Privacy Impact Assessment for the VA IT System called:

Fugitive Felon Program (FFP)

Veterans Health Administration (VHA)

VHA Member Services (MS), Health Eligibility Center (HEC)

eMASS ID #678

Date PIA submitted for review:

10/08/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Shirley P. Hobson	Shirley.Hobson@va.gov	629-259-3849
Information System Security Officer (ISSO)	Howard Knight	Howard.Knight@va.gov	404-828-5340
Information System Owner	William Brock	william.brock2@va.gov	404-321-6111 ext 206203

Abstract

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

The Fugitive Felon Program (FFP) was created because the Veterans Education and Benefits Expansion Act (VEBEA) of 2001 requires that the Department of Veterans Affairs (VA) withhold specified benefits (including health care) from Veterans and dependents of Veterans who are fugitive felons.

38 U.S.C. § 5313B prohibits VA against providing health care benefits to Veterans and Veterans' dependents who are verified as fugitive felons. This includes health care provided in the community at VA's expense. VHA Handbook 1000.02, VHA Fugitive Felon Program, provides policy and standards for ensuring compliance with the prohibition again providing health care benefits to Veterans and Veterans' dependents while in a verified fugitive felon status.

The Fugitive Felon Program was initiated through a Memorandum of Understanding (MOU) with multiple federal agencies and included agreements with all respective state agencies and administered by the VA Office of Inspector General (OIG). This MOU also grants access to a myriad of federal electronic databases which assists OIG with locating fugitive felons.

A fugitive felon is defined as a person who is fleeing to avoid prosecution, or custody or confinement after conviction, for an offense, or an attempt to commit an offense, which is a felony under the laws of the place from which the person flees; or violating a condition of probation or parole imposed for commission of a felony under Federal or State law.

Overview

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

1 General Description

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

The Fugitive Felon Program (FFP) is under the VHA Member Services, Health Eligibility Center (HEC) Program Office.

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

The purpose of the FFP is to prevent Veterans and dependents of Veterans who are verified as fugitive felons from getting VA health care benefits.

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

The FFP system is VA Owned and VA Operated.

2. Information Collection and Sharing

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

There are currently over 70,000 Veterans who are possible fugitive felons in the database, and over 400 VA employees to investigate or remediate their statuses.

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

Information in the FFP web application include personally identifying information (PII) on Veterans who are verified or potential fugitive felons, warrant information and other court and law enforcement data, and data pertaining dates and statuses of contact attempts.

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

Once the information is imported into the FFP web application, it is not shared outside of the application.

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

The FFP web application is only hosted on premises at the Health Eligibility Center (HEC).

3. Legal Authority and SORN

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

The Fugitive Felon Program (FFP) Veterans Education and Benefits Expansion Act (VEBEA) of 2001; 38 U.S.C. 5313B. Veterans' Health Care Eligibility Reform Act of 1996, Public Law 104-262; Title 38 U.S.C. Sections 1705, 1710, 1712 and 1722; Title 38 U.S.C Sections 5317 and 5319; Title 26 U.S.C. Section 6103 (I)(7) provide the legal authority.

Enrollment and Eligibility Records- VA 147VA10
https://www.govinfo.gov/content/pkg/FR-2021-08-17/pdf/2021-17528.pdf
Police and Security Records – VA SOR 103VA07B
https://www.govinfo.gov/content/pkg/FR-2022-10-21/pdf/2022-22899.pdf
Criminal Investigations – VA SOR 11VA51
https://www.govinfo.gov/content/pkg/FR-2019-04-17/pdf/2019-07647.pdf

I. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?

There are currently some minor changes in development, but these are superficial changes and will not in any way require amendments or revisions to the System of Records Notification (SORN).

4. System Changes

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

Cloud technology is not currently used by the FFP and there are no existing contracts that are expected to affect ownership rights over any of the data. Since there is no CSP provider, there will be no impact.

K. Will the completion of this PIA could potentially result in technology changes?
No.

Section 1. Characterization of the Information

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

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

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

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

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

- ☒ Name
- ☒ Social Security Number
- ☒ Date of Birth
- ☐ Mother's Maiden Name
- ☐ Personal Mailing Address
- ☐ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☐ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☐ Financial Information
- ☐ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers[1]
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☐ Medications
- ☐ Medical Records
- ☐ Race/Ethnicity
- ☐ Tax Identification Number
- ☐ Medical Record Number
- ☐ Gender
- ☐ Integrated Control Number (ICN)
- ☐ Military History/Service Connection
- ☐ Next of Kin
- ☒ Other Data Elements (list below)

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

Other PII/PHI data elements: none

Veterans Integrated Service Network (VISN); Facility Name/Number; VA Office of Inspector General (OIG) Case Number; Warrant Number; Originating Case Agency (OCA)_Number; Network username; Work Phone, VA email.

PII Mapping of Components (Servers/Database)

Fugitive Felon Program (FFP) consists of **3** key components (servers/databases/instances/applications/software/application programming interfaces (API). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **Fugitive Felon Program (FFP)** and the reasons for the collection of the PII are in the table below.

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
Source data files	**No**	**Yes**	Name, SSN, DOB, VISN, Facility, VA_OIG_Case_Number, Warrant_Number, OCA_Number	**To load into the application database.**	**Password protected encrypted files, transferred to and temporarily stored on a secure network folder.**
Database server	**No**	**Yes**	**Name, SSN, DOB, VISN, Facility, VA_OIG_Case_Number, Warrant_Number, OCA_Number**	**For verifications and processing progress of resolutions.**	**Stored in an encrypted secure database.**

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

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

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

VA Office of Inspector General (OIG) matches VHA data files with the National Crime Information Center (NCIC) to identify Veterans and dependents receiving VA health care benefits who are fugitive felons under 38 U.S.C. 5313B, Prohibition of Providing Certain Benefits with Respect to Persons Who Are Fugitive Felons.

1.2b Describe why information from sources other than the individual is required? For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question indicate why the system is using this source of data.

OIG provides the data to VHA Member Services, Health Eligibility Center. The Health Eligibility Center notifies appropriate VAMC staff to access the database and retrieve data specific to their facility. The information collected is used to validate the status of Veteran's or dependent of Veteran's warrant. When validated, notification of warrant is sent to the Veteran or dependent of the Veteran warrants. If no response is received from the Veteran or dependent of the Veteran within 60 days, the Veteran's or dependents of the Veteran VA health care benefits and services are terminated and billing is affected, if applicable.

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

The FFP database is a source of information for appropriate VAMC, CHAMPVA and FMP FFP Coordinators, VISN POCs, and VA Police, with a need to know.

1.3 How is the information collected?

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

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

The information is collected electronically based on guidance documented in VHA Directive 1520, Fugitive Felon Program.

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

No forms are used in the collection of FFP data.

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

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

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

Before decisions are made about a Veteran or dependent of a Veteran eligibility, the local VA Police conducts a manual of all warrants to determine if the warrants are still valid.

1.4b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?

No, there is no commercial aggregator of the information.

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

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

The Fugitive Felon Program (FFP) Veterans Education and Benefits Expansion Act (VEBEA) of 2001; 38 U.S.C. 5313B, Prohibition of Providing Certain Benefits with Respect to Persons Who Are Fugitive Felons; VHA Handbook 1000.02, Fugitive Felon Program

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

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

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

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

<u>Principle of Minimization:</u> 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: FFP uses Personally Identifiable Information (PII) as well as agency case and warrant numbers. If this information were to be breached or accidentally leaked to inappropriate parties or the public, it could result in financial, personal, and/or emotional harm to the individuals whose information is being used in the FFP system.

Mitigation: Individuals with need to know are required to complete applicable privacy and security training and are responsible for protecting their access information.

Section 2. Uses of the Information

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

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

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

PII/PHI Data Element	Internal Use	External Use
Name, SSN, DOB, VISN, Facility, VA OIG Case Number, Warrant Number, OCA Number	Used to ensure Veterans and dependents of Veterans are not receiving VA health care benefits while in a verified fugitive felon status	Not used

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

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

reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis?

The system allows field filtration of the data to ensure VA medical facility sites are only processing records specific to that site.

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

FFP does not create or make available new or previously unutilized information about an individual.

2.3 How is the information in the system secured?

These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

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

SSL protection for in transit; database encryption for data at rest

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

Limited access, encryption and training are used as additional protections in FFP system. All VA members with access to sensitive information must complete VA Privacy and Information Security Awareness training and Sign the Rules of Behavior (ROB) as well as the Privacy and Health Insurance Portability and Accountability Act (HIPAA) training. Access to SSNs is only to authorized, pre-approved users.

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

Data is encrypted in transit and at rest. User roles determine who has visibility.

2.4 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u>

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:

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

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

2.4a How is access to the PII determined?

