



Privacy Impact Assessment for the VA IT System called:

FLOW3: Enterprise Prosthetic Limb Workflow Management System Veterans Health Administration (VHA) Rehabilitation and Prosthetics Service

Date PIA submitted for review:

September 26, 2023

System Contacts:

System Contacts

		E-mail	Phone Number
Privacy Officer	<i>Dennis Lahl</i>	<i>Dennis.lahl@va.gov</i>	202-461-7330
Information System Security Officer (ISSO)	<i>Ralph Aguilar</i>	<i>Ralph.aguilar@va.gov</i>	310-478-3711
Information System Owner	<i>Jeffrey Bott</i>	<i>Jeffrey.bott@va.gov</i>	219-779-0100

Abstract

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

The FLOW system provides a total solution for the tracking, reporting, and workflow management of the artificial limb fabrication process from prescription to final delivery and check out. FLOW3 is a system of prosthetic limb care that creates a predictable, consistent, and high-quality Veteran experience across VHA.

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.*

FLOW3: Enterprise Prosthetic Limb Workflow Management System
Rehabilitation and Prosthetics Service (12RPS4) and VHA owned.

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

FLOW3 streamlines prosthetic limb processing by integrating disparate processes/systems, automating many manual processes in use today (e.g., creating documents automatically for the Prosthetic and Sensory Aide [PSAS] technician, etc.), ultimately providing greater transparency into the prosthetic limb acquisition workflow. It also standardizes the purchase request and coding process for Prosthetic limb acquisition and enhances follow up for clinical care.

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

The system is VHA developed and owned.

2. Information Collection and Sharing

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

There are approximately 90,000 Veterans with limb loss currently in VA. About 14,000 Veterans receive prosthetic limbs or repairs to limbs annually. The clinicians and support staff who care for these Veterans are the clients of the system along with the program office which oversees the program.

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

The system contains prescriptions for artificial limbs, repairs to limbs, supplies for limbs, the Veterans who receive these prescriptions along with various information relating to the provision of the limbs, such as the actions and dates of actions taken to provide the care.

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

At a high-level, FLOW3 is dashboard based, so that staff can look up an order status at each stage of processing (i.e., from Prosthetics order entered by the clinician to the purchase order entered by the purchasing agent) and is comprised of a database backend, a web application for user interaction, and reporting. Information comes from the Corporate Data Warehouse into the FLOW3 database. The FLOW3 database information is displayed using the Web App and various reports.

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

The system is hosted in the Hines Information Technology Center (HITC) in Hines, Illinois, and used VA-wide in multiple VA Medical Centers (VAMCs) by internal VA Staff. Controls in FLOW3 do not vary based on the VAMC (user) accessing it; user roles are established using the Corporate Data Warehouse (CDW) / Computerized Patient Record System (CPRS) per VA employee at their respective VAMC, and if elevated privileges are needed, by the FLOW3 staff.

3. *Legal Authority and SORN*

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

FLOW3 is provided under –Public Law 114-31; Veteran Information: Title 38, United States Code, Section 5107, Title 38, United States Code, Section 5106, and Title 38 United States Code 5701. Title 38, United States Code, section 81 11 (38 U.S.C. 5811 I), titled "Sharing of Department of Veterans Affairs and Department of Defense Health Care Resources." "Title 10, United States Code, section 1104 (10 U.S.C.5 1104), titled "Sharing of Resources with the Department of Veterans Affairs," which incorporates Title 31, United States Code, section 1535 (31 U.S.C. 51 535), titled "Agency Agreements," also known as the "Economy Act." E-government Act of 2002 (44 U.S.C. §208(b)). 38 United States Code 5706.

FLOW3 is covered under VA SORN (System of Records Notice) #79VA10P2 – Veterans Health Information Systems and Technology Architecture (VistA) Records-VA

- 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?*

The SORN does not require amendment or revision/approval. The system does not utilize cloud technology.

D. *System Changes*

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

None identified

K. Whether the completion of this PIA could potentially result in technology changes
None identified

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:

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

No Additional Information Collected

PII Mapping of Components (Servers/Database)

Version Date: October 1, 2022

Page 4 of 28

FLOW3 consists of **1** key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **FLOW3** 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
RPS_STAGE	Yes	Yes	SSN, DOB, Name	Identification of individuals receiving care	Hosted internally, used on internal networks, controlled physical and logical access, only approved and authorized users granted access to application based on least privilege/need-to-know. Data encrypted in use, in transit, and at rest.

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?

All information is acquired from the Corporate Data Warehouse (CDW) or from Cerner via Veteran Data Integration and Federation (VDIF). No information is collected from individuals.

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.

Information is pulled in from the patient's authoritative electronic health record.

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

N/A

1.3 How is the information collected?

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

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

Information is electronically acquired from CDW via Extract/Transform/Load (ETL) technology or from Cerner via HL7 messaging. FLOW3 does not alter any original data, instead the system models this information.

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.

N/A

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.

Accuracy reliance is on CDW data as it is provided through and ETL job from the nightly CDW extract. Information is checked by VA Medical and Procurement professionals.

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

FLOW3 is provided under –Public Law 114-31; Veteran Information: Title 38, United States Code, Section 5107, Title 38, United States Code, Section 5106, and Title 38 United States Code 5701. Title 38, United States Code, section 81 11 (38 U.S.C. 5811 I), titled "Sharing of Department of Veterans Affairs and Department of Defense Health Care Resources." Title 10, United States Code, section 1104 (10 U.S.C.5 1104), titled "Sharing of Resources with the Department of Veterans Affairs," which incorporates Title 31, United States Code, section 1535 (31 U.S.C. 51 535), titled "Agency Agreements," also known as the "Economy Act." E-government Act of 2002 (44 U.S.C. §208(b)). 38 United States Code 5706.

FLOW3 is covered under VA SORN (System of Records Notice) #79VA10P2 – Veterans Health Information Systems and Technology Architecture (VistA) Records-VA

The Privacy Act of 1974, as amended, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. The authority of maintenance of the system listed in question 1.1 falls under Title 28, United States Code, title 38, U.S.C., sections 501(a), 1705, 1710, 1722, and 5317.

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: Name and Last 4 of SSN

Mitigation: Captured through “Notice of Privacy Practice.” The information that we have is already agreed to by the patient and documented in CPRS – The patient has already consented before we receive the information. Vista states, “The Notice of Privacy Practice (NOPP) is a document which explains the collection and use of protected information to individuals applying for VHA benefits. A signed statement acknowledging that they individual read and understood the NOPP is scanned into each applicant’s electronic file. When updates are made to the NOPP copies are mailed to all VHA beneficiaries. Employees and contractors are required to review, sign and abide by the National Rules of Behavior on an annual basis.”

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.

The PII/SPII Information used in FLOW3 is as follows

- Name: Used as an identifier (VA Staff, Patient)
- Social Security #: Used as a patient identifier
- DOB: Used as a patient identifier

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.

This system does not process or analyze the data submitted. The data provided is used to verify identity.

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.

- Consult Templates – entry point for prosthesis prescription by clinician
- Consult Comment Tool – used by Prosthetist to capture workload for order
- Web-Based Application for HCPCS Generation – used by purchasing agents to generate HCPC Lists

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?

Multi-factor authorization is required for authorized users to view the data.

All data is stored in a secure CDW database.

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

Full SSNs are never available to any users. Only the last 4 is displayed to provide ease in looking up a patient in the Computerized Patient Record System (CPRS).

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

End User Training Requirement: Talent Management System (TMS) Course VA 10176 / VA Privacy and Information Security Awareness and Rules of Behavior

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?

FLOW3 utilizes BISL permissions for access to information.

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

Yes, both in system documentation (some still in progress) and in the Governance Risk & Compliance (GRC) tool Enterprise Mission Assurance Support System (eMASS).

2.4c Does access require manager approval?

Manager approval is required to access CPRS which permissions flow to BISL for single local site access. For VISN access request required VISN system owner approval.

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

Only access to the system and appropriate site level data is controlled.

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

The FLOW3 ISO and ISSO.

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*

Veterans' name, date of birth, last 4 digits of the social security number, and control numbers are the PII data that is retained per the schedule below.

