Privacy Impact Assessment for the VA IT System called:

Vets.gov

Date PIA completed:

May 8, 2017

VA System Contacts:

	Name	E-mail	Phone Number
Privacy Officer	Rita Grewal	Rita.grewal@va.gov	202.632.7861
Information Security Officer	Joseph Clar	Joseph.clar@va.gov	702.791.9000
System Owner	Angela Gant-Curtis	Angela.gant-curtis@va.gov	540.760.7222
Person Completing the Document	Brian Heckethorn	Brian.heckethorn@va.gov	703.457.3058

Abstract

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

Vets.gov is a publicly accessible website containing related Veteran support applications (e.g. Facility Locator, GI Bill Comparison Tool, Veteran Employment Center (VEC), Application for Health Benefits, Application for Education Benefits, Claim Status, Secure Healthcare Messaging, and Prescription Refill).

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:

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *If your system is a regional GSS, VistA, or LAN, include a list of the hospitals/medical centers, or other regional offices that fall under your system. Additionally, what region is the system under?*
- *A general description of the information in the IT system.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *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.*
- *A citation of the legal authority to operate the IT system.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*
- *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval?*
- *Does the system use cloud technology? 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.*
- *Does a contract with Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII?*
- *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 is the magnitude of harm if privacy related data is disclosed, intentionally or unintentionally? Would the reputation of the CSP or its customers (VA) be affected?*

Vets.gov is a platform into which existing VA web services and service-related content will be initially linked and eventually subsumed. Vets.gov will be the place that Veterans, their families, and their caregivers go to access VA services such as disability benefits, education benefits, employment and career development for veterans and their families, and healthcare, including preventative and primary care for our veterans. Other services include a facility locator and Government Issue (GI) Bill comparison tool.

Vets.gov is securely hosted within the VA-ATO/FedRAMP Amazon Web Services (AWS) GovCloud region. All information sent to/from is via a VA-NSOC approved, encrypted site-to-site VPN tunnel, across which approved connections to VA-internal systems are established. Vets.gov is not the system of record, however, some information is cached for a period of time during user requests. If every veteran were to log into the system at the same time, there could potentially be up toward ten (10) million active users connected to vets.gov. Actual daily usages is relative to va.gov. Vets.gov users are typically veterans of the United States military or members of a veteran's family.

- Digital Government Strategy (May 2012)
- OMB M-17-06, Policies for Federal Agency Public Websites and Digital Services (PDF, 1.2 MB, 18 pages, November 2016)
- OMB Circular A-130, Managing Information as a Strategic Resource (July 28, 2016)
- E-Government Act of 2002, Section 207

As-of the date of this PIA, the vets.gov platform contains the following components:

- Facility Locator, which allows users to find VA facilities by Zip Code, or City and State.
- Veterans Employment Center (VEC), which allows users to find career opportunities.
- Healthcare Application (HCA), which replaced the previous VOA/10-10EZ PDF form with a web-based form that Veterans use to apply for health benefits.
- Education Benefits Application (EBA), which replaces the VONAPP/22-1990 form with a web-based form that Veterans use to apply for education benefits.
- Veteran Information/Eligibility Record Service (VRS) Enterprise Military Information Service (eMIS): provides the requestor with the DoD's Authoritative Military Service Record (AMSR).
- Log-in (via ID.me and Master Veterans Index-Person Services (MVI-PSM)), which is used to validate a Veteran's identity, and provide authenticated and authorized access to the following components:
    - Claim Status, which is connected to eBenefits (EBN), provides users with the ability to view/track the status of their disability claims, and submit additional evidence in support of their existing claim.
    - Secure Messaging, which is connected to MyHealtheVet (MHV), provides users with the ability to exchange messages with their healthcare providers.
    - Prescription Refill, which is connected to MHV, provides users with the ability to refill existing prescriptions.
    - Blue Button, which is connected to MHV, allows the veteran to download their health records. Vets.gov does is only a "pass-through" and does not retain any of the information downloaded.
    - Veteran Information, which is connected to VRS eMIS, allows the veteran to view military service information. Vets.gov does is only a "pass-through" and does not retain any of the information downloaded.

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? Are the types of information collected, used, maintained, and/or shared specified in its Privacy Notices?

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 the VA Handbook 6500 (http://www.va.gov/vapubs/viewPublication.asp?Pub_ID=638&FType=2), published Sept. 2012, Appendix A.)
If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

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

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

☒ Name
☒ Social Security Number
☒ Date of Birth
☒ Mother's Maiden Name
☒ Mailing Address
☒ Zip Code
☒ Phone Number(s)
□ Fax Number
☒ Email Address
☒ Emergency Contact Information (Name, Phone Number, etc of a different individual)
☒ Financial Account Information
☒ Health Insurance Beneficiary Numbers Account numbers
□ Certificate/License numbers
□ Vehicle License Plate Number
☒ Internet Protocol (IP) Address Numbers
☒ Current Medications
□ Previous Medical Records
☒ Race/Ethnicity

The information needed to support vets.gov program activities and electronic services includes:

HCA:

Information sent from vets.gov to HCA:

- Name L/F/M
- Spouse's Name L/F/M
- Childs Name L/F/M
- Mothers Maiden Name
- Gender Male Female
- Birth date
- Spouses date of birth
- Child's date of birth (mm/dd/yyyyy)
- Are you Spanish, Hispanic or Latino
- What is your race: American Indian or Alaska Native, Black or African American , Asian, White, Native Hawaiian or other Pacific islander
- SSN
- Spouse's Social Security number

- Child's Social Security Number
- Permanent Address
- City
- State
- Zip
- Country
- Current Marital Status married/Never married/Separated/Widowed/Divorced
- Home telephone number
- Mobile telephone number
- E-mail address
- Place of Birth City and State
- I am enrolling to obtain minimum essential coverage under affordable care act Yes No
- Which VA Medical Center of Outpatient do you prefer
- Would you like for VA to contact you to schedule your first appointment
- Last Branch of service
- Last entry date
- Last discharge Date
- Discharge type
- Are you a Purple Heart Award Recipient Yes No
- Are you a former prisoner of war Yes No
- From MM DD YYYY
- Where you discharged or retired from military for a disability incurred in the line of duty? Yes No
- Did you serve in SW Asia during the gulf war between August 2, 1990 and November 11, 1998? Yes No
- Did you serve in Vietnam between January 9, 1962 and May 7, 1975? Yes No
- Were you exposed to radiation while in the military? Yes No
- Did you receive nose throat radium treatments while in the military? Yes No
- Enter your health insurance company name, address and telephone number (include coverage through spouse or other person)
- Name of policy holder
- policy number
- group code
- are eligible for Medicaid? Yes No
- Are you enrolled in Medicare Hospital insurance part A? Yes No

EBA:

Information sent from vets.gov to EBA:

- First Name
- Middle Name
- Last Name
- Social Security Number
- Date of Birth
- Gender
- What Education Benefit the Veteran is Applying For

- Relinquishing Eligibility of other Education Benefits if choosing CH33
- Effective Date of that Relinquishment
- Previously submitted Claim for VRE benefits
- Claim number used for previously submitted claim
- Whether the previous claim was filed under someone else's service
- First name of sponsor
- Middle name of sponsor
- Last name of sponsor
- File number of sponsor
- Payee number of sponsor
- Whether Veteran graduated from a military service academy
- Year of graduation
- Active duty status
- Terminal leave status
- If claimant is in receipt of money from armed forces or public health service for the same course applied for in application
- Military service history: branch, entry on duty date, release from active duty date, whether the period of service is applied to this or another benefit, if the Veteran was involuntarily called to active duty
- Whether Veteran was in a ROTC program
- If in ROTC: was commissioned through ROTC program, Year of ROTC program, Scholarship received while in ROTC program, Year of scholarship and amount, Current participation in a senior ROTC scholarship program
- Conditional of receiving benefits from US government as a civilian employee
- Made a kicker contribution towards education benefits
- Whether the Veteran qualifies for a kicker based on military service
- Whether the Veteran has a period of active duty that counts for purposes of repaying education loans, and if so start date (M/D/Y), end date (M/D/Y)
- If Veteran received a high school diploma (M/D/Y)
- Whether Veteran received Education after high school
- If education after high school: Name of college or training provider, City, State, From (date), To (date), Number of hours of education, Type of hours of education, Type of completion certificate received, Major course of study
- FAA certificates
- Whether the Veteran held a journeyman rating license to practice a profession
- What employment or training they received
- When the period of employment was
- Principal occupation
- Number of months worked under license or rating
- School selection: Type of education or training, whether the Veteran knows what school they will attend, name of school, street, city, country, state/province, postal/zip code, education objective
- Personal Information: Address (street, city, country, state/province, postal/zip code), email address, mobile number, telephone number, contact preference
- If secondary contact: secondary contact name, secondary phone number, secondary address
- Dependent information if active duty prior to 1977
- Whether the Veteran is married
- Any children under 18, over 18 but under 23
- Whether the Veteran has a dependent Parent
- Direct deposit account type
- Account number

- Routing number

Log-in (MVI-PSM):

Information sent from MVI-PSM to vets.gov:

- 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
- SSN Verification Status
- Pseudo SSN Reason
- ID Theft flag
- Date of Death
- Multiple Birth Indicator
- Date of Death
- IDType
- Assigning Facility
- Source ID
- Correlation IDs for Internal VA Systems: Integrated Control Number (ICN), ICN Status, DoD EDIPI Id, CORP Id, MHV User ID, BIRLS Id

Log-in (ID.me):

Information collected by ID.me:

- During Initial Registration/Level of Assurance (LoA) 1: Email and Password
- During Identity Proofing Process/LoA 3: First Name, Middle Name, Last Name, Gender, Date of Birth, SSN, Phone Number, Address
    - ID.me collects, but destroys immediately thereafter, a photo of a government-issued ID

Information sent from ID.me to Vets.gov:

- ID.me Universally Unique Identification (UUID)
- First Name
- Middle Name
- Last Name
- Gender
- Birth Date
- Social Security Number (SSN)
- LoA 1-3

Prescription Refill (MHV):

Information sent from MHV to vets.gov:

- Status
- Refill Submit Date
- Refill Date
- Refills Remaining
- Facility Name
- Refillable
- Trackable
- Prescription Id
- Ordered Date
- Quantity
- Expiration Date
- Prescription Number
- Prescription Name
- Dispensed Date
- Station Number

Information sent to MHV from vets.gov:

- User ID for all requests
- Prescription ID when requesting a prescription refill.

Secure Messaging (MHV):

Information sent from MHV to vets.gov:

- A session token for a valid user and account
- A list of triage teams for the user
- A list of message category types
- A list of folders for the user
- A single folder for the user
- A paged list of messages for a folder (without body or attachment fields)
- A single message including body or attachment fields (marked with READ status)
- A list of messages representing the history of the message thread (with body and no attachment fields)

Information sent to MHV from vets.gov:

- User ID for all requests, creation and sending of an email-like message to a health care provider team,
- Requesting to view a folder of message threads, requesting to delete a message, and requesting to move
- Messages between folders, and adding an attachment to a message.

Blue Button (MHV):

Information sent from MHV to vets.gov

- A session token for a valid user and account.
- A Personal Health Record (PHR) refresh can be requested.

- PHR Refresh status can be checked.
- Download the latest Blue Button report

These fields can be in a Blue Button report (last bullet above) sent to the user via vets.gov:

- Future VA Appointments
- Past VA Appointments (limited to past 2 years)
- VA Medication History
- Medications and Supplements, Self-Reported
- VA Laboratory Results
- VA Pathology Reports
- VA Radiology Reports
- VA Electrocardiogram (EKG) History performed at VA Treating Facilities
- Labs and Tests, Self-Reported
- VA Problem List
- VA Admissions and Discharges
- VA Notes from Jan 01, 2013 forward
- VA Wellness Reminders
- VA Allergies
- Allergies, Self-Reported
- VA Immunizations
- Immunizations, Self-Reported
- VA Vitals and Readings
- Vitals and Readings, Self-Reported
- Medical Events, Self-Reported
- Family Health History, Self-Reported
- Military Health History, Self-Reported
- Treatment Facilities, Self-Reported
- Health Care Providers, Self-Reported
- Activity Journal, Self-Reported
- Food Journal, Self-Reported
- My Goals: Current Goals, Self-Reported
- My Goals: Completed Goals, Self-Reported
- VA Demographics from VA Treating Facilities in the last 3 years
- Demographics, Self-Reported
- Health Insurance, Self-Reported
- Military Service Information

Claim Status (EBN):

Information sent from EBN to vets.gov:

