Privacy Impact Assessment for the VA IT System called:

Functional Status and Outcome Database

Enterprise Program Management Office (EPMO)

Date PIA submitted for review:

07/12/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Nancy Katz Johnson	Nancy.katz-johnson@va.gov	203-535-7280
Information System Security Officer (ISSO)	Gallegos Griselda	Griselda.Gallegos@va.gov	512-326-6037
Information System Owner	Brown Christopher	christopher.brown1@va.gov	202-270-1432

Abstract

The Functional Status and Outcomes Database (FSOD) system offers rehabilitation clinicians and managers the ability to track outcomes through the full continuum of rehabilitative care. Through FSOD, clinicians and managers gather functional outcome data for the entire time a patient receives rehabilitation care, covering the time in a formal rehabilitation bed unit and across all other inpatient and outpatient settings. The goal is to ensure valid and reliable outcomes at all VA facilities. This database was established in June 1994, through a cooperative agreement between the VHA Central Office of Physical Medicine and Rehabilitation, the Netsmart Technologies Inc (Netsmart) and the Austin Information Technology Center (AITC). Developed by Netsmart, it's the largest national registry of standardized information of medical rehabilitation inpatients in the United States. The Department of Veterans Affairs was given permission to develop this product for their use, but the VA's version is known as FSOD. FSOD collects recovery data on patients. (FSOD) is based upon the Functional Independence Measure (FIM™), a valid and reliable disability assessment tool. Developed by Netsmart, the largest national registry of standardized information of medical rehabilitation inpatients in the United States, FIM™ is considered to be the rehabilitation industry standard. FIM (FSOD) application has an average of 150 users.

Overview

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

1 General Description

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

Functional Status and Outcome Database - Enterprise Program Management Office (EPMO)

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

The Functional Status and Outcome Database (FSOD) for Rehabilitation offers rehabilitation clinicians and managers the ability to track outcomes through the full process of rehabilitative care. Through FSOD, clinicians and managers gather functional outcome data for the entire time a patient spends in a rehabilitation program and across inpatient and outpatient settings. The goal is to ensure valid and reliable outcomes at all VHA facilities. VHA facilities, as determined here, are all VA hospitals with Rehabilitation Services.

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

Enterprise Program Management Office (EPMO)

2. Information Collection and Sharing

A. 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 over 340,000 clients in the database. Annually over 7,000 cases are entered for veterans receiving in-patient rehabilitation.

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

- FSOD establishes the platform for VA rehabilitation teams to collect and monitor objective functional outcomes for veterans receiving in-patient rehabilitation. FSOD provides functional outcome data for the entire time a patient spends in a formal rehabilitation bed unit and across inpatient and outpatient settings, ensuring valid and reliable outcomes at all VA facilities.
- FSOD is based upon the Functional Independence Measure (FIM™), a valid and reliable disability assessment tool. Developed by Netsmart, the largest national registry of standardized information of medical rehabilitation inpatients in the United States, FIM™ has been considered to be the rehabilitation industry standard.

- This database was established in June 1994, through a cooperative agreement between the VHA Central Office of Physical Medicine and Rehabilitation, Uniform Data System for Medical Rehabilitation http://www.udsmr.org/ and AITC (http://www.cdco.va.gov/).
    - Netsmart Technologies Inc (Netsmart) purchased UDSmr in 2022 (https://www.ntst.com/)

- There are several components to the FSOD data flow that include both manual and batch processes:
    - **Data Management Interface (DMI QUEUE)**: This process allows the rehabilitation health data to be collected from VHA facilities in a file on the AITC mainframe on a Monday through Friday basis. It is formatted to allow FSOD (FIM™) to receive the data.
    - **CPRS**: This process allows FSOD (FIM™) to collect rehabilitation health data file from the AITC mainframe and insert it into its database. The process includes a check process for verifying completion of the database insert. See PFIMCHK below for how failures are handled.
    - **PFIMCHK**: This process runs only in the event the database insert process fails. A check is run for a file telling the mainframe that FSOD (FIM™) completed its database insert. If the file is not found, a message is sent via email to notify key person that the data needs to be verified and resent for processing.