Each VA medical facility and OCC (CHAMPVA and FMP) directors are responsible for identifying 2 FFP Coordinators and provide HEC the contact information of those individuals. FFP Coordinators are the only individual granted access to the FFP database by HEC. VHA Handbook 1000.02, Fugitive Felon Program, includes the responsibilities for FFP Coordinators. Currently LEAF Access Request for FFP is used for approval and process of FFP access.

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

Yes

2.4c Does access require manager approval?

Yes

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

Network access and web server access is monitored by the Cyber Security Operations Center (CSOC) for unusual activity.

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

FFP management team (VHA)

Section 3. Retention of Information

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

3.1 What information is retained?

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

The Veteran full name, SSN, DOB, law enforcement agency's name, address, phone number, offense, offense code, date warrant was issued, warrant number, VA medical facility number, VISN, VA OIG case number, OCA Number, date warrant sent to VA police, date warrant status received from VA police.

3.2 How long is information retained?

In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the

information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. ***The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.*** *If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

Information will be retained for a period of 7 years after the case is closed in the FFP database.

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

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

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

Yes

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

Records are retained Records Control Schedule (RCS 10-1), Health Eligibility Center Records 1250.1.

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

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

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

7 years after the case is closed in the FFP database, case files will be purged by permanent deletion from the secure server.

Electronic data and files of any type, including PHI, SPI, Human Resources records, and more are destroyed in accordance with the Media Sanitization section of the VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and are compliant with NIST SP 800-88. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle Bin. Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destruction.

https://www.va.gov/vapubs/search_action.cfm?dType=1

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

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

Information in the FFP database is used for training purposes but not research purposes. The training system is a limited access system that is separate from the production system which allows for actual data to be used during training sessions.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that information could be stored longer than necessary.

Mitigation: Mitigation plans are being developed to delete case files that have been closed over 7 years ago. Data is encrypted in transit and at rest via FIPS 140-3 compliant encryption.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
All VA medical facilities	Determine eligibility for VA health care and services	Full Name, SSN, DOB, VA OIG Case Number, Warrant Number, and OCA Number	Managed access to FFP web application
Veterans Health Administration (OIG Office)	Transfer/sharing refreshed data	Full Name, SSN, DOB, VA OIG Case Number, Warrant Number, and OCA Number	Secure File Share

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: The privacy risk associated with maintaining PII is that sharing data within the Department of Veterans' Affairs could happen and the data may be disclosed to individuals who do not require access and heightens the threat of the information being misused or improperly disclosed.
Mitigation: FFP data is only available to staff with a need to know and must comply with privacy and security protocols.

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 data elements (PII/PHI) are shared with each specific partner.

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN.
Is there a Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.

This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

List External Program Office or IT System information is	***List the purpose of information being shared /***	***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,***	***List the method of transmission and the measures in***

shared/received with	*received / transmitted with the specified program office or IT system*		*SORN routine use, etc. that permit external sharing (can be more than one)*	*place to secure data*
N/A	N/A	N/A	N/A	N/A

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

If no External Sharing listed on the table above, ***(State there is no external sharing in both the risk and mitigation fields).***

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.

Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.
This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

Privacy Risk: There is no sharing of data outside of the Department of Veterans Affairs.

Mitigation: There is no sharing of data outside of the Department of Veterans Affairs.

Section 6. Notice

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

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

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

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

VA provides notice to Veterans and their dependents on what information is collected on them and what that information is used for. This notice is provided in the Notice of Privacy Practices VA 10-163. Link provided in the appendix.

Specific to the FFP, Veterans and dependents of Veterans are not contacted prior to retrieving data. However, after the data is retrieved, Veterans and dependents of Veterans are notified in writing and afforded 60 days due process.

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

https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

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

1. The Enrollment and Eligibility Records VA SORN 147VA10 defines the information collected from Veterans, use of the information, and how the information is accessed and stored.

2. This Privacy Impact Assessment (PIA) also serves as a notice of this system and is available on the internet.

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

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress.

Veterans and dependents of Veterans must provide proof of a satisfied warrant during the due process period. When proof is not provided, the Veteran's or dependent of Veteran's health care benefits and services are terminated.

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.

Veterans and dependents of Veterans receiving care through the VA are provided the Notice of Privacy Practices. Veterans and dependents of Veterans verified as fugitive felons are not eligible to receive VA health care and services at VA's expense at 38 U.S.C. 5313B.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

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

Privacy Risk: Per 38 U.S.C. 5313B, VA has the authority to deny benefits to Veterans and dependents of Veterans who have been verified as fugitive felons. A notice is not provided to the Veteran or public because this system is internal to VA employees only.