- Veteran's Previously completed Claims
- Current pending claims
- What type of claim it is
- What date those claims were submitted or started
- The conditions or benefits that the Veteran claimed
- Whether those conditions are new, increases, secondary, reopened
- The Veteran's Power of Attorney
- The estimated completion date of the claim in question

- An N amount of documents being requested from the Veteran or a 3rd party
  What date that request was made
- What phase the Veteran's claim is in and the date of movement to that phase
- Names of the documents that have been submitted
- The date that document was received

Information sent to EBN by Veteran through document upload:
any number of documents in the form of a pdf, gif, jpg, jpeg, tif, tiff, bmp, or txt, the document type of that uploaded item, and document id for that specific document type

Veteran Information / Eligibility Record Service (VRS):

Information sent from vets.gov to VRS eMIS:

- Electronic Data Interchange Personal Identifier (EDIPI)

Information sent from VRS eMIS to vets.gov:

- Military Service Information: pay grade, pay grade date, service rank, active duty service agreement quantity, initial entry training end date, uniform service initial entry date, military accession source code, personnel start date, personnel termination date, active federal military service base date, service agreement duration in years, DoD beneficiary type, if veteran is in reserves and under the age of 60, Title 38 status code, post-9/11 deployment indicator, post-9/11 combat indicator, pre-9/11 deployment indicator, separation pay type, separation pay gross amount, separation pay net amount, separation pay begin date, separation pay end date, separation pay termination reason, disability severance pay combat code, federal income tax amount, separation pay status code
  Guard or Reserve Service Information: personnel organization code, personnel category type, personnel segment identifier, guard or reserves segment identifier, guard or reserves period start date, guard or reserves period end date, guard or reserves termination reason, guard or reserves character of service code, guard or reserves reason for separation, guard or reserves period statute, guard or reserves period project, post-9/11 GI Bill loss category, training indicator, reserve active duty monthly current paid days, reserve drill monthly current paid days, reserve drill current monthly paid date
- Deployment Information: personnel organization code, personnel category type, personnel segment identifier, deployment segment identifier, deployment start date, deployment end date, deployment project code, deployment termination reason, deployment transaction date, deployment location segment identifier, deployment country, deployment location major body of water, deployment location begin date, deployment location end date, deployment termination reason, deployment location transaction date
- Military Occupation Information: personnel organization code, personnel category type, personnel segment identifier, occupation segment identifier, DoD occupation type, service specific occupation type, service specific occupation date
- Disabilities Information: incurred date, rating code, disability percent, permanent or temporary indicator, pay amount
- Unit Information: personnel organization, personnel category type, personnel segment identifier, unit segment identifier, unit identification code, unit UIC type, unit assigned date

PII Mapping of Components

Vets.gov consists of 8 key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by vets.gov and the functions that collect it are mapped below.

PII Mapped to Components

Components	Does this function collect or store PII? (Yes/No)	Type of PII	Reason for Collection of PII	Safeguards
HCA	Yes	See list of fields in section 1.1	To allow user to sign up for benefits	All data encrypted in transit. Data only stored temporarily.
EBA	Yes	See list of fields in section 1.1	To allow user to sign up for benefits	All data encrypted in transit. Data only stored temporarily.
Prescription Refill	Yes	See list of fields in section 1.1	To allow users to submit refills and see status of their VA prescriptions.	All data encrypted in transit. Data only stored temporarily.
Secure Messaging	Yes	See list of fields in section 1.1	To allow users to message their health care provider	All data encrypted in transit. Data only stored temporarily.
Blue Button	Yes	See list of fields in section 1.1	To allow users to view andn download their electronic health records.	All data encrypted in transit. Data only stored temporarily.
ID.me Login	Yes	See list of fields in section 1.1	To authenticate users	All data encrypted in transit. Data only stored temporarily.
Veteran Information	Yes	See list of fields in section 1.1	To allow users to view military service information	All data encrypted in transit. Data only stored temporarily.
Claims Status	Yes	See list of fields in section 1.1	To allow users to view the current status of their claim.	All data encrypted in transit. Data only stored temporarily.

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

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?

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 1.3 indicate why the system is using this source of data.

If the system creates information (for example, a score, analysis, or report), list the system as a source of information.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

- HCA: User-entered information.
- EBA: 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.
- 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.

1.3 How is the information collected?

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 technology used in the storage or transmission of information in identifiable form?

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.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

- HCA: Users enter data into the required fields within the healthcare application.
- EBA: Users enter data into the required fields within the healthcare 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.
- 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.

1.4 What is the purpose of the information being collected, used, disseminated, created, or maintained?

Include a statement of why the particular SPI is collected, maintained, used, or disseminated in the system is necessary to the program's or agency's mission. Merely stating the general purpose of the system without explaining why this particular type of information should be collected and stored is not an adequate response to this question.

If the system collects, uses, disseminates, or maintains publically available or commercial data, include a discussion of why commercial data is relevant and necessary to the system's purpose.
This question is related to privacy control AP-2, Purpose Specification.

- HCA: The purpose of collecting information is to create and submit an application for VA healthcare benefits. The information is collected on vets.gov and submitted to the Enrollment System Redesign (ESR) for processing.
- EBA: The purpose of collecting information is to create and submit an application for VA education benefits. The information is collected on vets.gov and submitted to The Image Management System (TIMS) for processing.
- Log-in: The purpose of collecting information is to validate a user's identity in order to allow them authenticated access to secure VA systems that contain their information.
- Claim Status: The purpose of collecting information to provide additional evidence in support of a VA disability claim. The information is collected on vets.gov and submitted to EBN.
- Secure Messaging: The purpose of collecting information is to create and submit messages between a user and healthcare provider. The information is collected on vets.gov and submitted to MHV.
- Prescription Refill: The purpose of collecting information is to create a prescription refill. The information is collected on vets.gov and submitted to MHV.
- Veteran Information: Provides the Veteran/User the ability to view military service information including but not limited to deployments, reserve periods, disabilities, and retirement.

1.5 How will the information be checked for accuracy?

Discuss whether and how 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?

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.
This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

Any information entered by the Veteran is considered accurate, and therefore no additional checks are performed. However, validations built into the application on vets.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 considered to be accurate.

1.6 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

- Healthcare Application (HCA) formerly (VOA) 10-10EZ form, which is now part of Vets.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 Application (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.
- Secure Messaging, which is connected to MyHealtheVet (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."
- 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."

1.7 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.

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: A risk would be a compromise of Vets.gov that leads to interception and stealing of personal information.

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. To mitigate the possibility of data being compromised, user-entered data that is cached (stored temporarily) is only stored 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.

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.

Vets.gov is a platform into which existing VA web services and service-related content will be initially linked and eventually subsumed. Vets.gov will be the place that Veterans, their families, and their caregivers go to access VA benefits and services. Vets.gov will also include new services based on Veteran needs.

- HCA: Data collected is used in the determination of healthcare benefits eligibility.
- EBA: Data collected is used in the determination of education benefits eligibility.
- Claim Status: Data collected is used to provide additional evidence in support of a VA disability claim.
- 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.

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

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.

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.
This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

This application does not process or analyze data submitted.

2.3 PRIVACY IMPACT ASSESSMENT: Use of the information How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

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.

Vets.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 the 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.

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

- EBA: All data listed in 1.1.
- Claim Status: All data listed in 1.1.
- Secure Messaging: All data listed in 1.1.
- Prescription Refill: All data listed in 1.1
- Log-in (MVI-PSM): ICN, ICN Status, IDType, and SourceID state
- Log-in (ID.me): All data listed in 1.1 with the exception of a photo of a government-issued ID which is collected but then immediately destroyed once a user's identity has been verified.
- Veteran Information: All data listed in 1.1.

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.
This question is related to privacy control DM-2, Data Retention and Disposal.

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

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

The following component retains data only for 24 hours upon a user initiating an authenticated session within vets.gov.

- Claim Status

The following information is retained for 30 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 with the exception of 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)? If so please indicate the name of the records retention schedule.

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.
This question is related to privacy control DM-2, Data Retention and Disposal.

Not applicable as Vets.gov is not a system of record.

ID.me's federal accreditation under GSA's FICAM program addresses records retention requirements in order 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 vets.gov contract (VA118-16-C-1000) agreements.

3.4 What are the procedures for the elimination of SPI?

Explain how records are destroyed or eliminated at the end of the 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

All data cached/stored by vets.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 that programmatically triggers a clean up script.

With respect to ID.me, once a user has an ID.me wallet, they have one, regardless of if a vets.gov contract exists or not. If the contract is terminated, a user with an ID.me wallet would not be able to login at vets.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 vets.gov contract (VA118-16-C-1000) and VA Interconnection Security Agreement Memorandum of Understanding (ISA MOU) and the use of the information from vets.gov is simply for verification of the user account.

3.5 Does the system, where feasible, use techniques to minimize the risk to privacy of 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. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?
This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research

Digital Service at VA (DSVA) 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).

Vets.gov does NOT use PII/PHI for testing information systems or pre-production prior to deploying to production.

DSVA 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-boarding).

3.6 <u>PRIVACY IMPACT ASSESSMENT: Retention of information</u>

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.

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:

<u>Principle of Minimization:</u> 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?

<u>Principle of Data Quality and Integrity:</u> 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: vets.gov only retains data long enough (1 hour) to ensure a consistent user experience.

Mitigation: vets.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

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? What information is shared/received, and for what purpose? How is the information transmitted or disclosed?

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 information is 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.

Program Office or IT System information is shared with	***Reason why information is shared with the specified program or IT system***	***List the specific information types that are shared with the Program or IT system***	***Method of transmittal***
Enrollment System Redesign	ESR is the system of record for all health enrollment information.	Please see Section 1.1	Data entered into the form fields by the Veteran is encrypted (via SSL) and transmitted to ESR across our NSOC-monitored, site-to-site VPN connection.
TIMS SFTP	TIMS SFTP is used to capture completed applications for education benefit.	Please see Section 1.1	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.
MVI-PSM	MVI-PSM is a system of record for Veteran validation information.	Please see Section 1.1	Data entered into the form fields (for log-in) by the Veteran is encrypted (via SSL). Data transmitted to MVI-PSM across

			our NSOC-monitored, site-to-site VPN connection.
MHV (Prescription Refill/Secure Messaging/Blue Button)	MHV is the system of record for allowing the veteran access to information and tools to improve their health.	Please see Section 1.1	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
eBenefits	eBenefits is the system of record for retrieving existing claim status and allowing users to submit additional evidence in support of their existing claims.	Please see Section 1.1	Data entered into the form fields by the Veteran is immediately encrypted (via SSL) and transmitted to eBenefits.
HCA	HCA is the system of record for retrieving information for VA healthcare benefits	Please see Section 1.1	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.
VRS eMIS	eMIS is the system of record for retrieving information for Veteran Military services	Please see Section 1.1	Data transmitted to VRS eMIS across our NSOC-monitored, site-to-site VPN connection
EBA	EBA is the system of record for retrieving information for VA education benefits.	Please see Section 1.1	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.

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

Follow the format below:
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 vets.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

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

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

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

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

For each interface with a system outside VA, state what specific information is 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

Program Office or IT System information is shared with	***Reason why information is shared with the specified program or IT system***	***List the specific information types that are shared with the Program or IT system***	***Legal authority, binding agreement, SORN routine use, etc that permit external sharing (can be more than one)***	***Method of transmission and measures in place to secure data***
ID.me	Used in the verification of veteran identities.	Please see 1.1	Information sharing is covered and approved per the agreement set for in the vets.gov contract	Secure Socket Layer (SSL) encryption; ID.me's accreditation with Kantara and GSA FICAM has robust controls, technical and policy, with respect to privacy. Additionally, the authentication applied must be commensurate with the risk of the transaction; end users are only asked for the minimum set of attributes reasonably required to perform a given transaction; and, a consent screen with granular, data field insight is presented to the user prior to authorizing the release of any personal data to a related application. Additional information regarding the controls and standards in support of LoA3 can be found here:

			(VA118-16-C-1000) and via a VA Interconnection Security Agreement Memorandum of Understanding (ISA MOU)	https://kantarainitiative.org/confluence/display/LC/Identity+Assurance+Framework

If specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16, note them here.

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: 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 vets.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

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 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?

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. If notice was provided in the Federal Register, provide the citation.

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

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.
This question is 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.

Yes. Notice is provided to Veteran upon entering any information into vets.gov. It reinforces to the user that any information they enter into form-fields on the application will be collected. Please see Appendix A 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?

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

Information is required to determine eligibility. Providing information is a basic assumption and requirement of any application, as an application is by definition 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?

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

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

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.

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: As with any website, there is a risk that the data entered is captured during transmission from the application to the Enterprise System (ES).

Mitigation: 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 Vets.gov and the ES conforms to these standards.

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?

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.

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).

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.
This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

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

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.

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 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).

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.

If the VA has information that conflicts with that provided by the Veteran, the VA corresponds directly with the Veteran to request confirmation and additional supporting documentation, if needed.

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.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

<u>Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.</u>

Not Applicable, as formal redress is provided.

7.5 <u>PRIVACY IMPACT ASSESSMENT:</u> 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.*

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: Information provided via vets.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?

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

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?

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.

This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.

Vets.gov is primarily a publicly accessible website providing general content for anonymous use. Components of Vets.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 Enterprise Veterans Self Service (EVSS). 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 Vets.gov cannot use Vets.gov to display information retrieved from MHV without having an active MHV account.

Any user registered with ID.me may login to Vets.gov, but without additional authorization a user will not receive access to custom resources. Once logged in, Vets.gov attempts to validate the user exists in the VA MVI. If the user exists in the MVI, Vets.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 Vets.gov cannot use Vets.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 Services at Veterans Affairs (DSVA) users, only users from United States Digital Service (USDS) and Ad Hoc have access to the source code, system, and datastores. No users (including DSVA, USDS, Ad Hoc) have the ability to access data on behalf of another individual user. Access to the underlying application and infrastructure is managed via the processes defined within the vets.gov Access Control Standard Operating Procedure (SOP), found here: https://github.com/department-of-veterans-affairs/vets.gov-ato/blob/master/sops/AC.md

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.

Requests for access is authorized via signature of the vets.gov System Owner and the vets.gov ISO.

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 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.

Vets.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).

vets.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).

vets.gov role-based security training consists of the following VA OIT TMS training:

3.1.1 Translate Information Security Role-Based Training for System Administrators (WBT), Number 1357076 which enables System Administrators to incorporate security actions into their day-to-day tasks to support risk-based decision making for each step of VA's Risk Management Framework (RMF). This course provides VA's System Administrator personnel with the IT security and privacy requirements of FISMA and related NIST guidance and general information security practices.

Completion of VA Privacy and Information Security Awareness and Rules of Behavior is tracked and monitored by the Enterprise Program Management Office (EPMO), Workforce Shaping & Compliance Workforce Management;

Non-compliance (past due date) notifications are sent to EPMO and the COR, who then follows up via email with the respective employee/contractor.

Personnel who do not complete the required training within a two-week grace period are removed from accessing the information system(s).

Individual security training records are maintained for the entire term of employment and updated on an annual basis for refresher training as required.

All contracts are reviewed quarterly with the TAC, COR and vets.gov PM.

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.

Vets.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).

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

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

If so, provide the date the Authority to Operate (ATO) was granted. Please note that all systems containing SPI are categorized at a minimum level of "moderate" under Federal Information Processing Standards Publication 199.

Vets.gov is operating under full Authority to Operate (ATO) granted on March 07, 2017.

Section 9. References

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

RITA K GREWAL 114938

Digitally signed by RITA K GREWAL 114938
DN: dc=gov, dc=va, o=internal, ou=people, 0.9.2342.19200300.100.1.1=rita.grewal@va.gov, cn=RITA K GREWAL 114938
Date: 2017.05.19 12:17:25 -04'00'

Privacy Officer, Rita Grewal

Information Security Officer, Joseph Clar

Angela Gant-Curtis 105447

Digitally signed by Angela Gant-Curtis 105447
DN: dc=gov, dc=va, o=internal, ou=people, 0.9.2342.19200300.100.1.1=angela.gant-curtis@va.gov, cn=Angela Gant-Curtis 105447
Date: 2017.05.19 11:23:40 -05'00'

System Owner, Angela Gant-Curtis

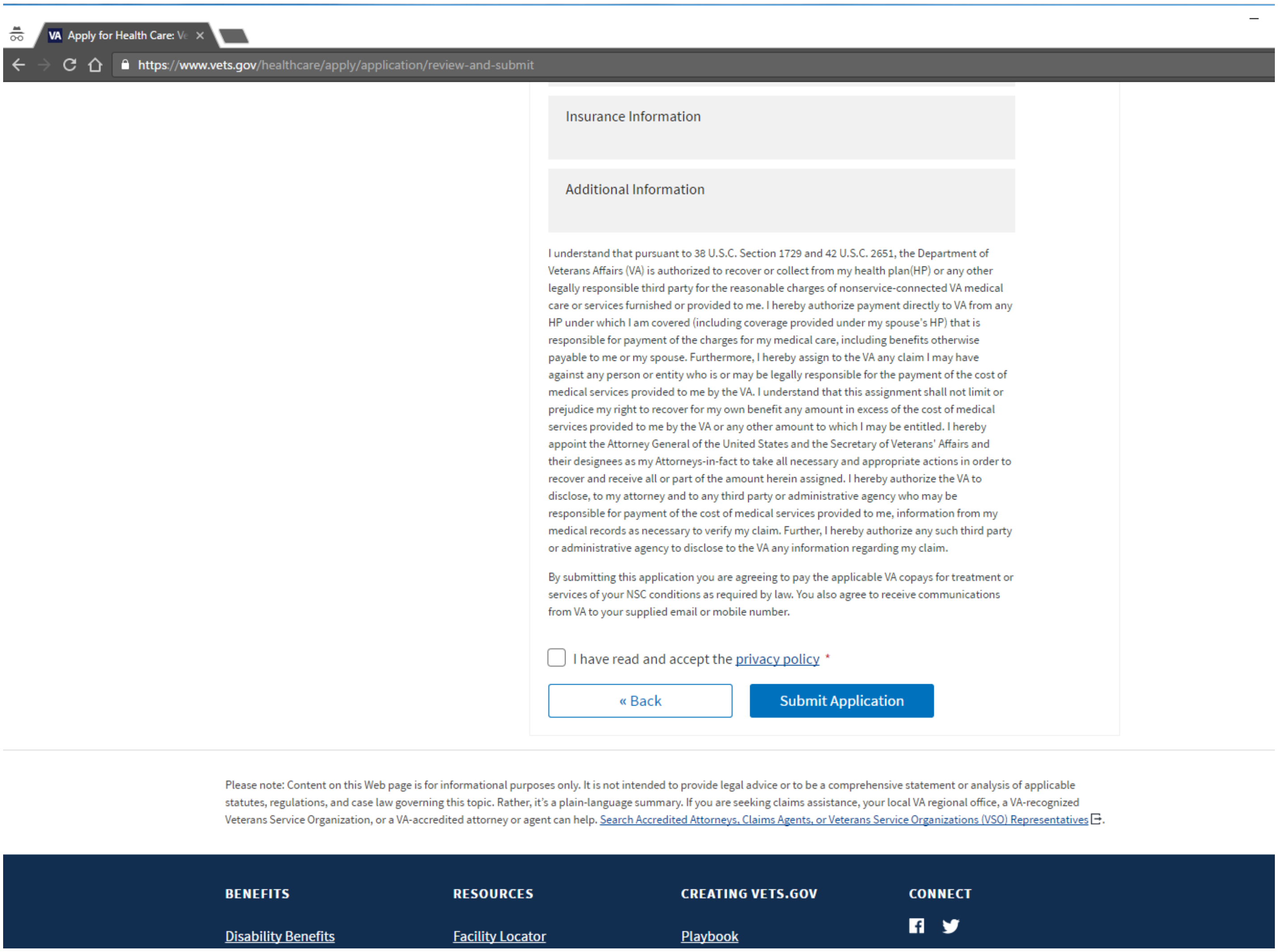
Individual Completing the PIA, Brian Heckethorn