- The following two processes have components that are external to the VA and documented in Interconnection Security Agreements and Memorandums of Understand (ISA MOUs):
    - **MedTel**: There are two processes that run between the FSOD system and MedTel. First, there is a monthly VB6 job that runs on the 20th of each month which exports discharged cases from The FSOD database from the previous month for facilities that have a contract with MedTel. The data is then uploaded via secure web page to the MedTel server. Second, there is a quarterly VB 6process that updates the FSOD database with case information gathered and analyzed by MedTel.
    - **Netsmart Technologies Inc (Netsmart) [previously known as Uniform Data Systems (UDS)]**: This process involves two steps: collecting quarterly discharges and follow-up assessment records from FSOD and transferring (via secure ftp) the assessment data to the Netsmart ftp server.

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

FSOD shares FIM based data with Netsmart for aggregate outcome reporting for VA Rehabilitation programs and also PHI data with MedTel to assist in collecting follow up FIM based outcomes on Veterans completing inpatient rehabilitation

D. *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.*

FSOD is a national application with accounts available for all VHA facilities.

3. Legal Authority and SORN

A. *A citation of the legal authority to operate the IT system.*

The legal authority for operating the information system comes from the Privacy Act of 1974, 5 U.S.C. 552a(e) and Title 38, Veterans' Benefits, Part III, Sections 3100-3122, Readjustment and Related Benefits. Covered under SORN National Patient Databases-VA'' (121VA10).

B. *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?*

No changes are expected to the existing records.

D. System Changes

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

No changes anticipated

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

No technology changes anticipated

Section 1. Characterization of the Information

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

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

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

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

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1.

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

☒ Name
☒ Social Security Number
☒ Date of Birth
□ Mother's Maiden Name
☒ Personal Mailing Address
☒ Personal Phone Number(s)
□ Personal Fax Number
□ Personal Email Address
□ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
□ Financial Information

□ Health Insurance Beneficiary Numbers Account numbers
□ Certificate/License numbers*
□ Vehicle License Plate Number
□ Internet Protocol (IP) Address Numbers
□ Medications
□ Medical Records
☒ Race/Ethnicity
□ Tax Identification Number
□ Medical Record Number
☒ Gender

□ Integrated Control Number (ICN)
□Military History/Service Connection
□ Next of Kin
☒ Other Data Elements (list below)

Other Data Elements - Patient Marital Status, Facility ID, Care Class Code, Impairment Code, Onset Date, Diagnosis Codes, Etiology Code, Asia Code, Admission Dates, Discharge Dates, Transfer Dates, Return Dates, Therapy Dates, Assessment Dates, and Rehabilitation Assessments Scores.

VHA Facility Coordinators collect the Rehabilitation Health Information for their patients and load this information into HL7 protocol format records. This information is collected through the DMI

QUEUE to be inserted into FIM™. Data is also entered directly into FSOD by the VHA Facility Coordinator, with manual review/completion of each case required in FSOD to reach Netsmart (completed) status.

PII Mapping of Components (Servers/Database)

Functional Status and Outcomes Database (FSOD) consists of 1 key component (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by FSOD and the reasons for the collection of the PII are in the table below.

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

Internal Database Connections

Database Name of the information system collecting/storing PII	**Does this system collect PII? (Yes/No)**	**Does this system store PII? (Yes/No)**	**Type of PII (SSN, DOB, etc.)**	**Reason for Collection/ Storage of PII**	**Safeguards**
VistA FIM Tool	Yes	Yes	Assessment records (Name, Social Security Number, Date of Birth, Personal Mailing Address, Personal Phone Number(s), Personal Email Address, Race/Ethnicity, Gender)	Patient demographics when FIM to CPRS is used.	SSOi access

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?

VHA Facility Coordinators collect the Rehabilitation Health Information (Patient ID/SSN, Patient Birthdate, Patient Address, Patient Phone Number, Patient Marital Status, Patient Gender, Patient Ethnicity, Facility ID, Care Class Code, Impairment Code, Onset Date, Diagnosis Codes, Etiology Code, Asia Code, Admission Dates, Discharge Dates, Transfer Dates, Return Dates, Therapy Dates, Assessment Dates, and Rehabilitation Assessments Scores) for their patients and load this information into HL7 protocol format records. This information is collected through the DMI QUEUE to be inserted into FIM™. Data is also entered directly into FSOD by the VHA Facility Coordinator, with manual review/completion of each case required in FSOD to reach Netsmart (completed) status.

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.

MedTel is used to capture follow up FIM scores for inpatient rehabilitation programs in VHA.

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

MedTel LLC collects and transmits follow up FIM scores back to FSOD.

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?

There are two ways that data is entered into FSOD. The first method used is VHA Facility Coordinators collect the Rehabilitation Health Information using the Veterans Health Information Systems and Technology Architecture (VISTA) Function Independence Measure (FIM™) Tool. This application is outside the FSOD (FIM™) accreditation boundary. The means of collection for FSOD (FIM™) is a sFTP from the AITC mainframe. The second method of data entry is directly into FSOD which is access through the Citrix portal.

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

Use of a paper form is not required by any national directive. Cannot speak to individual facility practice.

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.

The FSOD (FIM™) system assumes that the original source data was checked for accuracy when it was first entered into the source systems. Data can be checked for completeness by system audits, manual verifications, and annual questionnaires through automated Veteran letters.

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

N/A

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

Authority for Maintenance of the System is Title 38 USC Section 501 and Title 38, Chapter 31, Sections 3100-3122.: To provide for all services and assistance necessary to enable veterans with service-connected disabilities to achieve maximum independence in daily living and, to the maximum extent feasible, to become employable and to obtain and maintain suitable employment.

> *Covered under* National Patient Databases-VA’’ (121VA10). AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 38 United States Code Section 501.

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?
This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

Privacy Risk: FSOD (FIM™) collects its data from an external source, there is a risk that data could be corrupted during data transfer and/or host system data entry.

Mitigation: If the data file is corrupted, FSOD (FIM™) would request the data file be resent. There is a check in place to see if the data insertion is completed and if not, an email is sent to key personnel. Data entry errors would have to be addressed at the host system.

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.

- Patient Name - is used to verify Veteran/patient identity.
- Social Security Number - Used as a patient identifier and as a resource for verifying income information with the Social Security Administration.
- Date of Birth – is used to verify Veteran/patient identity.
- Patient Address - Used to verify Veteran/patient identity as well as for correspondence.
- Personal Phone Number(s) - Used to verify Veteran/patient identity as well as for communication.
- Race/Ethnicity - is used to verify Veteran/patient identity.
- Gender - is used to verify Veteran/patient identity.

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.

FSOD (FIM™) has a reporting component which provides summary and individual patient listing reports to end users to assist with facility level analysis of the patient rehabilitation data. It also does provide discharged case information to External Data Partner, MedTel, to be analyzed and receives the analytic result back from MedTel. This exchange of information ensures valid and reliable outcomes at all VHA facilities.

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.

N/A

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?

For Data at Rest, the storage device used to collect, process and/or retain Social Security Numbers is an Encrypted Storage Array which is FIPS-140 certified. For Data in Transit, the Oracle database uses Oracle Native Network Encryption to protect data in transit. It provides data network encryption and integrity to ensure that data is secure as it travels across the network from Client to Database server and back. Oracle Database supports the Federal Information Processing Standard (FIPS) encryption algorithm, Advanced Encryption Standard (AES).

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

All data protected as outlined in 2.3a above

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

All data protected as outlined in 2.3.a above

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

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

2.4a How is access to the PII determined?

Access to PII is processed through the e9957 process. Local approval from supervisors and designated authorization officials are required prior to granting access to the database. Most recent user login is accessible through the user table to the application.

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

The SORN defines the information collected from veterans, use of the information, and how the information is accessed and stored. The information collected is used for determining a veteran' s benefits, such as compensation or education.

National Patient Databases-VA'' (121VA10). specifies the purpose and routine uses associated with this System of Record. The official System of Records Notice (SORN) is the "National Patient Databases-VA" (121VA10) at 2023-07638.pdf (govinfo.gov)
FSOD (FIM™) is used by Rehabilitative Clinicians and Manager to track patient outcomes throughout the full process of rehabilitative care. Information is provided through the processes outlined in the system overview.

2.4c Does access require manager approval?

Yes

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

Yes

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

Each FSOD/ FIM user is authorized by the appropriate supervisor at their local site and is granted access to FSOD/ FIM and is assigned to the security level deemed appropriate to fulfill their job duties.

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*

- Patient Name
- Patient SSN
- Date of Birth
- Patient Address
- Patient Personal Phone Number
- Patient Race/Ethnicity
- Patient Marital Status
- Facility ID
- Care Class Code
- Impairment Code
- Onset Date
- Diagnosis Codes
- Etiology Code
- Asia Code
- Admission Dates
- Discharge Dates
- Transfer Dates
- Return Dates
- Therapy Dates
- Assessment Dates
- Rehabilitation Assessments Scores

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.*

The records are disposed of in accordance with POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Records in this system are retained and disposed of in accordance with the schedule approved by the Archivist of the United States, General Records Schedule, 5.2, item 020.

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.

SORN 121VA10 states: in accordance with the SORN, Records in this system are retained and disposed of in accordance with the schedule approved by the Archivist of the United States, General Records Schedule, 5.2, item 020. (https://www.archives.gov/files/records-mgmt/grs/grs05-2.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.

Disposition of Electronic Data:

Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with the Department of Veterans' Affairs Handbook 6500.1, section 2.b.(5) (February 24, 2021), https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=1254&FType=2.

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 per VA Handbook 6500.1.Electronic media sanitization, when the records are authorized for destruction (or upon system decommission), will be carried out in accordance with VA Directive 6500 VA Cybersecurity Program.

Disposition of Printed Data:

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

Forms and other types of printed output produced by any computer systems and related peripherals will be evaluated by the responsible staff member for data sensitivity. Printed output containing sensitive data will be stored in locked cabinets or desks and disposed of properly (when the approved records schedule permits destruction) by shredding or similar VA approved methods in Version Date: February 27, 2020, Page 13 of 29 accordance with VA Directive 6371.

Program listings and documentation relating to the use of or access to a computer system require special handling if the listings or documentation provide information about a system which processes sensitive data. VA personnel are responsible for retrieving/removing all printed outputs they request from printers.

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.

At the database level, the controls implemented to protect PII are referenced in section 2.3. Specific PII protection and controls for research, testing and/or training should be implemented at the application level. Procedures are in place to scramble PII information to mitigate security concerns.

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?*

<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:

<u>Privacy Risk:</u> There is a risk that the information maintained by FSOD (FIM™) could be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached.

<u>Mitigation:</u> To mitigate the risk posed by information retention, FSOD (FIM™) adheres to the NARA General Records Schedule. When the retention date is reached for a record, the individual's information is carefully disposed of by the determined method as described in General Records Schedule 5.2 item 20.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
VISTA FIM Tool	VHA	Patient Rehabilitation Information	sFTP of HL7 data

4.2 <u>PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure</u>

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:

<u>Privacy Risk:</u> There is a risk that data contained in FSOD (FIM™) may be shared with unauthorized individuals or that those individuals, even with permission to access the data, may share it with other individuals.

<u>Mitigation:</u> All users of the system are VA users. All VA users with access to Veteran’s information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually. FSOD (FIM™) adheres to all information security requirements instituted by the VA Office of Information Technology (OIT). Information is shared in accordance with VA Handbook 6500. Access to veteran data for use is under Title 38 U.S.C. Section 5106.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

NOTE: Question 3.10 on Privacy Threshold Analysis should be used to answer this question.

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

For each interface with a system outside VA, state what specific data elements (PII/PHI) are shared with each specific partner.

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

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.
This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

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

MedTel Outcomes LLC	MedTel	SSN, Name, Address	ISA/MOU	Site to Site (S2S) VPN Tunnel
Netsmart Technologies Inc	Netsmart	PHI, demographics, and rehabilitation outcomes.	ISA/MOU	Site to Site (S2S)

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 the data could be shared with an inappropriate and/or unauthorized external organization or institution.

Mitigation: The potential harm is mitigated by access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information integrity, security assessment and authorization, incident response, risk assessment, planning and maintenance. All personnel with access to Veteran's information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually.

- FSOD (FIM™) adheres to all information security requirements instituted by the VA Office of Information Technology (OIT).
- Information is shared in accordance with VA Handbook 6500.
- All personnel accessing Veteran's information must first have a successfully adjudicated fingerprint check. This fingerprint check is conducted by the Federal Bureau of Investigation(FBI) Justice Information and criminal history records. Individual users are given access to Veteran's data through the issuance of a user ID and password, and by the use of a Personal Identity Verification (PIV) card. This ensures the identity of the user by requiring two-factor authentication.

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.

Collection of information is done outside the accreditation boundary of FSOD (FIM™). FSOD (FIM™) only receives electronic data. While notice is not provided directly to individuals that FSOD (FIM™) is using their data contained in other VA IT systems, this PIA does serve as notice of the system's existence and its SPI collection use, maintenance, and dissemination practices.

The Department of Veterans Affairs does provide public notice that the system does exist. This notice is provided below:

The VHA Notice of Privacy Practice (NOPP) https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946 explains the collection and use of protected health information to individuals receiving health care from VA. The NOPP is mailed every three years or when there is a major change to all enrolled Veterans. Non Veterans receiving care are provided the notice at the time of their encounter.

