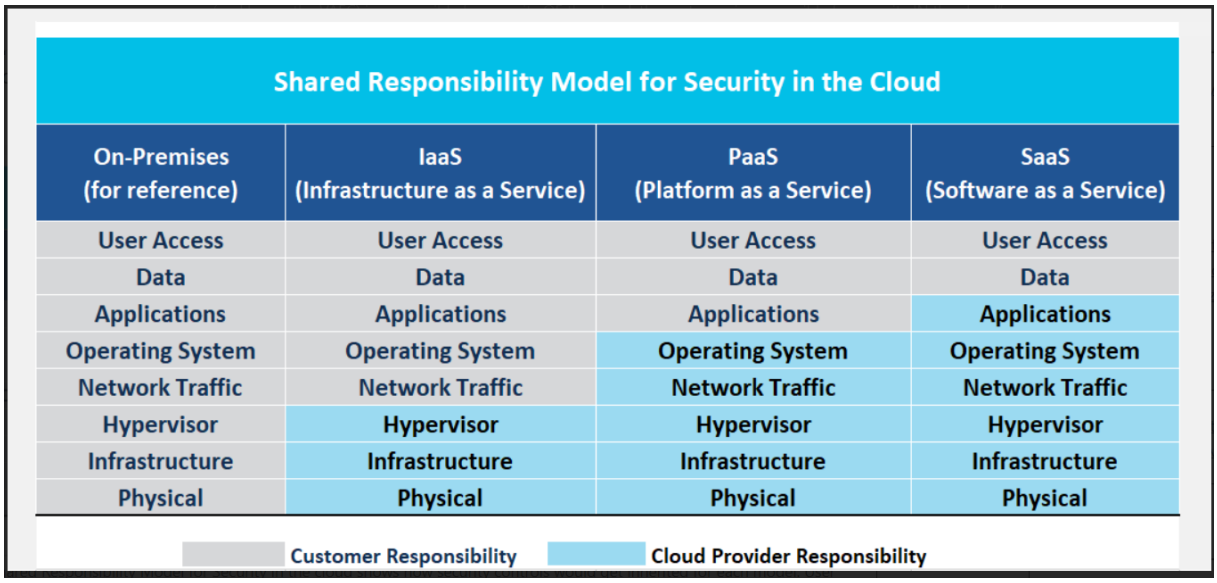
According to Circular a130, anything that VA creates, collects, processes, maintains, disseminates, or disposes of by or for the federal government is considered federal information (VA data).

While VA will ensure SaaS compliance with ATO requirements, SaaS vendor is primarily responsible for the security of their platform, which includes physical security, infrastructure and application security.

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.

Cloud-leveraged systems use a shared responsibility model where the accountability for security is split among the Cloud Service Provider (CSP), the VA enterprise, and the project team. VA project teams obtains an Authority-to-Operate or ATO with their application that only reviews the security controls that they are responsible for. The remaining security controls are "inherited" from the lower layer components which have already by tested by the Federal Risk and Authorization Management Program (FedRAMP) or VA OIT.



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).

Yes, when BTSSS requires and/or utilizes automation, the potential of moving PII/PHI information between BTSSS environment and Power BI repository exist.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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

Signature of Responsible Officials

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

SHIRLEY HOBSON

Digitally signed by SHIRLEY HOBSON
Date: 2022.11.08 12:06:34 -06'00'

Privacy Officer, Shirley Hobson

TERRY DZIADIK

Digitally signed by TERRY DZIADIK
Date: 2022.11.20 11:50:21 -05'00'

Information Systems Security Officer, Terry Dziadik

Tony L. Sines 167047

Digitally signed by Tony L. Sines 167047
Date: 2022.11.23 08:25:48 -06'00'

Information Systems Owner, Tony Sines

APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy, a Privacy Act notice on forms).

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices

The Veterans Health Information Systems and Technology Architecture (VistA) (79VA10), Privacy Act System of Records. Also, a notice was published prior to 1995 for the Individuals Submitting Invoices Vouchers for Payment-VA (13VA047).

HELPFUL LINKS:

Record Control Schedules:

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

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

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

National Archives (Federal Records Management):

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

VHA Publications:

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

VA Privacy Service Privacy Hub:

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

Notice of Privacy Practice (NOPP):

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices