Privacy Impact Assessment for the VA IT System called:

VETERANS-FACING SERVICES PLATFORM-VA.GOV(VFSP-VA.gov)

VACO

Office of the Chief Technology Officer

eMASS ID: #1027

Date PIA submitted for review:

10/11/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Gina Siefert	oitprivacy@va.gov	202-632-8430
Information System Security Officer (ISSO)	Griselda Gallegos	Griselda.Gallegos@va.gov	512-326-6037
Information System Owner	Christopher Johnston	Christopher.Johnston2@VA.gov	202-503-6267

Abstract

The Veterans-Facing Services Platform-VA (VFSP-VA.gov) is a set of online tools, services, and content that enables Veterans and their families to learn about, apply for, track, and manage their VA benefits through a publicly accessible website and mobile application.

Overview

VFSP-VA.gov is hosted within the VA Enterprise Cloud (VAEC) Amazon Web Services (AWS) GovCloud High environment, identified as a critical system within the VA (1-Bedrock system). VFSP-VA.gov is tracked with the VA Systems Inventory (VASI) as ID 2103.

VFSP-VA.gov is under the Veteran Experience Services (VES) portfolio and Digital Experience product line within the Office of Information and Technology (OIT).

VFSP-Va.gov is the place that Veterans, their families, and their caregivers go to access VA benefits and services. VFSP-VA.gov provides the following types of support and services: Health Care, Disability, Education, Burials & Memorials, Profile & Records, Pension & Fiduciary, Digital Notifications, and other VA benefit information.

Digital Experience and Chief Technology Office manages this system.

The system hosts www.va.gov (VA.gov), the official website of the U.S. Department of Veterans Affairs which sees about 15 million total visitors, and almost 2 million unique authenticated users each month. VA.gov is the home page and entry portal for Veterans, their spouses, dependents, survivors, and family caregivers

The information collected is needed to support Veterans Facing Services Platform-VA.gov (VFSP-VA.gov) program activities and electronic services.

VFSP-VA.gov maintains the following system interconnections:

- Appeals/Caseflow - Appeals status data is presented to users alongside disability claims data.
- ArcGIS – Provides facility data including geographical coordinates and other attributes.
- Benefit Gateway Service (BGS) - Provides information about Veterans' benefits and awards.
- Caregiver Record Management Application (CARMA) - Used to intake, track, and process Form 10-10CG submissions.
- Content Management System (CMS) – Editor-centered management of Veteran-centered content on VA.gov
- Debt Management Center (Debts) – Provides Veterans with information about debts they owe to the VA.
- Eligibility Office Automation System (EOAS) – For submitting preneed burial applications.
- Enrollment Service (ES) – For submitting health care applications.
- Enterprise Military Information Services (eMIS) - Provides information about Veterans' military service history.
- Enterprise Veteran Self-Service Portal Platform (EVSS) – Provides Veteran benefit data.

- GI Bill Comparison Tool Data Service (GIDS) – Provides institution profiles for GI Bill approved schools.
- ID.me – Provides login and identify verification services.
- Intake, Conversion and Mail Handling Services (ICHMS) – Provides information about Veteran benefit decision reviews and acts as a secure alternative to paper and fax submissions.
- Loan Guaranty (LGY) – Loan Guaranty Calculator and related services.
- Login.gov - Provides login and identify verification services.
- MuleSoft - Used to intake, track, and process Form 10-10CG submissions.
- My HealtheVet (MHV) - Provides login and identify verification services.
- Master Person Index (MPI) - Provides login and identify verification services.
- Search.gov - Provides indexed search results for federal government websites.
- VA: Health and Benefits App – Provides a subset of the functionality available on VA.gov.
- VA Notify – SMS and Email notification service for users interacting with VA.gov.
- VA Profile – Provides contact information and user profile data.
- VBS - Provide a Veteran's patient information for statements they owe to the VHA.
- Veterans Benefits Management System (VBMS) – Provides information about Veterans' benefits claims.
- VEText - Manages Veteran notifications, primarily healthcare related.
- VR&E CMS - Used to submit VA form 21-1900.

VFSP-VA.gov is hosted within VAEC AWS GOVCLOUD HIGH and connected to the broader VA network and the Internet through the Trusted Internet Connection (TIC). The majority of the VFSP-VA.gov production environment is hosted within a dedicated AWS Virtual Private Cloud (VPC), with some Minor Applications residing in their own dedicated VPC or separate AWS Accounts.

Veterans Facing Services Platform-VA.gov (VFSP-VA.gov) is a moderate system operating under Authority to Operate (ATO) granted on January 7, 2021, through January 7, 2024.

The following security documents are available to system stakeholders on a need-to-know basis:

1. The Security Plan Status, - Active
2. The Security Plan Status Date - 11/27/2020
3. The Authorization Status- Active
4. The Authorization Date - 01/07/2021
5. The Authorization Termination Date – 01/07/2024
6. The Risk Review Completion Date – 01/07/2021
7. The FIPS 199 classification of the system (LOW/MODERATE/HIGH) - Moderate.

VFSP-Va.gov falls under SORN 58VA21/22/28 and its applicable retention period and the SORN does not require amendment.

This PIA will result in no change to business processes.

This PIA will result in no change to technology.

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?

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)

The information needed to support Veterans Facing Services Platform-VA.gov (VFSP-VA.gov) program activities and electronic services includes:

- Electronic Data Interchange Personal Identifier (EDIPI)
- Universally Unique Identification (UUID)
- Place of Birth City and State
- Claim number
- Alias Name
- Date of Death
- User ID
- VA File Number

PII Mapping of Components

VFSP-Va.gov consists of 20 key components. Each component has been analyzed to determine if any elements of that component collect PII.

1.2 What are the sources of the information in the system?

The information in the system is gathered from a number of sources including but not limited to:

- Veteran
- Veteran dependents
- Veteran caregivers
- Military Records (Department of Defense)
- Physicians and other medical personnel
- Educational entities
- VA Benefits
- ID.me
- HCA: User-entered information.
- EBA: User-entered information.
- Pension Application: User-entered information
- Burial Application: User-entered information
- Log-in: New/existing users submit information for verification and authentication. ID.me and MVI-PSM return validated information.
- Claim Status: Existing claim information/status is retrieved from EBN. Users can submit additional evidence in support of their existing claim.
- VA Letters: Existing letter information is retrieved from EBN.
- Post 9/11 Enrollment Status: Existing status information is retrieved from EBN.
- Secure Messaging: New/replied messages are submitted via the user. Responses are retrieved from MHV.
- Prescription Refill: Users click 'yes' if they'd like to refill. Existing prescription information is retrieved from MHV.
- Veteran Information: Existing military information is retrieved from VRS eMIS.
- Caseflow: User-entered information.
- EOAS: User-entered information.
- VA: Health and Benefits App: User Entered Information.
- HCA: User-entered information.
- EBA: User-entered information.
- Pension Application: User-entered information
- Burial Application: User-entered information
- Log-in: New/existing users submit information for verification and authentication. ID.me and MVI-PSM return validated information.
- Claim Status: Existing claim information/status is retrieved from EBN. Users can submit additional evidence in support of their existing claim.
- VA Letters: Existing letter information is retrieved from EBN.
- Post 9/11 Enrollment Status: Existing status information is retrieved from EBN.
- Secure Messaging: New/replied messages are submitted via the user. Responses are retrieved from MHV.
- Prescription Refill: Users click 'yes' if they'd like to refill. Existing prescription information is retrieved from MHV.
- Veteran Information: Existing military information is retrieved from VRS eMIS.
- Caseflow: User-entered information.
- EOAS: User-entered information.
- Mobile App: User Entered Information.
- The Content Management System (CMS)
- VANotify: User Entered Information.
- VA: Health and Benefits. User Entered Information.

1.3 How is the information collected?

- HCA: Users enter data into the required fields within the healthcare application.
- EBA: Users enter data into the required fields within the education application.
- Pension: Users enter data into the required fields within the pension application.
- Burial: Users enter data into the required fields within the burial application.
- Log-in: New/existing users submit enter data into the required fields for verification and authentication.
- Claim Status: Users can submit additional evidence in support of their existing claim.
- VA Letters: The system retrieves the information from EBEN.
- Post-9/11 GI Bill Enrollment Status: The system retrieves the information from EBEN.
- Secure Messaging: New/replied messages are submitted via the user.
- Prescription Refill: The system retrieves any existing prescription information from MHV. If the user would then like to refill a prescription, they click 'Yes'. That information is then sent back to MHV, which process the prescription refill request.
- Veteran Information: The system retrieves the Veteran's DoD Authoritative Military Service Record (AMSR) from VRS eMIS.
- Case flow: The system retrieves any existing appeal information from Case flow.
- EOAS: Users enter data into the required fields within the application.
- VA Notify: Retrieves the data from VA profile.
- VA: Health and Benefits App: Retrieves the data from VA profile.
- CMS No PHI or PII is collected, stored, or shared by this application.

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

Any information entered by the Veteran is considered accurate, and therefore no additional checks are performed. However, validations built into the application on VA.gov will only allow data to be entered that matches the field criteria. For example: A Veteran would be unable to enter a 10-digit number in the field designated for a 9-digit Social Security Number. Information retrieved and displayed from existing VA systems is assumed to be accurate.

Validations built into the application on VA.gov will only allow data to be entered that matches the field criteria. For example: A Veteran would be unable to enter a 10-digit number in the field designated for a 9-digit Social Security Number. Information retrieved and displayed from existing VA systems is assumed to be accurate.

Because information entered by the Veteran is considered accurate, it is not regularly checked for accuracy.

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

- Healthcare Application (HCA) formerly (VOA) 10-10EZ form is now part of VFSP- VA.gov under 38 U.S.C. Sections 1705, 1710, 1712, and 1722 in order for VA to determine your eligibility for medical benefits.
- Education Benefits Applications (EBA), which replaces the VONAPP/22-1990 form with a web- based form that Veterans use to apply for education benefits, under GI Bill chapter 33 of title 38, U.S. Code, Chapter 30
- Claim Status, which is connected to eBenefits (EBN), provides users with the ability to view/track the status of their disability claims, as well as submit new disability claims, under Title 38, United States Code, Section 5106.
- VA Letters, for eBenefits (EBN), provides users with the ability to generate and download letters from VA that certify information about their military service and earned benefits: Title 38, United States Code, Section 5106.
- Post-9/11 GI Bill Enrollment Status, for eBenefits (EBN), provides users with the ability to track the status of their Post-9/11 GI Bill Entitlement: Title 38, United States Code, Section 5106
- Secure Messaging, which is connected to My HealtheVet (MHV), provides users with the ability to exchange messages with their healthcare providers, under E-government Act of 2002 (44 U.S.C. § 208(b)) and VA Directive 6508.
- Prescription Refill: —VA'' 130VA19 as set forth in the Federal Register 193 FR 59991, is based upon the Privacy Act of 1974, 5 U.S.C. 552a(e). The authority for maintenance of the system is Title 38, United States Code, §501."
- Caseflow (Appeal-Status): Title 38 United States Code 5701
- EOAS: Title 38 United States Code 5701
- MHV Account Management: E-government Act of 2002 (44 U.S.C. § 208(b)) and VA Directive 6508.
- U.S.C. section 501(a) and chapters 11, 13, 15, 18, 23, 30, 31, 32, 33, 34, 35, 36, 39, 51, 53, and 55. SSNs
- are used to establish the Veteran's eligibility for education benefits. (Education applications 22- 1990, 22-1990, 22-1995, 22-1990N, 22-5490, 22-5495, Pension Application 21P-527EZ, Burial Application 21P-53.
- Veteran Information: Title 38, United States Code, Section 5106, and Title 38 United States Code 5701. Title 38, United States Code, section 81 11 (38 U.S.C. 5811 I), titled "Sharing of Department of Veterans Affairs and Department of Defense Health Care Resources. "Title 10, United States Code, section 1104 (10 U.S.C.5 1104), titled "Sharing of Resources with the Department of Veterans Affairs," which incorporates Title 31, United States Code, section 1535 (31 U.S.C. 51 535), titled "Agency Agreements," also known as the "Economy Act."

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Privacy Risk: A risk would be a compromise of VFSP-VA.gov that leads to interception and stealing of personal information.

Mitigation: The VFSP-Va.gov Platform, hosted in AWS GovCloud, adheres to stringent data protection standards, utilizing FIPS 140-2 compliant endpoints. The Platform and its applications ensure a comprehensive encryption model, safeguarding data in transit, at the application level, and when at rest. During data transit, encryption is facilitated through Transport Layer Security (TLS) protocols, using digital certificates. Within the application, AES-GCM-256 is used with rotating cryptographic keys. Keys are stored and rotated using AWS Key Management Service (KMS). When data is at rest, AWS Relational Database Service uses AES-256 to encrypt the Postgres Database used by the backend application.

Section 2. Uses of the Information

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

VFSP-Va.gov is an intermediary system that transmits information to the system of record. Information is sent to other VA systems for processing. Therefore, the usage of these data elements by VFSP-Va.gov is transmittal. This is how the data elements are used:

- EBA: Data collected is used in the determination of education benefits eligibility.
- Pension: Data collected is used in the determination of pension benefits eligibility.
- Burial: Data collected is used in the determination of burial benefits.
- Claim Status: Data collected is used to provide additional evidence in support of a VA disability claim.
- VA Letters: Benefit letters are passed through to the user.
- Post-9/11 GI Bill Enrollment Status: Entitlement status is passed through to the user.
- Secure Messaging: Data collected is used to communicate with healthcare providers.
- Prescription Refill: Data collected is used to refill existing prescriptions.
- Blue Button: Health records collected are passed through to the user.
- Veteran Information: Military records are passed through to the user.
- EOAS: Data collected is checked and passed through to Burial Operations Support System (BOSS)
- Caseflow: Data collected is used for automated error checking.
- VANotify: Send notification to Veterans and their families and the people who support them internal to VA and external to VA.
- VA: Health and Benefits App: To route additional traffic to va.gov.
- Big Query: To transmit data of Veterans users.

2.2 What types of tools are used to analyze data and what type of data may be produced?

This application does not process or analyze data submitted.

2.3 How is the information in the system secured?

The VFSP-Va.gov Platform, hosted in AWS GovCloud, adheres to stringent data protection standards, utilizing FIPS 140-2 compliant endpoints. The Platform and its applications ensure a comprehensive encryption model, safeguarding data in transit, at the application level, and when at rest. During data transit, encryption is facilitated through Transport Layer Security (TLS) protocols, using digital certificates. Within the application, AES-GCM-256 is used with rotating cryptographic keys. Keys are stored and rotated using AWS Key Management Service (KMS). When data is at rest, AWS Relational Database Service uses AES-256 to encrypt the Postgres Database used by the backend application. This is also used to protect SSN data.

The user community for Department of Veterans Affairs' System and ID.me are Veterans, their dependents, the designated representatives, and VA Business Partners.

Identification and Authentication - User Access control is managed by strong authentication methods and must be

assigned on the "Least Privilege" Principal. VA utilizes “two-factor authentication” for general users. A separate token and non-mail enabled account is required for users who require elevated privileges on IT systems.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

VFSP-Va.gov is responsible for provisioning production access to the AWS (Amazon Web Services) console for Va.gov. VFSP-VA.gov infrastructure and data (including Vets API and related databases) is hosted in AWS GovCloud. This account is shared amongst several teams and changes to resources in this account affect various services. When an individual requests production access, a review is completed and approved by the Contract Officer Representative (COR) to validate that the individual has been both vetted by VA and truly requires elevated privileges based on their roles and responsibilities on VFSP-Va.gov.

VFSP-VA.gov adheres to National Institute of Standards and Technology (NIST) Special Publication 800-53, FedRAMP and VA 6500 directives for moderate impact systems to cover security-related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and information processed, stored, and transmitted by those systems.

The security-related areas include access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; system and information integrity; and privacy.

All access to VFSP-VA.gov infrastructure is monitored and recorded via AWS CloudTrail, which is a service that enables governance, compliance, operational auditing, and risk auditing of AWS accounts. Access management procedures are documented and made available on a need-to-know basis. Access requires manager approval and is recorded.

VFSP-Va.gov has dedicated engineering and security personnel responsible for implementing, assuring, communicating, monitoring, and auditing safeguards for PII. This responsibility is shared with Program and Engineering Leadership, the Contract Officer Representatives (CORs), the Information System Owner (ISO), and the Information System Security Officer (ISSO). Additionally, guidance and support are provided by the VA OIT Privacy Service to ensure controls and safeguards are implemented in accordance with VA’s standards and requirements.

Section 3. Retention of Information

3.1 What information is retained?

All data elements listed in 1.1 are retained by the system.

3.2 How long is information retained?

The following components retain data (cached) only for 1 hour upon a user initiating an authenticated session

within VFSP-VA.gov.

- Log-in (MVI-PSM)
- Veteran Information (VRS eMIS)

The following components retains data only for 24 hours upon a user initiating an authenticated session within VFSP-VA.gov*:*

- Claim Status
- VA Letters
- Post-9/11 GI Bill Enrollment Status
- EOAS

The following information is retained for 60 days:

EBA:

- Completed forms (all data listed in 1.1)
- Form completion logs (stored anonymously) containing:
    - Date Submitted
    - Region
    - Time Submitted
    - Benefit Selected

The following information is retained permanently:

- Log-in (ID.me): All data listed in 1.1 except for a photo of a government-issued ID which is collected but then immediately destroyed once a user's identity has been verified.

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

VFSP-Va.gov falls under SORN 58VA21/22/28 and its applicable retention period.

ID.me's federal accreditation under GSA's FICAM program addresses records retention requirements for ID.me to comply with federal standards. For LOA 3 issuance, ID.me must retain records for at least five (5) years. At the end of the retention period, ID. me will follow VFSP-VA.gov contract (VA118-16-C-1000) agreements.

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

All data cached/stored by VA.gov is deleted upon reaching the deletion timeframes as specified in 3.2. Log-in and EBA operate on time-based deletion rules, while Claim Status is a CRON job (a time-based job scheduler in Unix-like computer operating systems) that programmatically triggers a cleanup script.

With respect to ID.me, once a user has an ID.me wallet, they have one, regardless of if a VFSP- VA.gov contract exists or not. If the contract is terminated, a user with an ID.me wallet would not be able to login at VA.gov, but their data at ID.me would still exist. The data collected by ID.me is the responsibility of ID.me and will eliminate SPI data based on VFSP-VA.gov contract (VA118-16-C- 1000) and VA Interconnection Security Agreement Memorandum of Understanding (ISA MOU) and the use of the information from VA.gov is simply for verification of the user account.

3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?

Veterans Facing Services Platform-VA.gov (VA.gov) does NOT use PII/PHI for testing information systems or pre-production prior to deploying to production.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Privacy Risk: Veterans Facing Services Platform-VA.gov (VA.gov) only retains data long enough (1 hour) to ensure a consistent user experience.

Mitigation: Veterans Facing Services Platform-VA.gov (VA.gov) only retains data long enough (1 hour) to ensure a consistent user experience, allowing authenticated users access to the information retrieved from the various applications outlined within.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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?

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***
Veteran Benefit Administration - The Image Management System/Secure File Transfer Protocol (TIMS/SFTP)	Used to apply for education benefits	• Name • Mother's Maiden Name • Social Security Number • Benefits Information • Claims Decision • DD- 214 • Date of Birth • Place of Birth City	Data entered into the form fields by the Veteran is encrypted (via SSL). Data transmitted to TIMS via SFTP across our NSOC-monitored, site-to-site VPN connection.

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*
		• Place of Birth State • Address • Phone Number • Gender	
Veteran Benefit Administration - MVI-PSM	Access to VA Healthcare for Veterans	• First Name • Middle Name • Last Name • Prefix • Suffix • Date of Birth • Place of Birth City • Place of Birth State Address • Phone Number • Alias • Mother's Maiden Name • SSN	Data entered into the form fields by the Veteran is encrypted (via SSL). Data transmitted to TIMS via SFTP across our NSOC- monitored, site-to-site VPN connection
Veteran Health Administration - My HealtheVet (MHV)	Access to VA Healthcare for Veterans	• User ID • Prescription Id • Email Address • Name • Spouse's Name • Childs Name • Mother's Maiden Name • Gender: M/F • Birth date • Spouses date of birth • Child's date of birth (mm/dd/yyyy) • Are you Spanish, Hispanic or Latino	• Data entered into the form fields by the Veteran is encrypted (via SSL). Data transmitted to MHV across our NSOC-monitored, site-to-site VPN connection
Veteran Benefit Administration - eBenefits	Manage Veteran benefits	• First Name • Middle Name • Last Name • Prefix • Suffix • Date of Birth • Place of Birth City • Place of Birth State	• Data entered into the form fields by the Veteran is immediately encrypted (via SSL) and transmitted to benefits. Data

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*
		• Address • Phone Number	transmitted from benefits across our NSOC-monitored, site- to-site VPN connection
Veteran Health Administration - Health Care Application (HCA)	Apply for healthcare benefits	• Name L/F/M • Spouse's Name L/F/M • Childs Name L/F/M • Mother's Maiden Name • Gender: M/F • Birth date • Spouses date of birth • Child's date of birth (mm/dd/yyyy) • Are you Spanish, Hispanic or Latino?	• Data entered into the form fields by the Veteran is encrypted (via SSL). Data transmitted to HCA across our NSOC-monitored, site to-site VPN connection
Veteran Benefit Administration - Veteran Record Service (VRS) eMIS	Linking Veteran's DoD service history with the VA system	• Electronic Data Interchange Personal Identifier (EDIPI) • Integrated Control Number (ICN)	• Data transmitted to VRS eMIS across our NSOC-monitored, site-to-site VPN connection
Veteran Benefit Administration - Education Benefit Application (EBA)	Apply for education benefits	• First Name • Middle Name • Last Name • Social Security Number • Date of Birth • Gender	• Data entered the form fields by the Veteran is encrypted (via SSL).Data transmitted to EBA across our NSOC-monitored, site-to-site VPN connection.

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*
Veteran Benefit Administration - Caseflow (Appeals Status)	Manage appeal caseflow	• SSN • Date of Birth • Gender	• Data entered into the form fields by the Veteran is encrypted (via SSL). Data transmitted to EBA across our NSOC-monitored, site-to-site VPN connection.
Veteran Benefit Administration - Eligibility Office Automation System (EOAS)	Manage Veteran burial benefit eligibility	• Email • Phone number • Applicant relationship to claimant • Address • City • Country code • Postal zip • State • First name • Last name	• Data entered into the form fields by the Veteran is encrypted (via SSL). Data transmitted to EBA across our NSOC-monitored, site-to-site VPN connection
Veteran Benefit Administration – VIC (Veteran ID Card)	Manage Veteran ID card applications	• First Name • Last Name • Maiden Name • Middle Name • Address	• Data Sent from VFSP-Va.gov to internal VA Salesforce environment
Veteran Benefit Administration - GI Bill Feedback Tools (GIBFT)	Manage GI Bill feedback	• First Name • Middle Name • Last Name • Social Security Number • Date of Birth • Gender	• Data sent from VFSP-Va.gov to EBA
Va.gov – VA Notify	Allows consumer services to send emails and texts to their user	• Name • Spouse's Name • Child's Name • Mother's Maiden Name	• Data sent from VFSP-Va.gov to VANotify.

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*
		• Phone Number • VA File Number • Date of Birth	
Va.gov - VA: Health and Benefits Mobile App	Allows Veterans to manage a subset of benefits using a mobile platform	• Mobile Phone Number • Country Code • ID Type (Driver's License, Passport, State ID) • Area Code • State • City • Gender	• Data sent from VFSP-Va.gov to Va Mobile App
Va.gov - CMS	Manages content across VA.gov/Platform products	• Name L/F/M Spouse's • Name L/F/M Child's • Name L/F/M • Mother's Maiden	• Veterans do not enter data into the CMS. CMS data is entered by VA staff only.
Va.gov – Big Query	Storage of VA.gov analytic data	• Name L/F/M • Spouse's Name L/F/M • Child's Name L/F/M • Mother's Maiden	• Data sent from VFSPVA.gov to Big Query

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Privacy Risk: There is a risk that data could be shared with an inappropriate VA organization or program or, sensitive data could be accessed by unauthorized individuals during transmission.

Mitigation: Data entered into the form fields by the Veteran is encrypted in-transit via SSL across our NSOC- monitored, site-to-site VPN connection. User-entered data may be cached (stored temporarily) for up to 1 hour and is encrypted at-rest.

The validity of the data is verified during transmission and the validity of the form is checked against the unique identifier that was assigned to the session when it was initially presented to the Veteran.

The Department of Veterans Affairs takes safeguarding and protecting information very seriously. Causing any harm to the security or the information on Veterans Facing Services Platform-VA.gov is forbidden by

law. It is against the law to threaten, attempt, or try to change this system. It is against the law to prevent access to this system. It is also against the law to access data that does not belong to you. These actions violate Federal laws and may result in criminal, civil, or administrative penalties. These Federal laws include 18 U.S.C. 1030 (Fraud and Related Activity in Connection with Computers) and 18 U.S.C. 2701 (Unlawful Access to Stored Communications)

Section 5. External Sharing/Receiving and Disclosure

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?

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***
ID.me	Login information for ID.me	• ID.me Universally Unique Identification (UUID) • First Name • Middle Name • Last Name • Gender • Birth Date • Social Security • Zip Code	• VFSP-gov redirects to eAuth using SAML and HTTPS which redirects users to ID.me to authenticate and returns the validated authentication back through eAuth and then to VFSP-Va.gov using SAML and HTTPS	• MOU and Information is covered and approved per the agreement set forth in the vfsp-va.gov contract.
Login.gov	Login information for Login.gov	• Login.gov Universally Unique Identification (UUID) • First Name • Middle Name • Last Name	• VFSP-gov redirects to eAuth using SAML and HTTPS which redirects users	• MOU and Information is covered and approved per the

		• Gender • Birth Date • Social Security • Zip Code	to ID.me to authenticate and returns the validated authentication back through eAuth and then to VFSP-Va.gov using SAML and HTTPS	agreement set forth in the vfsp-va.gov contract.

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

Privacy Risk: There is a risk that unauthorized individuals could access data during transmission.

Mitigation: Data entered into the form fields by the Veteran is encrypted in-transit via SSL across our NSOC- monitored, site-to-site VPN connection. User-entered data may be cached (stored temporarily) for up to 1 hour and is encrypted at-rest.

The validity of the data is verified during transmission and the validity of the form is checked against the unique identifier that was assigned to the session when it was initially presented to the Veteran. The Department of Veterans Affairs takes safeguarding and protecting information very seriously.

Causing any harm to the security or the information on VA.gov is forbidden by law. It is against the law to threaten, attempt, or try to change this system. It is against the law to prevent access to this system. It is also against the law to access data that does not belong to you. These actions violate Federal laws and may result in criminal, civil, or administrative penalties. These Federal laws include 18 U.S.C. 1030 (Fraud and Related Activity in Connection with Computers) and 18 U.S.C. 2701 (Unlawful Access to Stored Communications).

Data passed from ID.me is encrypted in-transit via SSL and sent across our NSOC-monitored, site- to-site VPN connection.

Section 6. Notice

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?

Users are provided with a notice which includes the below:

"I understand that pursuant to 38 U.S.C. Section 1729 and 42 U.S.C. 2651, the Department of Veterans Affairs (VA) is authorized to recover or collect from my health plan (HP) or any other legally responsible third party for the reasonable charges of nonservice-connected VA medical care or services furnished or provided to me. I hereby authorize payment directly to VA from any HP under which I am covered (including coverage provided under my spouse's HP) that is responsible for payment of the charges for my medical care, including benefits otherwise payable to me or my spouse. Furthermore, I hereby assign to the VA any claim I may have against any person or entity who is or may be legally responsible for the payment of the cost of medical services provided to me by the VA. I understand that this assignment shall not limit or prejudice my right to recover for my own benefit any amount in excess of the cost of medical services provided to me by the VA or any other amount to which I may be entitled. I hereby appoint the Attorney General of the United States and the Secretary of Veterans' Affairs and their designees as my Attorneys-in-fact to take all necessary and appropriate actions in order to recover and receive all or part of the amount herein assigned. I hereby authorize the VA to disclose, to my attorney and to any third party or administrative agency who may be responsible for payment of the cost of medical services provided to me, information from my medical records as necessary to verify my claim. Further, I hereby authorize any such third party or administrative agency to disclose to the VA any information regarding my claim. By submitting this application, you are agreeing to pay to the applicable VA copays for treatment or services of your NSC conditions as required by law. You also agree to receive communications from VA to your supplied email or mobile number."

This Privacy Impact Assessment (PIA) also serves as notice of the Veterans-Facing Services Platform-Va.gov. 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 agencies. VA System of Record Notices (SORNs) which are published in the Federal Register and available online: 58VA21/22/28/86FR61858; Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA. (11/8/2021) https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

It reinforces to the user that any information they enter form-fields on the application will be collected. Please see Appendix A 6A for an example.

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

Information is required to determine eligibility. Providing information is a basic assumption and requirement of any application, as an application is a collection of information in order to determine eligibility.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

The information submitted is used to determine eligibility for VA healthcare or education benefits. The application indicates consent to use the information to decide for eligibility for healthcare or education benefits.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Privacy Risk: There is a risk that individuals are unaware that their information is being collected and is not used for the purpose it was collected as a result of insufficient notice provided to the Veterans.

Mitigation: Individuals/Veterans are provided with a notice which includes the below:

> "I understand that pursuant to 38 U.S.C. Section 1729 and 42 U.S.C. 2651, the Department of Veterans Affairs (VA) is authorized to recover or collect from my health plan (HP) or any other legally responsible third party for the reasonable charges of nonservice-connected VA medical care or services furnished or provided to me. I hereby authorize payment directly to VA from any HP under which I am covered (including coverage provided under my spouse's HP) that is responsible for payment of the charges for my medical care, including benefits otherwise payable to me or my spouse. Furthermore, I hereby assign to the VA any claim I may have against any person or entity who is or may be legally responsible for the payment of the cost of medical services provided to me by the VA. I understand that this assignment shall not limit or prejudice my right to recover for my own benefit any amount in excess of the cost of medical services provided to me by the VA or any other amount to which I may be entitled. I hereby appoint the Attorney General of the United States and the Secretary of Veterans' Affairs and their designees as my Attorneys-in-fact to take all necessary and appropriate actions in order to recover and receive all or part of the amount herein assigned. I hereby authorize the VA to disclose, to my attorney and to any third party or administrative agency who may be responsible for payment of the cost of medical services provided to me, information from my medical records as necessary to verify my claim. Further, I hereby authorize any such third party or administrative agency to disclose to the VA any information regarding my claim. By submitting this application, you are agreeing to pay to the applicable VA copays for treatment or services of your NSC conditions as required by law. You also agree to receive communications from VA to your supplied email or mobile number."

The applicant is required to click a check box next to a statement that says, "I have read and accept the privacy policy" indicating that they have read and accept the Privacy Policy displayed above the statement before proceeding with the application.

Step eight of the application process presents a note to the applicant that states, "According to Federal Law, there are criminal penalties, including a fine and/or imprisonment for up to 5 years, for withholding information or for providing incorrect information. (See 18 U.S.C. 1001). The applicant must click the check box next to, "I have read and accept the privacy policy", indicating, once again, that they have read and accept the previously presented Privacy Policy before applying. If an applicant attempts to submit prior to clicking the check box, a red warning is displayed that states, "The check box must be checked before an applicant can submit an application."

The VA abides by NIST standards and VA Handbook 6500 directives on how PII/PHI should be encrypted and transmitted from one system to another, the connection between VA.gov and the ES conforms to these standards. Data entered into the form fields by the Veteran is encrypted in-transit via SSL across our NSOC- monitored, site-to-site VPN connection. User-entered data may be cached (stored temporarily) for up to 1 hour and is encrypted at-rest

Section 7. Access, Redress, and Correction

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

Veterans wishing to gain access to the information they submitted through VA.gov will request their records using the procedure in place for the various VA minor systems identified within Va.gov.

System is not exempt from the Privacy Act.

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

Veterans wishing to change the information they submitted through VA.gov will request the change using the procedure in place for the various VA minor systems identified within Va.gov.

The SORN 58VA21/22/28 contains procedures for how individuals can correct inaccurate or erroneous information: 58VA21/22/28/86FR61858; Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA. (11/8/2021) https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

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

The validity of the data is verified during transmission and the validity of the form is checked against the unique identifier that was assigned to the session when it was initially presented to the Veteran. The Department of Veterans Affairs takes safeguarding and protecting information very seriously.

Causing any harm to the security or the information on Veteran's Online Application (VOA) is forbidden by law. It is against the law to threaten, attempt, or try to change this system. It is against the law to prevent access to this system. It is also against the law to access data that does not belong to you. These actions violate Federal laws and may result in criminal, civil, or administrative penalties.

These Federal laws include 18 U.S.C. 1030 (Fraud and Related Activity in Connection with Computers) and 18 U.S.C. 2701 (Unlawful Access to Stored Communications. Individuals are responsible for ensuring that their information being inputted is accurate and correct to the best of their knowledge. In the event a user realizes the information is inaccurate or needs to be updated, the steps to be taken to update or correct the error can be found at https://www.va.gov/resources/managing-your-vagov-profile/ or https://www.va.gov/change-address/

The SORN 58VA21/22/28 contains procedures describing how individuals can correct their information. 58VA21/22/28/86FR61858; Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA. (11/8/2021) https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

7.4 If no formal redress is provided, what alternatives are available to the individual?

Not Applicable, as formal redress is provided.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Privacy Risk: Information provided via VA.gov may be inaccurate.

Mitigation: Any conflicts between the data provided by the Veteran and the data held by the respective VA systems are resolved through those respective system's procedures of contacting the Veteran to verify the correct data and resolve the conflict.

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?

VFSP-VA.gov is primarily a publicly accessible website providing general content for anonymous use. Components of VFSP-VA.gov that provide individualized content, such as a Veteran's claim status or list of prescription medicine, do so by retrieving information directly from the internal VA systems that already exist such as MHV and eBenefits. As such, the determination of which components can be accessed by which users is wholly within the purview of the underlying systems. For example, a user of VFSP-VA.gov *cannot* use VFSP-VA.gov to display information retrieved from MHV without having an active MHV account.

Any user registered with ID.me may login to VFSP-VA.gov but without additional authorization a user will not receive access to custom resources. Once logged in, VA.gov *attempts* to validate the user exists in the VA MVI. If the user exists in the MVI, VA.gov receives additional information relevant to the user, specifically the correlation IDs for that user to access VA systems. The combination of a logged-in user, a validated identity, and internal VA correlation IDs dictates the access granted to a specific user. For example, a user of VA.gov cannot use VA.gov to display information retrieved from MHV without having an MHV account, an LOA3 identity-proofed account at ID.me, and an MHV correlation ID retrieved from MVI.

Besides Digital Experience Product Office (DEPO) users, only users from United States Digital Service (USDS), Oddball and Ad Hoc have access to the source code, system, and datastores. No users (including DEPO, USDS, Oddball, Ad Hoc) can access data on behalf of another individual user. Access to the underlying application and infrastructure is enforced through identity and access management procedures such as:

- Identity and Access Management (IAM)
  - Creating individual accounts for those who require access to the virtual infrastructure or Application Programming Interfaces (API's) or use IAM federation from Veteran's Affairs identity management system.
  - Use groups or roles to assign permissions to IAM users and VA.gov.

- Enable multi-factor authentication for all IAM users.
- Use roles for applications that run on Elastic Compute Cloud (EC2) instances.
- Delegate by using roles instead of sharing credentials.
- Rotate credentials regularly.
- Store Secure Shell (SSH) keys securely to prevent disclosure, and promptly replace lost or compromised key.

- Application Security Groups
- VFSP- VA.gov has created AWS security groups associated with VPC's to provide full control over inbound and outbound traffic.
- A specific set of Virtual Private Clouds (VPCs) (development, staging, and production) have been implemented. All VPCs have public and private subnets used to separate and control IP address space within each individual VPC.

Requests for access is authorized via signature of the VFSP-VA.gov System Owner and the VFSP-VA.gov ISSO.

Roles:

- Software Developers may make changes to the underlying application, infrastructure, and content. Anonymous Users may read content and submit forms to the VA that do not require authentication or authorization
- LOA1 Users have registered with ID.me but not completed the identity proofing process; they have no
- ability to view information different than Anonymous Users
- LOA3 Users have registered with ID.me and completed the identity proofing process. These users have authorization to attempt to connect to internal VA systems and retrieve information specific to them, if correct information exists in MVI to make the correlation with these systems.

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?

Veterans Facing Services Platform-VA.gov (VFSP-VA.gov) provides security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users, when required by system changes, and at least annually thereafter via the VA OIT Talent Management System (TMS). All users are required to sign a Non-Disclosure Agreement as part of the training and onboarding.

Veterans Facing Services Platform-VA.gov (VFSP-VA.gov) awareness training program commences with the VA OIT TMS training, *VA Privacy and Information Security Awareness and Rules of Behavior (ROB), number 10176*. Following the training, all information system users will be able to identify the types of information that must be carefully handled to protect privacy; recognize the required information security practices, legal requirements, and consequences and penalties for non-compliance; and explain how to report incidents. The awareness program is consistent, updated and deployed for all employees regularly.

Personnel will also receive information on recognizing and reporting potential indicators of insider threat (for example, in new staff orientation and contractor on-boarding)

Veterans Facing Services Platform-VA.gov (VFSP-VA.gov) role-based security training consists of the

following VA OIT TMS training.

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

Digital Experience Product Office at VA (DEPO) provides security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users, when required by system changes, and at least annually thereafter via the VA OIT Talent Management System (TMS).

DEPO awareness training program commences with the VA OIT TMS training, VA Privacy and Information Security Awareness and Rules of Behavior (ROB), number 10176. Following the training, all information system users will be able to identify the types of information that must be carefully handled to protect privacy; recognize the required information security practices, legal requirements, and consequences and penalties for non- compliance; and explain how to report incidents. The awareness program is consistent, updated and deployed for all employees regularly.

Personnel will also receive information on a recognizing and reporting potential indicators of insider threat (for example, in new staff orientation and contractor on-board

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

1. The Security Plan Status – **Active**
2. The Security Plan Status Date – **03/03/2023**
3. The Authorization Status – **Active**
4. The Authorization Date - **01/07/2021**
5. The Authorization Termination Date – **01/07/2024**
6. The Risk Review Completion Date – **01/07/2021**
7. The FIPS 199 classification of the system (LOW/MODERATE/HIGH) - **Moderate**.

Veterans Facing Services Platform-VA.gov (VFSP-VA.gov) is a moderate system operating under Authority to Operate (ATO) granted on January 7, 2021, through January 7, 2024. Security documents are available to va.gov's system stakeholders on a need-to-know basis.

Section 9 – Technology Usage

9.1 Does the system use cloud technology? If so, what cloud model is being utilized?

Yes.VFSP-Va.gov is hosted within the VA Enterprise Cloud (VAEC) Amazon Web Services (AWS) GovCloud High environment. This FedRAMP approved, FISMA high environment provides Infrastructure as a Service (IaaS) capabilities to VFSP-Va.gov.

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).

Please refer to the VAEC office for a copy of the copy of the contract between AWS (VAEC AWS

GOVCLOUD HIGH) and VFSP-Va.gov.

9.3 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?

VAEC AWS GOVCLOUD HIGH is responsible for various security controls implemented on VFSP-Va.gov. All data collected and stored in the AWS cloud is securely protected and a FEDRAMP authorization of F1603047866 has been granted within the VA.

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?

Yes. Please refer to the VAEC office for a copy of the copy of the contract between AWS (VAEC AWS GOVCLOUD HIGH) and VFSP-Va.gov.

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

This system does not utilize Robotics Process Automation (RPA).

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

ID	Privacy Controls
AP	**Authority and Purpose**
AP-1	Authority to Collect
AP-2	Purpose Specification
AR	**Accountability, Audit, and Risk Management**
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-7	Privacy-Enhanced System Design and Development
AR-8	Accounting of Disclosures
DI	**Data Quality and Integrity**
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
DM	**Data Minimization and Retention**

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.

GINA SIEFERT Digitally signed by GINA SIEFERT
Date: 2023.11.16 04:51:55 -06'00'

Privacy Officer, Gina Siefert

Griselda Gallegos 204736 Digitally signed by Griselda Gallegos 204736
Date: 2023.11.16 07:47:08 -06'00'

Information System Security Officer, Griselda Gallegos

CHRISTOPHER JOHNSTON Digitally signed by CHRISTOPHER JOHNSTON
Date: 2023.11.15 19:23:52 -05'00'

Information System Owner, Christopher Johnston

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).

58VA21/22/28/86FR61858; Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA. (11/8/2021) https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

> "I understand that pursuant to 38 U.S.C. Section 1729 and 42 U.S.C. 2651, the Department of Veterans Affairs (VA) is authorized to recover or collect from my health plan (HP) or any other legally responsible third party for the reasonable charges of nonservice-connected VA medical care or services furnished or provided to me. I hereby authorize payment directly to VA from any HP under which I am covered (including coverage provided under my spouse's HP) that is responsible for payment of the charges for my medical care, including benefits otherwise payable to me or my spouse. Furthermore, I hereby assign to the VA any claim I may have against any person or entity who is or may be legally responsible for the payment of the cost of medical services provided to me by the VA. I understand that this assignment shall not limit or prejudice my right to recover for my own benefit any amount in excess of the cost of medical services provided to me by the VA or any other amount to which I may be entitled. I hereby appoint the Attorney General of the United States and the Secretary of Veterans' Affairs and their designees as my Attorneys-in-fact to take all necessary and appropriate actions in order to recover and receive all or part of the amount herein assigned. I hereby authorize the VA to disclose, to my attorney and to any third party or administrative agency who may be responsible for payment of the cost of medical services provided to me, information from my medical records as necessary to verify my claim. Further, I hereby authorize any such third party or administrative agency to disclose to the VA any information regarding my claim. By submitting this application, you are agreeing to pay to the applicable VA copays for treatment or services of your NSC conditions as required by law. You also agree to receive communications from VA to your supplied email or mobile number."

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