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.*

Medical Records Folder File or CHR (Consolidated Health Record) contains all professional and administrative material necessary to document the episodes of medical care and benefits provided to individuals by the VA health care system. The medical records folder will be retained in the VA health care facility until 3 years after last episode of care, and then converted to an inactive medical record. Once designated an inactive medical record, it will be moved to a VA records storage facility. Patient medical records are retained for a total of 75 years after the last episode of care. (Department of Veterans Affairs Record Control Schedule (RCS)-10, Section II: Human Resources Management, Item No. XLIII (dated January 2019)). FLOW3's data is not the official system of record; it is in fact a copy. FLOW3 copies of data will be deleted after five years or after the Veteran is deceased so we can maintain metrics measurements.

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. 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?

FLOW 3 does not fall under NARA because it is not a System of Record. Medical Records Folder File or CHR (Consolidated Health Record) contains all professional and administrative material necessary to document the episodes of medical care and benefits provided to individuals by the VA health care system. The medical records folder will be retained in the VA health care facility until 3 years after last episode of care, and then converted to an inactive medical record. Once designated an inactive medical record, it will be moved to a VA records storage facility. Patient medical records are retained for a total of 75 years after the last episode of care. (Department of Veterans Affairs Record Control Schedule (RCS)-10, Section II: Human Resources Management, Item No. XLIII (dated November 2017)). FLOW3's data is not the official system of record; it is in fact a copy. FLOW3 copies of data will be deleted after five years or after the Veteran is deceased so we can maintain metrics measurements.

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

FLOW 3 does not fall under NARA because it is not a System of Record. FLOW3's data is not the official system of record; it is in fact a copy. FLOW3 copies of data will be deleted after five years or after the Veteran is deceased so we can maintain metrics measurements.

GENERAL RECORDS SCHEDULE 3.2: Information Systems Security Records Disposition
Authority: DAA-GRS-2013-0006-0003 URL: <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.

FLOW 3 does not fall under NARA because it is not a System of Record. Medical Records Folder File or CHR (Consolidated Health Record) contains all professional and administrative material necessary to document the episodes of medical care and benefits provided to individuals by the VA health care system. The medical records folder will be retained in the VA health care facility until 3 years after last episode of care, and then converted to an inactive medical record. Once designated an inactive medical record, it will be moved to a VA records storage facility. Patient medical records are retained for a total of 75 years after the last episode of care. (Department of Veterans Affairs Record Control Schedule (RCS)-10, Section II: Human Resources Management, Item No. XLIII (dated November 2017)). FLOW3's data is not the official system of record; it is in fact a copy. FLOW3 copies of data will be deleted after five years or after the Veteran is deceased so we can maintain metrics measurements.

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.

- End User Training Requirement: Talent Management System (TMS) Course VA 10176 / VA Privacy and Information Security Awareness and Rules of Behavior
- End User Training Requirement: Talent Management System (TMS) Course VA 10203 / Privacy and HIPAA Training
- PII is not used in the FLOW3 System, only de-identified or test patients are used during training

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: Name, Last 4 digits of the Social Security Number, and Date of Birth.

Mitigation: FLOW3 copies of data will be deleted after five years or after the Veteran is deceased so we can maintain metrics measurements. FLOW3 only keeps and exposes the Patient Name and Last 4 of SSN – risk of using it is minimized. Full SSN is only used internally and never exposed to users.

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

<i>List the Program Office or IT System information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</i>	<i>Describe the method of transmittal</i>
MCAO	MCAO uses the information for cost accounting	SSN	SFTP transfer

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: All parties sharing this information are already able to access it in the EHR. Thus, it does not increase the risks from an internal sharing standpoint.

Mitigation: Existing mitigation techniques used to protect privacy from internal sharing and disclosure risks, such as trainings, will suffice as mitigation, since there is no increased risk. Enterprise Risk increases with the number of people having access to protected information.

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

<i>List External Program Office or IT System information is shared/received with</i>	<i>List the purpose of information being shared / received / transmitted with the specified program office or IT system</i>	<i>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program or IT system</i>	<i>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</i>	<i>List the method of transmission and the measures in place to secure data</i>
None	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.

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: FLOW 3 does not transmit information to any external entities.

Mitigation: FLOW 3 does not transmit information to any external entities.

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.

The Notice of Privacy Practice (NOPP) is a document which explains the collection and use of protected information to individuals applying for VHA benefits. Revisions are made to the NOPP every three years or when there is a major change and the NOPP is e mailed to all enrolled Veterans . Employees and contractors are required to review, sign and abide by the National Rules of Behavior on an annual basis.

6.1b If notice was not provided, explain why. If it was provided, attach a copy of the current notice. Not Applicable – these actions take place at the provider level outside of FLOW3. 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.

Not Applicable – these actions take place at the provider level outside of FLOW3.

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.

The patient's information is pulled from authoritative sources and is not changed within FLOW3.

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.

FLOW3 is not the SOR and does not manage the PII or correction thereof. This is accomplished by authoritative EHR at the provider level.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

Principle of Use Limitation: *Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?*

This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.

Follow the format below:

Privacy Risk: There is a risk that an individual may not receive notice that their information is being collected, maintained, processed, or disseminated by the Veterans' Health Administration prior to providing the information to the VHA.

Mitigation: This risk is mitigated by the common practice of providing the NOPP when Veterans apply for benefits. Additionally, new NOPPs are provided to beneficiaries and periodic monitoring is performed to check that the signed acknowledgment form has been scanned into electronic records. Employees and contractors are required to review, sign and abide by the National Rules of Behavior on a yearly basis as required by VA Handbook 6500 as well as complete annual mandatory Information Security and Privacy Awareness training. Additional mitigation is provided by making the System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) available for review online, as discussed in question 6.1 and the Overview section of this PIA.

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.

Since Flow3 only pulls from the EHR, patients can access their records using standard release of information procedures. Vista states, "There are several ways a veteran or other beneficiary may access information about them. The Department of Veterans' Affairs has created the MyHealthEVet program to allow online access to their medical records. More information on this program and how to sign up to participate can be found online at <https://www.myhealth.va.gov/index.htm> 1. Veterans and other individuals may also request copies of their medical records and other records containing personal data from the medical facility's Release of Information (ROI) office. VHA Directive 1605.01, Privacy and Release of Information, Paragraph 7 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).

Not Applicable

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.

Not Applicable

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.

FLOW3 is not the SOR and as such does not correct data. This is accomplished through actions associated with the authoritative EHR at the provider level. **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.

FLOW3 is not the SOR and as such does not correct data. This is accomplished through actions associated with the authoritative EHR at the provider level.

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 ensure data accuracy.***

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

FLOW3 is not the SOR and as such does not correct data. This is accomplished through actions associated with the authoritative EHR at the provider (and higher VA) level.

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: The procedures for correcting inaccurate or erroneous information are the same formal procedures that are applied broadly for VA Medical Records as cited in section 7.3.

Mitigation: The procedures for correcting inaccurate or erroneous information are the same formal procedures that are applied broadly for VA Medical Records as cited in section 7.3.

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.

FLOW3 utilizes BSL permissions, which requires Supervisor approval, for secure access

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?

Access to FLOW3 is limited to VHA staff only.

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.

General users have access to all data that they are authorized to view. These users are limited by BSL permissions and have limited access to change information. Administrators have access to system configuration data and are controlled by system administrator access only.

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.

No Contractors are involved with FLOW3

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.

- End User Training Requirement: Talent Management System (TMS) Course VA 10176 / VA Privacy and Information Security Awareness and Rules of Behavior
- End User Training Requirement: Talent Management System (TMS) Course VA 10203 / Privacy and HIPAA Training

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 18-Mar-2021
3. *The Authorization Status:* ATO
4. *The Authorization Date:* 01-Jun-2021
5. *The Authorization Termination Date:* 31-May-2024
6. *The Risk Review Completion Date:* 26-May-2021
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

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

Please provide response here

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)

On premises only; Hines Data Center – no cloud usage

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).

Not Applicable

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 they provided in this Privacy Impact Assessment is true and accurate.

Privacy Officer, Dennis Lahl

Information System Security Officer, Ralph Aguilar

Information System Owner, Jeffrey Bott

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).

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](#)