APPENDIX A-6.1

Notice of Privacy Practices

Effective Date:

Please provide a copy of the notice below (A notice may include a posted privacy policy, a Privacy Act notice on forms).

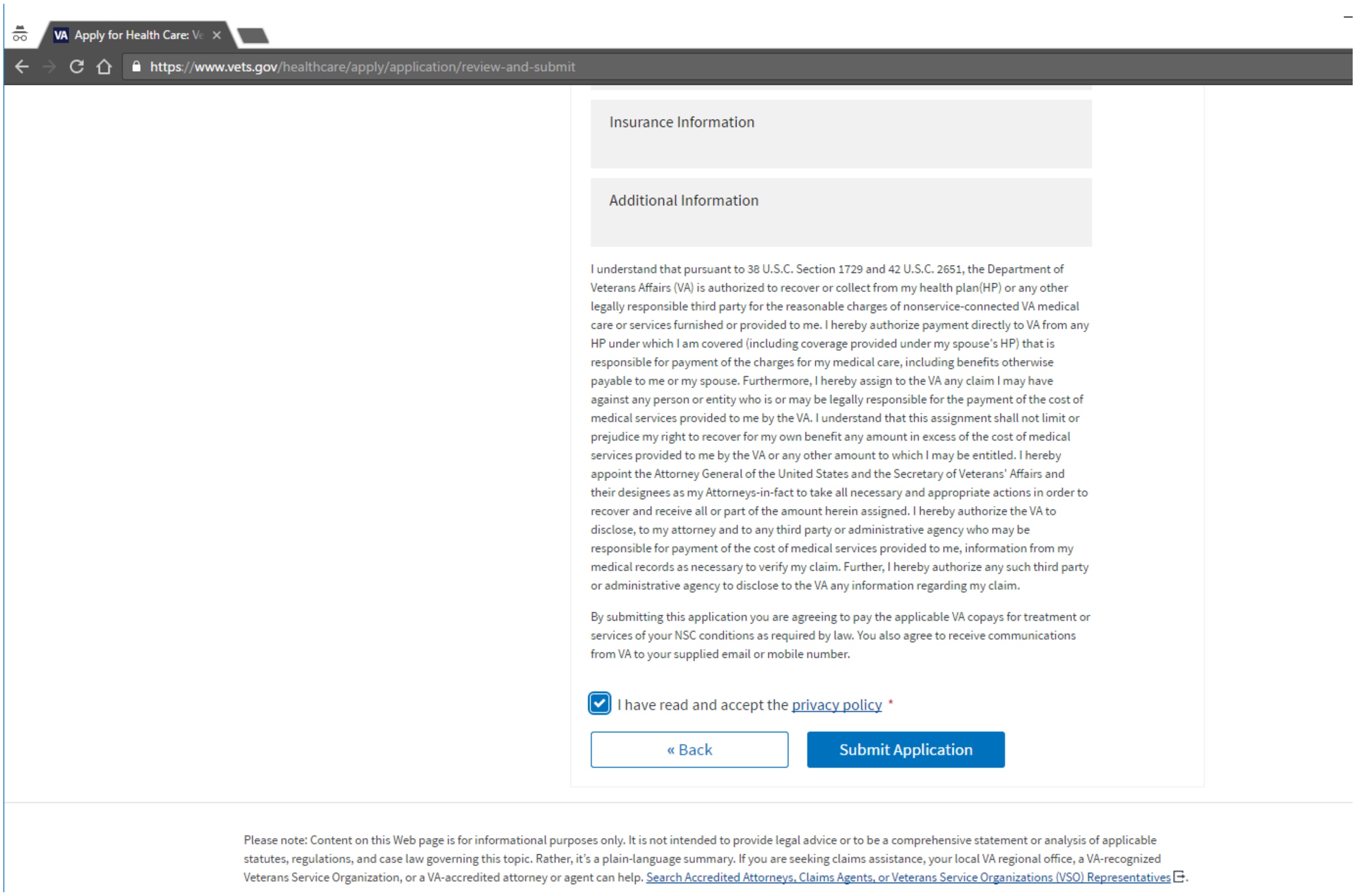

VA Apply for Health Care: V
https://www.vets.gov/healthcare/apply/application/review-and-submit
Insurance Information
Additional Information

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 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.

□ I have read and accept the privacy policy *

Please note: Content on this Web page is for informational purposes only. It is not intended to provide legal advice or to be a comprehensive statement or analysis of applicable statutes, regulations, and case law governing this topic. Rather, it's a plain-language summary. If you are seeking claims assistance, your local VA regional office, a VA-recognized Veterans Service Organization, or a VA-accredited attorney or agent can help. Search Accredited Attorneys, Claims Agents, or Veterans Service Organizations (VSO) Representatives.



Apply for Health Care: Ve
https://www.vets.gov/healthcare/apply/application/review-and-submit

Insurance Information

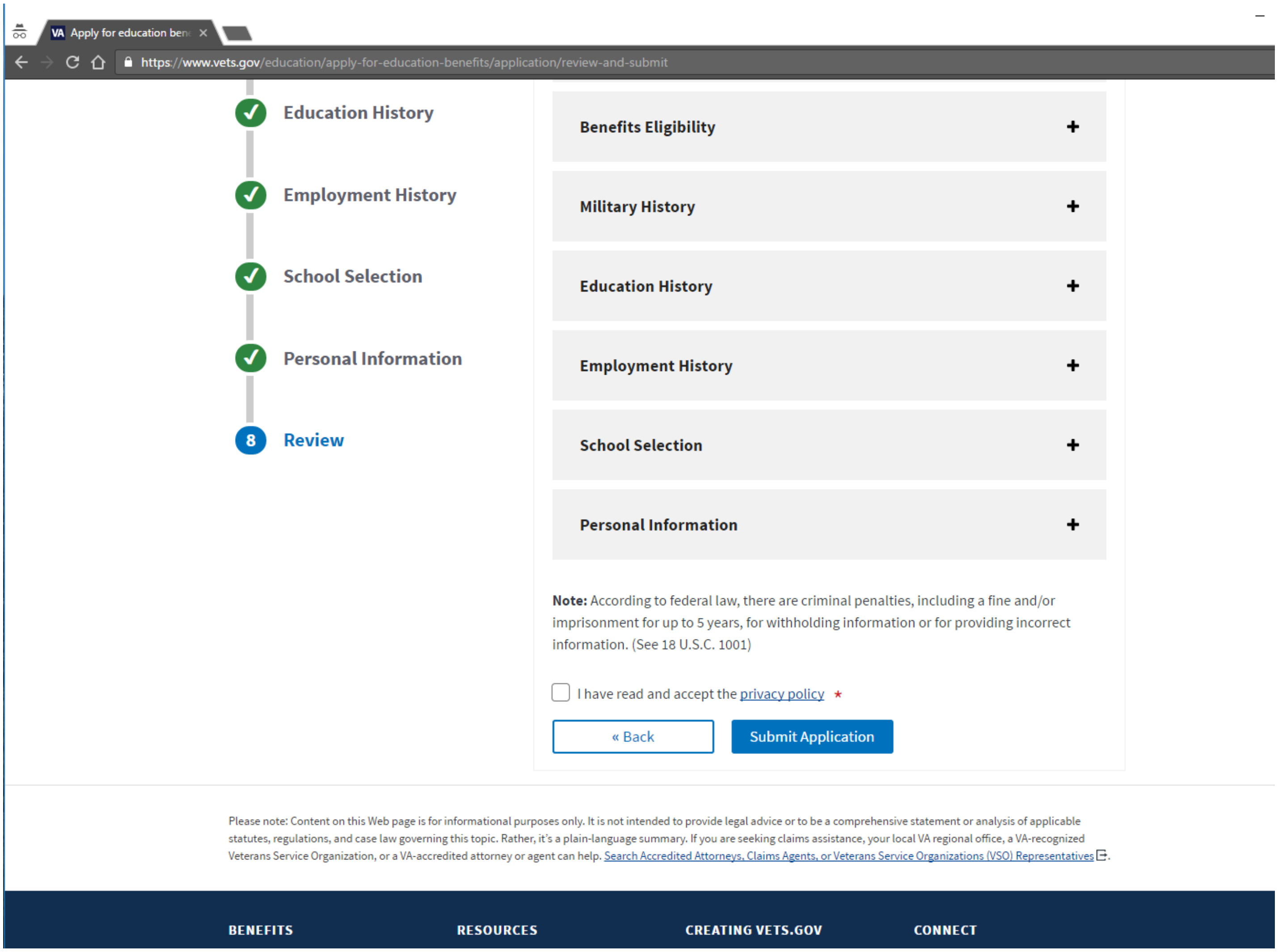
Additional Information

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 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.

☑ I have read and accept the privacy policy *

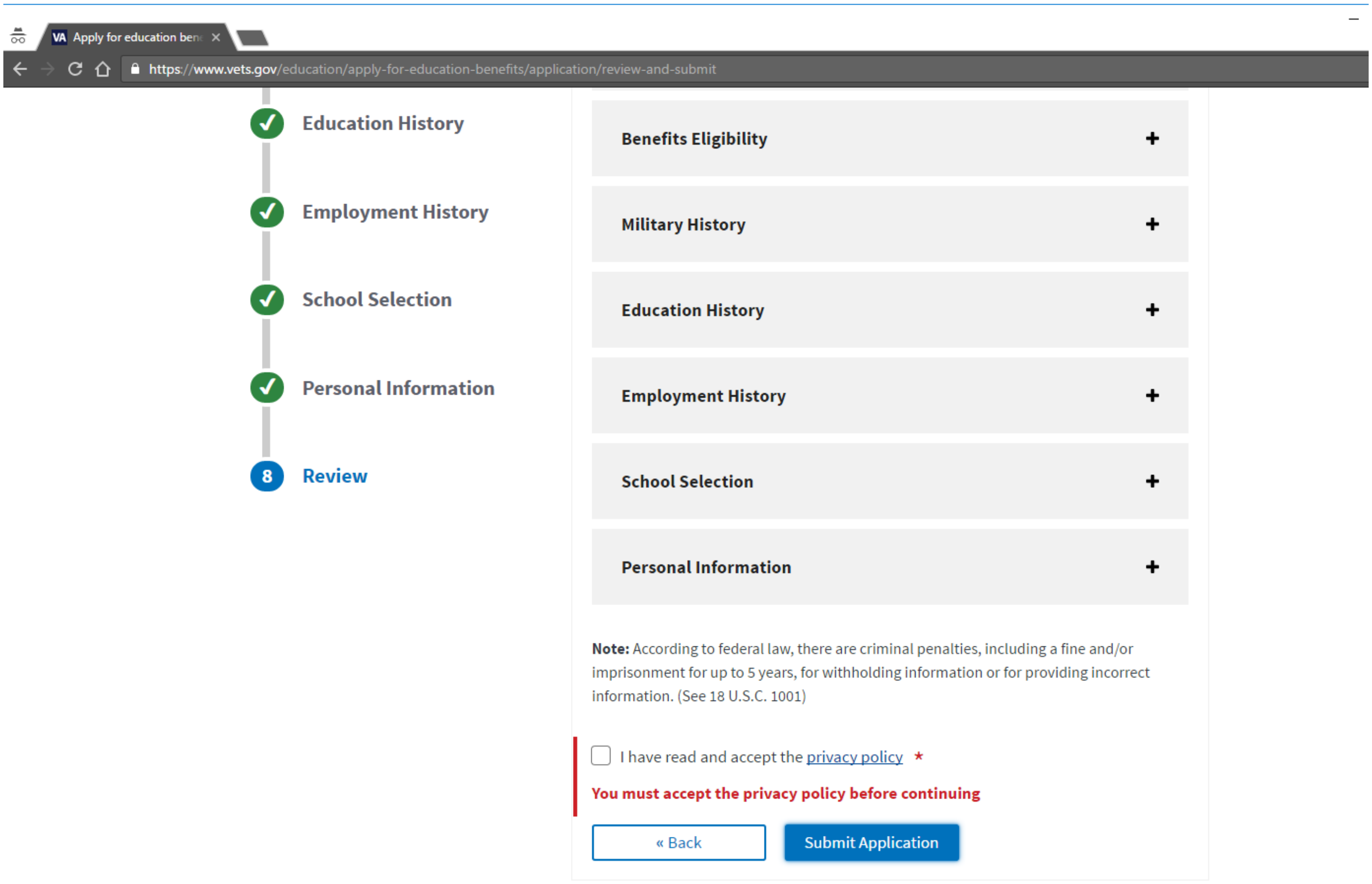
Please note: Content on this Web page is for informational purposes only. It is not intended to provide legal advice or to be a comprehensive statement or analysis of applicable statutes, regulations, and case law governing this topic. Rather, it's a plain-language summary. If you are seeking claims assistance, your local VA regional office, a VA-recognized Veterans Service Organization, or a VA-accredited attorney or agent can help. Search Accredited Attorneys, Claims Agents, or Veterans Service Organizations (VSO) Representatives.



Note: 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)

□ I have read and accept the privacy policy *

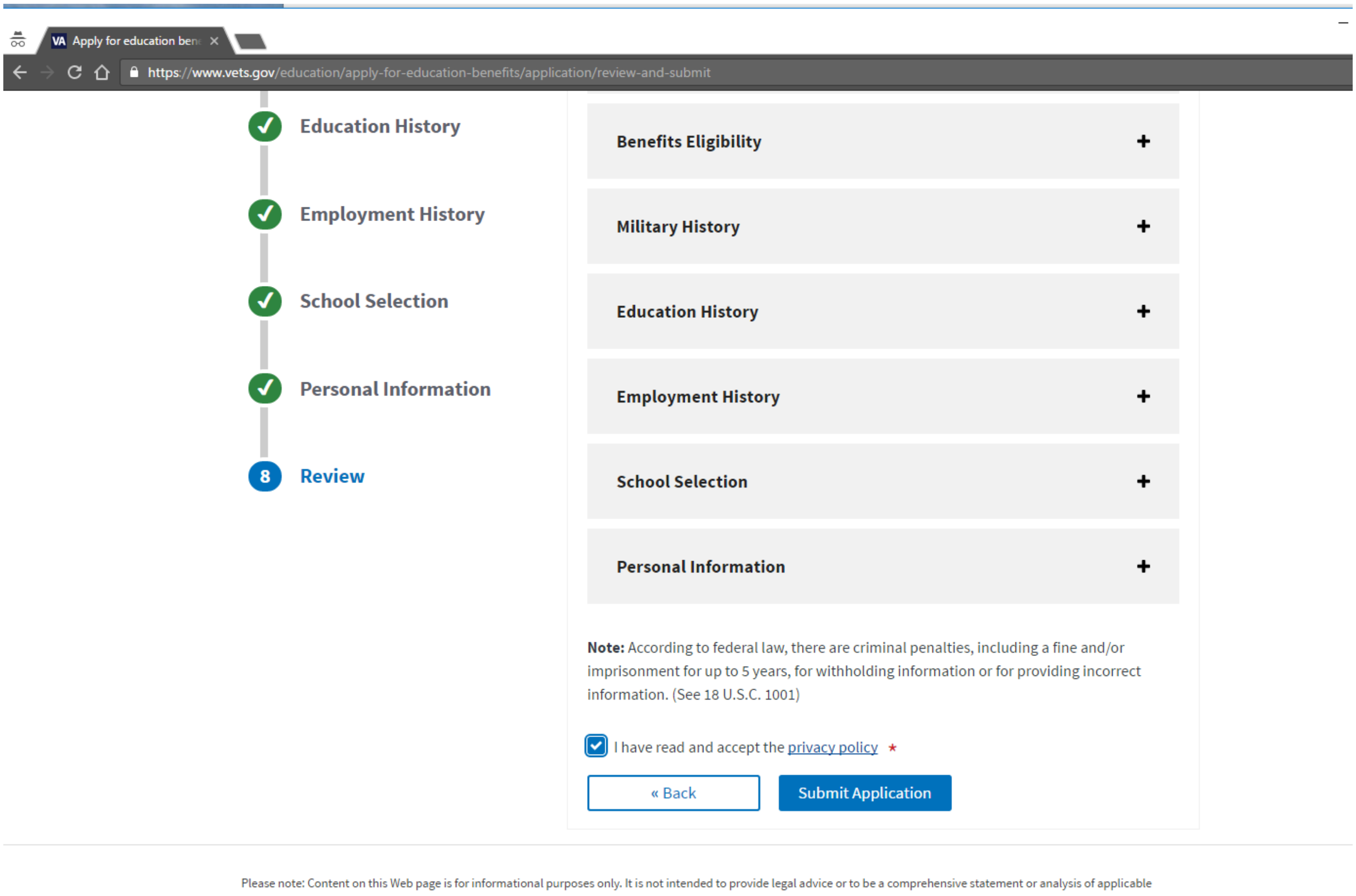
Please note: Content on this Web page is for informational purposes only. It is not intended to provide legal advice or to be a comprehensive statement or analysis of applicable statutes, regulations, and case law governing this topic. Rather, it's a plain-language summary. If you are seeking claims assistance, your local VA regional office, a VA-recognized Veterans Service Organization, or a VA-accredited attorney or agent can help. Search Accredited Attorneys, Claims Agents, or Veterans Service Organizations (VSO) Representatives.



Note: 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)

□ I have read and accept the privacy policy *

You must accept the privacy policy before continuing



Note: 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)

☑ I have read and accept the privacy policy *

Please note: Content on this Web page is for informational purposes only. It is not intended to provide legal advice or to be a comprehensive statement or analysis of applicable