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

Notice is also provided in the Federal Register with the publication of the SORN: "
(121VA10 at 2023-07638.pdf (govinfo.gov)

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

N/A

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

N/A

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

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

Individuals' ability to decline to provide information is based on the needs and practices of the originating VA IT systems. Individuals do not have the opportunity to decline to provide information to FMS because information is not collected directly from them.

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.

Information is used, accessed and disclosed in accordance with the Privacy Act, 5 USC 552a, Title 38 USC 5701, Confidential Nature of Claims, Title USC 7332 and the HIPAA Privacy Rule 45 CFR.
Individuals are provided with a copy of the Notice of Privacy Practices that indicates when information will be used without their consent and when they will be asked to provide consent. Information is used, accessed and disclosed in accordance with the Privacy Act, 5 USC 552a, Title 38 USC 5701, Confidential Nature of Claims, Title USC 7332 and the HIPAA Privacy Rule 45 CFR.

Individuals or their legal representative may consent to the use or disclosure of information via a written request submitted to their facility Privacy Officer. Individuals also have the right to request a restriction to the use of their information. The written request must state what information and/or to whom the information is restricted and must include their signature and date of the request. The request is then forwarded to facility Privacy Officer for review and processing. Individuals may also request to Opt-Out of the facility directory during an inpatient admission. If the individual chooses to opt-out, information is not disclosed from the facility directory unless otherwise required by law.

6.4 <u>PRIVACY IMPACT ASSESSMENT: Notice</u>

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:

<u>Principle of Transparency:</u> Has sufficient notice been provided to the individual?

<u>Principle of Use Limitation:</u> 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:

<u>Privacy Risk:</u> There is a risk that individuals who provide their SPI and Patient Rehabilitation Health information will not know how their information is being shared and used internally at the Department of Veterans Affairs.

<u>Mitigation:</u> This risk is mitigated by the common practice of providing the NOPP when Veterans apply for benefits. Additionally, new NOPPs are mailed to beneficiaries at least every 3 years and periodic monitoring is performed to check that all employees are aware of the requirement to provide guidance to Veterans and that the signed acknowledgment form, when applicable, is scanned into electronic records, The NOPP is also available at all VHA medical centers from the facility Privacy Officer.
The System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) are also available for review online, as discussed in question 6.1.

Section 7. Access, Redress, and Correction

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

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

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

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

VHA Directive 1605.01, Privacy and Release of Information, outlines policy and procedures for VHA and its staff to provide individuals with access to and copies of their PII in compliance with the Privacy Act and HIPAA Privacy Rule requirements. VHA also created VA form 10-5345a for use by individuals in requesting copies of their health information under right of access.VA Form 10-5345a is voluntary but does provide an easy way for individual to request their records.

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

N/A

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

N/A

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

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed. If the correction procedures are the same as those given in question 7.1, state as much. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Individuals are required to provide a written request to amend or correct their records to the appropriate Privacy Officer or System Manager as outlined in the Privacy Act SOR. Every Privacy Act SOR contains information on Contesting Record Procedure which informs the individual who to contact for redress. Further information regarding access and correction procedures can be found in the notices listed in Appendix A. The VHA Notice of Privacy Practices also informs individuals how to file an amendment request with VHA.

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.

Notification for correcting the information must be accomplished by informing the individual to whom the record pertains by mail. The individual making the amendment must be advised in writing that the record has been amended and provided with a copy of the amended record. The System Manager for the concerned VHA system of records, the facility Privacy Officer, or their designee, must notify the relevant persons or organizations who had previously received the record about the amendment. If 38 U.S.C. 7332-protected information was amended, the individual must provide written authorization to allow the sharing of the amendment with relevant persons or organizations request to amend a record must be acknowledged in writing within 10 workdays of receipt. If a determination has not been made within this time period, the System Manager for the concerned VHA system of records or designee, and/or the facility Privacy Officer, or designee, must advise the individual when the facility expects to notify the individual of the action taken on the request. The review must be completed as soon as possible, in most cases within 30 workdays from receipt of the request. If the anticipated completion date indicated in the acknowledgment cannot be met, the individual must be advised, in writing, of the reasons for the delay and the date action is expected to be completed. The delay may not exceed 90 calendar days from receipt of the request.

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.

If the individual discovers that incorrect information was provided during intake, they simply follow the same contact procedures as before, and state that the documentation they are now providing supersedes that previously provided.

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:
<u>Principle of Individual Participation:</u> Is the individual provided with the ability to find out whether a project maintains a record relating to him?

<u>Principle of Individual Participation:</u> 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?