Mitigation: Per 38 U.S.C. 5313B, VA has the authority to deny benefits to Veterans and dependents of Veterans who have been verified as fugitive felons. VA mitigates privacy impacts risk by ensuring user rights to access is limited by system permissions.

Section 7. Access, Redress, and Correction

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

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

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

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

The 60-day notification letter includes the Veteran's or dependent of Veteran's PII, including the warrant information. This provides the Veteran or dependent of the Veteran to

verify the information that was retrieved. The 60-day notification letter provides Veterans and dependents of Veterans a point of contact should they need additional information.

7.1b If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR)?

FFP system is not exempt from the Privacy Act.

7.1c If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information?

The FFP system is a Privacy Act system.

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.

If the warrant information is incorrect, the Veteran or dependent of the Veteran is advised to work with the issuing law enforcement agency to correct the erroneous information associated with their identifier. Supporting documentation is then provided to the VA by the veteran or dependent to support claim of misrepresentation.

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.

Guidance to correct erroneous information is provided in the 60-Day notification letter that is mailed to the Veteran or dependent of the Veteran.

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

The 60-day notification letter provides Veterans and dependents of Veterans with appeal rights and a point of contact at their local VA medical facility should they need additional information. Veterans or dependent of Veterans may also contact the Privacy Office at their local VA medical facility.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that information may be used for purposes other than for what it was intended for.

Mitigation: The 60-day notification letter provides Veterans and dependents of Veterans with appeal rights and a point of contact at their local VA medical facility should they need additional information. Veterans or dependent of Veterans may also contact the Privacy Office at their local VA medical facility. The letter is mailed only to the intended recipient and access to the system is limited based on user rights.

Section 8. Technical Access and Security

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

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

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

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

Access is requested and approved through the VHA LEAF workflow system. Supervisors and FFP management approve access and access roles via this system.

8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

No users from other agencies have access to the FFP system.

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

- Admin – access to Admin area, edit all cases, read all cases, manage users
- Admin Viewer – access to Admin area, read all cases, read users list, NO edit access
- Facility – read and edit their own facility-specific cases, read/search other facility cases, request case transfer
- VISN – read their own VISN-specific cases, request case transfer
- Viewer – read cases, request case transfer

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

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII. This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.

VA contractors must take annual HIPAA training, Security and Privacy Awareness Training and sign the Contractor Rules of Behavior.

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.

VA employees with access to VA sensitive information are required to take the VA Privacy and Information Security Awareness and Rules of Behavior training annually, as well as Privacy and HIPAA Focused Training.

8.4 Has Authorization and Accreditation (A&A) been completed for the system? No

8.4a If Yes, provide:

1. *The Security Plan Status: N/A*
2. *The System Security Plan Status Date: N/A*
3. *The Authorization Status: N/A*
4. *The Authorization Date:* N/A
5. *The Authorization Termination Date: N/A*
6. *The Risk Review Completion Date:* N/A
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* N/A

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

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

FFP is a minor application currently covered under the Area Atlanta information system enclave, eMASS entry 508, system ID# 678. FIPS 199 classified moderate risk. Authority to Operate (ATO) signed 22 May 2022 by the Authorizing Official (AO), Dewaine Beard. The ATO expires on 21 May 2025.

Section 9 – Technology Usage

The following questions are used to identify the technologies being used by the IT system or project.

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

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.

Currently it does not use cloud technology.

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract).

(*Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

N/A

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

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.

This question is related to privacy control DI-1, Data Quality.

N/A

9.4 NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

N/A

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

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

N/A

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

SHIRLEY HOBSON

Digitally signed by SHIRLEY HOBSON
Date: 2024.11.14 08:50:39 -06'00'

Privacy Officer, Shirley P. Hobson

Knight, Howard (HEC ISSO)

Digitally signed by Knight, Howard (HEC ISSO)
Date: 2024.11.08 07:02:07 -05'00'

Information Systems Security Officer, Howard Knight

WILLIAM BROCK

Digitally signed by WILLIAM BROCK
Date: 2024.11.08 11:31:36 -05'00'

Information Systems Owner, William Brock

APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy; a Privacy Act notice on forms; screen shot of a website collection privacy notice).

Notice of Privacy Practices
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

HELPFUL LINKS:

General Records Schedule
https://www.archives.gov/records-mgmt/grs.html

National Archives (Federal Records Management):
https://www.archives.gov/records-mgmt/grs

VA Publications:
https://www.va.gov/vapubs/

VA Privacy Service Privacy Hub:
https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):
VHA Notice of Privacy Practices
VHA Handbook 1605.04: Notice of Privacy Practices