<u>Principle of Individual Participation:</u> 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:

<u>Privacy Risk:</u> There is no direct way for individuals to review or correct their information in FSOD (FIM™), there is a risk that the system may submit inaccurate data for external analysis.

<u>Mitigation:</u> The FSOD (FIM™) application resides on a server that is physically housed in a government-owned building, Austin Information Technology Center (AITC), Austin, Texas. Only employees of the Department of Veterans Affairs and VA contractors occupy the building. It is not open to the general public. AITC provides system operations and maintenance service for FSOD (FIM™). Overall security for FSOD (FIM™) is provided by AITC personnel and procedures. These procedures include providing change control for the server connectivity, providing physical security for the equipment, and providing security for access to the information system. AITC system administrators keep the FSOD (FIM™) servers up to date with all the latest software security patches and new software applications where indicated.

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.

There are no users other than administrators for FSOD (FIM™) application. Administrators complete a e9957 (Access Form) for access and completes training as noted below. Per VA Directive and Handbook 6330, every 5 years the Office of Information & Technology (OI&T) develops, disseminates, and reviews/updates a formal, documented policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among entities, and compliance; along with formal, documented procedures to facilitate the implementation of the control policy and associated controls. OI&T documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and retains individual training records for 7 years. This documentation and monitoring is performed the Talent Management System (TMS).The approved e9957 then is forward to the development team and an account creation request is created in Service Now (SNow) to document the record creation. The Approved e9957 is attached the SNow ticket.

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?

There are developers and database analysts that will have access to the system for administrative and software maintenance. The CIO will establish department-wide requirements, and provide oversight and guidance related to the protection of personally identifiable information (PII) including PHI throughout VA.

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.

Developers and database analysts do not have the ability to amend any information. Their duties are for support of the software.

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.*

FSOD (FIM™) administrators may be authorized VA and contract employees. There are contract system administration personnel within the Austin Information Technology Center (AITC) who maintain the server hardware and software.
Contracts are reviewed annually by the FSOD (FIM™) Program Manager, Information System Owner, Information Owner, Contract Officer, Privacy Officer, and the Contracting Officer's Technical Representative. Contracting Officer's Representative. This review is conducted each time the contract period expires.

- Individuals are subject to a background investigation before given access to Veteran's information.
- All personnel with access to Veteran's information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually.
- VA maintains Business Associate Agreements (BAA) and Non-Disclosure Agreements with contracted resources in order to maintain confidentiality of the information.
- Personnel including contractors that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training which all personnel must complete via the VA's Talent Management System (TMS). After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system.
- After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system.

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.

Personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the VA Privacy and Information Security awareness training which all personnel must complete via the VA's Talent Management System (TMS). After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system. VA users with access to protected health information must complete mandatory HIPAA Privacy training annually in TMS .

VA requires Privacy and Information Security Awareness training be completed on an annual basis. The Talent Management System offers the following applicable privacy courses:

- VA 10176: Privacy and Information Security Awareness and Rules of Behavior
- VA 10203: Privacy and HIPPA Training
- VA 3812493: Annual Government Ethics

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* January 3rd 2023
3. *The Authorization Status:* 365 Day ATO
4. *The Authorization Date:* February 20th 2023
5. *The Authorization Termination Date:* February 20th 2024
6. *The Risk Review Completion Date:* February 9th 2023
7. *The FIPS 199 classification of the system MODERATE*
8. *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. N/A***

Section 9 – Technology Usage

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

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

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

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

No.

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**

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

Signature of Responsible Officials

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

NANCY KATZ-JOHNSON

Digitally signed by NANCY KATZ-JOHNSON
Date: 2023.09.19 14:17:33 -04'00'

Privacy Officer, Nancy Katz Johnson

Griselda Gallegos 204736

Digitally signed by Griselda Gallegos 204736
Date: 2023.09.20 12:30:49 -05'00'

Information System Security Officer, Gallegos Griselda

CHRISTOPHER BROWN

Digitally signed by CHRISTOPHER BROWN
Date: 2023.09.21 11:13:36 -05'00'

Information System Owner, Brown Christopher

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).

Link to VA Privacy Website: https://www.va.gov/privacy/

Link to VHA Notice of Privacy Practices:
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=3048

HELPFUL LINKS:

Record Control Schedules:

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

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

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

National Archives (Federal Records Management):

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

VHA Publications:

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

VA Privacy Service Privacy Hub:

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

Notice of Privacy Practice (NOPP):

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices