Privacy Impact Assessment for the VA IT System called:

CC (Community Care) Referral Documentation (REFDOC)

Veteran Health Administration (VHA)

Office of Integrated Veteran Care (IVC)

Date PIA submitted for review:

08/14/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Michael Hartmann	Michael.Hartmann@va.gov	303-780-4753
Information System Security Officer (ISSO)	Kimberly Keene	Kimberly.Keene@va.gov	401-248-5933
Information System Owner	Tony Sines	Tony.Sines@va.gov	316-249-8510

Abstract

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

The Community Care Referral Documentation System (REFDOC) project is focused on the enterprise implementation of a web application that is being used in local Veterans Affairs Medical Center's (VAMC) to allow VA staff to quickly pull information from Veterans Health Information Systems and Technology Architecture (VistA) and Corporate Data Warehouse (CDW) based on an individual's health record and place that information into a Portable Document Format (PDF) that can be shared with Community Providers for care coordination when a Veteran will be utilizing the Community Care network of external providers.

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.

The system has been designated the Community Care Referral Documentation System. The acronym for the system is REFDOC. It is sponsored by and serves the Community Care initiative.

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

REFDOC provides the external Community Care Program providers timely information on Veterans entrusted to their care. It automates and digitizes a manual process for extracting and gathering this information. Pulling data directly from VA databases, this application populates and generates a single PDF file with all of this information. It features a web-based interface for access from anywhere inside the VA network.

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

VA 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.

As this is an internal application only to the VA network, the typical users will be VA staff including VA Nurse Case Managers, Community Care Team Members, and Community Care Support Users. Currently the user information stored within REFDOC is for 15,178 users.

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

REFDOC provides the external Community Care Program providers timely information on Veterans entrusted to their care. It automates and digitizes a manual process for extracting and gathering this information. Pulling data directly from VA databases, this application populates and

generates a single PDF file with all of this information. It features a web-based interface for access from anywhere inside the VA network.

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

REFDOC interfaces with Veterans Data Integration and Federation (VDIF)//VistA and CDW for data calls and queries to these databases. After the information is collected in a PDF file by a user, the user saves it to the user's local hard drive or shared drive. This is where the REFDOC chain of custody ends. REFDOC has no responsibility for what the user does with the file after it is created. It is the user's responsibility to dispose of the PII, sensitive personal information (SPI), and PHI in the file. The user may send the file to a Community Care provider via encrypted email or via a third-party portal. Again, as REFDOC is a VA intranet application, it is the responsibility of the user to safeguard the PII and PHI in the file from that point forward. REFDOC is not involved in any way with the transmission of the PDF to a third party, e.g., an external provider in the Community Care network

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.

REFDOC is located within the VAEC Cloud.

3. Legal Authority and SORN

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

79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records - VA (12/23/2020)
172VA10, VHA Corporate Data Warehouse - VA (12/22/2021).
Title 38, United States Code, section 7301(a)
Title 38, United States Code, Sections 501(b) and 304
Title 38, United States Code (U.S.C.), Chapter 1, 3 & 17, Veterans' Benefits
Executive Order 9397, Numbering System for Federal Accounts Relating to the Individual Persons
Executive Order 13478, Amendment to Executive order 9397 Relating to Federal Agency Uses of Social Security Numbers (Nov 2008)
Title 38 of U.S.C., Section 1705(c) (1)(2)
Pub. L. 104-262, SEC 104. Management of Health care, SEC 1705. Management of Health care: patient enrollment system. SEC 1706 Management of Healthcare: other requirements (a) (b) (1)
5 U.S.C. 552a, "Privacy Act," c. 1974 o 5 U.S.C. 552, "Freedom of Information Act," c. 1967 HIPAA Privacy Rule, 45 C.F.R. Part 164, Standards for Privacy of Individually Identifiable Health Information
VA Claims Confidentiality Statute 38 U.S.C. 552
Confidentiality of Certain Medical Records, 38 U.S.C. § 7332
Federal Information Security Management Act (FISMA) of 2002
OMB M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002
The Freedom of Information Act, as amended 5 U.S.C. 552
VA Directive 2012-035 on Reduction of the Use and Collection of Social Security Number (SSN)
VHA Directive 1906, Data Quality Requirements for Healthcare Identity Management and Master Veterans Index Functions

Federal Information Processing Standard (FIPS) 199
National Institute of Standards and Technology (NIST) SP 800-60

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 SORNs do not require revision for approval.

D. System Changes

J. *Whether the completion of this PIA will result in circumstances that require changes to business processes*
The PIA will not result in changes to business processes.

K. *Whether the completion of this PIA could potentially result in technology changes*
The PIA will not result in technology changes.

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	☒ Date of Birth	☒ Personal Mailing Address
☒ Social Security Number	☐ Mother's Maiden Name	

☒ 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)

Active Directory Name of System User, Security Identification (SecID) Single Sign-On Identification (SSOi) Enumeration), Progress Notes, Lab Results

PII Mapping of Components (Servers/Database)

REFDOC consists of one 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 REFDOC 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
REFDOC	**Yes**	**Yes**	Name, Integration Control Number, Social Security Number, Date of Birth, Personal Mailing Address.	SQL Tables are populated daily via an ETL process in CDW that collects patient information into the REFDOC SQL instance.	This instance in CDW is safeguarded by CDW's existing security and the application use of the VA 2-factor authentication and PIV. Only

					users onboard via the VA process for PII/PHI safeguards can use REFDOC to access the protected data.

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?

REFDOC capabilities and functionality use data from VistA/VDIF encrypted web services and the Corporate Data Warehouse (CDW) databases through encrypted SQL connections from each system.

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.

REFDOC requires this functionality to pull aggregated information based on an individual health record to produce a Portable Document Format file.

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

The REFDOC system creates a PDF file to bring all information together for the referral but is not the source of the information.

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?

REFDOC information is collected via encrypted SQL connections to databases. VistA/VDIF is an encrypted web service. REFDOC uses a TRM-approved PDF generator utility to create a PDF file. Only the REFDOC user has control of the file after it is created.

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.

REFDOC does not collect information from a form.

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.

REFDOC does not check any data for accuracy. REFDOC retrieves the data stored in the Corporate Data Warehouse or VistA/VDIF web service and relies on controls and processes native to those systems to ensure that the data is accurate.

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.

REFDOC does not check any data for accuracy. REFDOC retrieves the data stored in the Corporate Data Warehouse or VistA/VDIF web service and relies on controls and processes native to those systems to ensure that the data is accurate.

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

79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records - VA (12/23/2020)
172VA10, VHA Corporate Data Warehouse - VA (12/22/2021)
Title 38, United States Code, section 7301(a)
Title 38, United States Code, Sections 501(b) and 304
Title 38, United States Code (U.S.C.), Chapter 1, 3 & 17, Veterans' Benefits
Executive Order 9397, Numbering System for Federal Accounts Relating to the Individual Persons Executive Order 13478, Amendment to Executive order 9397 Relating to Federal Agency Uses of Social Security Numbers (Nov 2008)
Title 38 of U.S.C., Section 1705(c) (1)(2)
Pub. L. 104-262, SEC 104. Management of Health care, SEC 1705. Management of Health care: patient enrollment system. SEC 1706 Management of Healthcare: other requirements (a) (b) (1)
5 U.S.C. 552a, "Privacy Act," c. 1974 o 5 U.S.C. 552, "Freedom of Information Act," c. 1967
HIPAA Privacy Rule, 45 C.F.R. Part 164, Standards for Privacy of Individually Identifiable Health Information
VA Claims Confidentiality Statute 38 U.S.C. 552
Confidentiality of Certain Medical Records, 38 U.S.C. § 7332
Federal Information Security Management Act (FISMA) of 2002
OMB M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002
The Freedom of Information Act, as amended 5 U.S.C. 552
VA Directive 2012-035 on Reduction of the Use and Collection of Social Security Number (SSN) VHA Directive 1906, Data Quality Requirements for Healthcare Identity Management and Master Veterans Index Functions
Federal Information Processing Standard (FIPS) 199
National Institute of Standards and Technology (NIST) SP 800-60

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: Unauthorized access or disclosure of sensitive information is a risk. REFDOC collects a large amount of PII. Due to the sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious personal, professional, or financial harm might result.

Mitigation: Multiple levels of auditing and validating are implemented to ensure that only thoroughly vetted and authorized individuals can access PII, PHI, or SPI.

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.

1. Name: Veteran's identification 2. Date of Birth: Used to verify Veteran identity. 3. Used for initial identification of Veteran and for association of the record when provided to the Third-Party Administrator portal. 4. Personal Mailing Address: Provided in referral package for use by the Community Care provider in correspondence with the Veteran. 5. Personal Phone Number: Provided in referral package for use by the Community Care provider in correspondence with the Veteran. 6. Progress Notes: Notes regarding the Veteran's medical conditions, treatment plans, and other recommendations. Provided in referral package to Community Care provider when needed to support requested medical care. 7. Medications: A list of medications provided by the VA and other medications that were obtained outside the VA. Provided in referral package to inform Community Care provider and support medical treatment decision making. 8. Lab Results: Most recent results for 22 common labs relevant to Community Care medical services and any additional labs that are deemed relevant. Provided in referral package to inform Community Care provider and support medical treatment decision making.

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.

REFDOC does not perform any complex analytical tasks and does not create new information or records, nor does it insert information in any record about any patient. REFDOC only retrieves patient data from existing databases and redisplays that information in a formatted manner. It does not create or populate a local database with any derived or new information. The user determines what information is included in the referral package designed by REFDOC. REFDOC does not retain the referral documentation package, but it is "handed off" to the VA user as a PDF document. The system does not retain any information about the Veteran after this 'hand-off.'

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.

REFDOC only retrieves patient data from existing databases and redisplays that information in a formatted manner. The only other record created by REFDOC is a usage log for each patient search. It identifies the user, the date/time when the patient search was initiated, the time it took for REFDOC to retrieve data, and if the user created a PDF package. The usage data supports application troubleshooting and is displayed within REFDOC in various reports for Community Care to monitor tool usage by VISN, site, and user, including many unique Veterans who had at least one referral documentation package created by REFDOC. The reports involve fundamental analysis, such as aggregating counts at the day/week/month and station levels. It undertakes no regressions, no predictions, no extrapolations, or statistical comparison.

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?

Data at rest using AES-256 and in transit using SSL/TLS 1.2 SHA-256 are protected by encryption certificates that encrypts the data.

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

SSNs are protected by encryption through certificates and encryption when it is stored. Data at rest uses AES-256 and data in transit is using SSL/TLS 1.2 SHA-256.

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

PII/PHI is protected by encryption through certificates and encryption when it is stored. Data at rest uses AES-256 and data in transit is using SSL/TLS 1.2 SHA-256. The certificates used are provided by VA-Internal-s2-ICA4 and uses RSA-256.

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?

The REFDOC information does not commission/modify/decommission or authenticate users independently. Instead, it relies on the Community Care user's standard process for their station to access the downstream applications that REFDOC relies on; PHI/PII (CDW/BISL, VistA/CPRS). Once the user has obtained the necessary access, they can access and utilize REFDOC. Only with the proper authorizations from the downstream applications will Veteran data be made available in the REFDOC process.

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

REFDOC has a user guide that informs users how to obtain access to REFDOC as well as an access control standard operating procedure that documents the controls and responsibilities for access.

2.4c Does access require manager approval?

Access requested through the user's station and PHI/PII (CDW/BISL, VistA/CPRS) does require manager approval.

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

When the REFDOC application is called, users will authenticate using SSOi and a check against CDW/BISL and VistA/CPRS and activity is logged and recorded. VA Clearance procedures are implemented to monitor access, and accounts are disabled after 30 days of inactivity.

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

VHA ensures that the practices stated in the PIA are reinforced by requiring Contractors and VA employees to complete all VA trainings including VA Privacy and Information Security Awareness and Rules of Behavior (VA 10176) and Privacy and HIPAA Training (VA 10203). Contractors and VA employees are required to agree to all rules and regulations outlined in trainings, along with any consequences that may arise if failure to comply. Through TMS employees and contractors are monitored, CORS are responsible for ensuring assignment in TMS training. Training audits occur monthly and are conducted by ISSOs throughout the VA. Training records are stored in the TMS system. Any user who is not current in Privacy/Infosec training loses access to all VA data (including DAPER) until they become current on required training. All incidents are required to be reported to the supervisor or ISSO / Privacy Officer within 1 hour of occurrence. If the ISSO determines a security event has occurred, they open a PSETS ticket and inform CSOC and DBRS. Credit monitoring may be provided to any person whose sensitive information has been violated, and the system user who put the data at risk will be retrained and consequences of actions up to loss of job.

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*

REFDOC retains NO information about the Veteran who is the subject of the PDF it creates. REFDOC collects the following data to populate an electronically generated PDF file for a given Veteran that is used to facilitate an appointment for medical care in the Community Care network.1. Name 2. Date of Birth 3. Social Security Number (SSN) 4. Mailing Address 5. Personal Phone Number 6. Progress Note 7. Medications 8. Lab Results.

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.*

Data retrieved by REFDOC is retained only until the user performs another patient search or exits REFDOC.

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?

REFDOC is not a system of record. Data is compiled from other sources and all VHA records are disposed of following the records retention standards approved by the Archivist of the United Sates, National Archives and Records Administration.

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

REFDOC is not a system of record

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.

Data retrieved by REFDOC is retained only until the user performs another patient search to create another PDF or exits REFDOC. A slightly technical explanation will best illustrate this fact. Like most applications, REFDOC uses the computer's processor, operating in RAM (Random Access Memory), to create the PDF in question. The RAM is the electronic 'workspace' for the application, where the actual work to generate the PDF takes place. When the user launches REFDOC, the processor issues instructions to pull into RAM from CDW and VistA/VIA the data needed to populate the desired PDF. The processor then gives instructions in the RAM 'workspace' to create and populate the selected PDF. Finally, the processor 'delivers' the PDF to the user, who saves it to their local hard disk or a shared drive by separate and independent action. At this point, either the user exits REFDOC or initiates the creation of another PDF with the application. Either way, the RAM is cleared of any data at this time. No retention takes place.

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.

The REFDOC Sustainment team does not test or train with live patient data. The REFDOC team is provided a set of test patients that are created within CDW and VistA. In addition, the only technical team with access to PHI/PII for REFDOC are developers. All other team members within the REFDOC Sustainment team do not have access to PHI/PII data. For support purposes, developers may see live patient data as part of their troubleshooting process with Community Care users. In those instances, they adhere to and follow the below training and directives: Completion of VA Privacy and Information Security Awareness training and Rules of Behavior annually via the VA Talent Management System, VA Directive 6510, VA Identity and Access Management, VA Handbook 6500.6

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

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

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that the information maintained by REFDOC 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.

Mitigation: REFDOC does not retain data after a PDF is created. To mitigate any issue, REFDOC users will adhere to VA Handbook 6500.2 Management of Data Breaches Involving Sensitive Personal Information (SPI) contains the policies and responsibilities that VA components must follow to manage data breaches, including detection, correlation, notification, remediation, and reporting.

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***
Veterans Health Administration Corporate Data Warehouse (CDW)	REFDOC collects data from CDW databases to populate an electronically generated PDF file that is used to facilitate an appointment for medical care in the Community Care network of external providers	Name, Social Security Number (SSN), Date of Birth (DOB), Mailing Address, Personal Phone Number(s), Lab Results, Progress Notes, Current Medications	HTTPS Data in transit is encrypted using FIPS-140-2 encryption (SSL encryption, Port 1433) to transmit data securely
Veterans Health Administration VistA	REFDOC collects data in the form of Radiological Images from VistA/VDIF to populate an electronically generated PDF file that is used to facilitate an appointment for medical care in the Community Care network of external providers.	Name, Date of Birth (DOB), Social Security Number (SSN), Mailing Address, Personal Phone Number(s), Lab Result, Progress Notes, Current Medications	VistA through VDIF Data in transit is encrypted using FIPS-140-2 encryption (SSL encryption, Port 443) to transmit data securely
Veterans Health Administration Identity and Access Management (IAM)	The VHA IAM service SSOi is used to provide internal single sign on and identify and access management within	Active Directory Name of System User, Security Identification (SecID) Single Sign-On Identification (SSOi) Enumeration	HTTPS Data in transit is encrypted using FIPS-140-2 encryption (SSL encryption, Port

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*
SSOi	the VA network, for VA Employees.		443) to transmit data securely
Veterans Health Administration Identity and Access Management (IAM) SSOi - provisioning	The VHA IAM service SSOi is used to provide internal single sign on and identify and access management within the VA network, for VA Employees.	Security Identification (SecID) Single Sign-On Identification (SSOi) Enumeration	HTTPS Data in transit is encrypted using FIPS-140-2 encryption (SSL encryption, Port 443) to transmit data securely

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: The privacy risk associated with maintaining PII is that sharing data within the Department of Veterans Affairs could happen. The data may be disclosed to individuals who do not require access, which heightens the threat of the information being misused.

Mitigation: The principle of need-to-know is strictly adhered to by the REFDOC personnel. Only personnel with a clear business purpose are allowed access to the system and the 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

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***
N/A	N/A	N/A	N/A	N/A

5.2 <u>PRIVACY IMPACT ASSESSMENT: External sharing and disclosure</u>

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: The REFDOC Information system does not share data externally, therefore, there is not privacy risk from the information system.

Mitigation: Continue to not share data externally from the information system.
.

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 REFDOC data is retrieved from other VA systems. No new data is collected from individuals.

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

REFDOC pulls information from other information systems within the VA and does not collect new data. Notice of collecting information is the responsibility of the information systems in which the information is pulled from.

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.

REFDOC pulls information from other information systems within the VA and does not collect new data. Notice of collecting information is the responsibility of the information systems in which the information is pulled from.

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.

REFDOC pulls information from other information systems within the VA and does not collect new data. Notice of revocation availability of information is the responsibility of the information systems in which the information is pulled from.

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

REFDOC pulls information from other information systems within the VA and does not collect new data. Notice of right to consent to particular use of information is the responsibility of the information systems in which the information is pulled from.

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.

REFDOC pulls information from other information systems within the VA and does not collect new data from individuals, therefore, this question is not applicable.

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:

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 members of the public may not know that the REFDOC system exists within the Department of Veterans Affairs.

Mitigation: The VA mitigates this risk by providing the public with two forms of notice that the system exists, as discussed in detail in question 6.1, including the Privacy Impact Assessment and the System of Record Notice.

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.***

Data is not retained within REFDOC nor is it a system of record.

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).

Data is not retained within REFDOC nor is it a system of record.

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.

Data is not retained within REFDOC nor is it a system of record.

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

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

Data is not retained within REFDOC nor is it a system of record.

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.

Data is not retained within REFDOC nor is it a system of record.

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

Data is not retained within REFDOC nor is it a system of record.

7.5 <u>PRIVACY IMPACT ASSESSMENT: Access, redress, and correction</u>

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that erroneous information is placed into REFDOC via the feed from Community Care.

Mitigation: The information in REFDOC is obtained via Community Care. If there is erroneous or inaccurate information, it should be addressed with the Non-VA Care Coordination (NVCC) staff. Any validation performed would merely be the Veteran personally reviewing the data before providing it. Individuals can provide updated information for their records by submitting new forms or correspondence and indicating to the VA that the further information supersedes the previous data.

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.

REFDOC does not provision users. REFDOC checks to ensure the user has access to VistA/CPRS and CDW/BISL and if both are true the user is granted permission to REFDOC.

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?

VA staff who have taken the required training and agreed to rule of behavior will have view only access on a need-to-know basis.

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.

All users must be VA cleared.

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.

A.). The VA Handbook 6500.6 establishes in detail the procedures, roles and responsibilities, and contract language that governs contractor access to VA systems. These guidelines are followed in granting REFDOC access to any contractor. Applicable procedures from VA Handbook 6500.6 on contractor security requirements: Information generated by a contractor or subcontractor as part of the contractor/subcontractor's normal business operations, such as health record information created in the course of providing treatment or health care services to VA's Veterans is subject to review to determine if the information is owned by VA and subject to VA security policy. VA sensitive information that has been properly disclosed by VA to the contractor is not subject to the VAAR security clause. If the information is not owned by VA, the requirements outlined in this Handbook do not apply and the VAAR security clause should not be added to the contract. The CO, the PO, and if required, Regional Counsel can be consulted. VA OIG counsel will conduct the review for the OIG generated contracts. B.) VA requires that facilities and program offices ensure that contractors, subcontractors, and third-party servicers or associates, or on behalf of any of these entities, regardless of format or whether the VA information resides on a VA system or contractor/subcontractor's electronic information system(s) operating for or on VA's behalf, employ adequate security controls as appropriate in accordance with VA directives and handbooks, regulations, guidance, and established service level agreements. C.). Information security requirements must be considered in all phases or stages of VA's procurement process. The applicable Program Manager, Information System Owner, and Information Owner are responsible for ensuring that the solicitation document includes the appropriate information security and privacy requirements. The information security requirements must be sufficiently detailed to enable service providers to understand what is required. A general statement that the service provider must agree to comply with applicable requirements is not acceptable. See Appendix C for a catalog of security and privacy language statements that have been developed, reviewed, and approved and can be used in contracts, as appropriate. This language summarizes for the contractors the most important Federal and VA policy issues that need to be addressed, as appropriate, in contracts to ensure adequate security and privacy controls are included in the contract vehicle. Additional security or privacy language can be added, as required. Program managers, project designers, and acquisition professionals must take security requirements, measures, and controls into account when designing and making agency acquisitions; appropriate security controls drive requirements, specifications, deliverables, and costs. Acquisition staffs need to consult information security officials to determine what level of security and which security controls may be required in this process. VA Handbook 6500, Information Security Program, provides the

security requirements and policy for VA.D.) The applicable VA Program Manager, Information System Owner, Information Owner, the CO, PO, ISO, and the Contracting Officer's Technical Representative (COTR) are responsible for ensuring that VA information system security and privacy requirements, as appropriate, are implemented and complied with per the requirements detailed in the contract. Compliance and Records Management Officers should also be contacted, as appropriate, to ensure the requirements and language they require are included in the contract. E.) VA requires that all facilities and program offices monitor information security control compliance of their respective contracts and acquisitions by doing the following: (1) Adhere to the security and privacy contract language as outlined in the contracts.(2) Ensure that COs work with their COTR, ISO, and PO and other applicable staff to complete Appendix A for all service acquisitions and contracts. This appendix assists in determining the security requirements for VA acquisitions and contracts during the planning phase of the acquisition process. The checklist must be included as part of the overall contract file by the CO for new service acquisitions and contracts and a copy must be maintained in the applicable contracts file and accessible to the COTR, ISO, and PO. (3) Ensure that contracting officials include VA's approved security clause, Appendix B, into any applicable contracts, if required as indicated by completing Appendix A. NOTE: The security clause in Appendix B is currently undergoing official VA rulemaking by the Office of Acquisitions and Logistics (OA&L). The final version of the clause may be revised after it is presented to the public for review via the Federal Register. (4) Ensure that contractors, third party partners, and servicers implement the VA security and privacy requirements, as defined in the contract. These requirements can also be added to the contract Statement of Work (SOW). The requirements apply to applicable contracts in which VA sensitive information is stored, generated, transmitted, or exchanged by VA, a contractor, subcontractor or a third-party, or on behalf of any of these entities regardless of format or whether it resides on a VA system or contractor or subcontractor's electronic information system(s) operating for or on the VA's behalf. (5) Ensure that contractor systems that have negotiated with VA to store, generate, transmit, or exchange VA sensitive information in a contractor developed and maintained system are certified and accredited (authorized), and registered and monitored in VA's Security Management and Reporting Tool (SMART) database that monitors FISMA compliance. The Program Manager and/or the ISO are responsible for contacting the Information Protection and Risk Management's (IPRM) Certification Program Office (CPO) within OI&T to register the system or to answer questions regarding the authorization of systems(6) Ensure that Certification and Accreditation (Authorization) (C&A), is accomplished in compliance with VA policy (per the results of the completed checklist provided in Appendix A) and VA Handbook 6500.3, Certification and Accreditation of VA Information Systems. The OI&T CPO within the Office of Cyber Security (OCS) must be contacted regarding procedures for C&A (Authorization) of contractor managed systems. (7) Ensure that the Program Manager, the COTR and the CO, with the assistance of the ISO, monitor compliance with the contract or agreement security requirements throughout the life of the contract. For IT systems, this includes ensuring that annual self-assessments are conducted by the contractor with appropriate Plan of Actions and Milestones (POA&M) initiated and completed. (8) Ensure that service providers and contractors who have negotiated agreements with VA that involve VA sensitive information, but do not maintain systems that require C&A, complete a Contractor Security Control Assessment (CSCA) within 30 days of contract approval and annually on the due date of the contract renewal. The ISO/COTR or CO can also request that a CSCA be completed by the contractor anytime there are potential security issues identified or suspected by VA or to ensure that applicable security controls are being implemented. The completion of the CSCA by the contractor is the responsibility of the COTR. The CSCA template is maintained on the IPRM portal under the C&A Section. The COTR can contact the ISO to obtain a copy of the CSCA from the portal or to seek assistance in the completion of the assessment. The completed CSCA must be

provided and reviewed by the ISO and by the CPO to ensure that adequate security is being addressed by contractors in situations where the C&A of a system is not applicable. A copy of the CSCA is uploaded by the ISO and maintained in the document section of the SMART database. (9) Ensure that contractors and third-party servicers accessing VA information sign the Contractor Rules of Behavior, Appendix D. The VA National Rules of Behavior do not need to be signed if the VA Contractor Rules of Behavior" are signed. (10) Ensure that contractors and third-party service positions receive the proper risk level designation based upon the review of the Position Designation System and Automated Tool (PDAT) established by the Operations, Security, and Preparedness Office (007). Background investigations of all contractors must adhere to the results of the PDAT per VA Directive and Handbook 0710, Personnel Suitability and Security Program.(11) Ensure that contractors take the required security and privacy training as outlined in Appendix C. (12) Ensure that all IT procurements, including contracts, are submitted through the IT Acquisition Request System (ITARS), VA's acquisition approval system for review and approval as required by the VA CIO. (13) Ensure that language is included in appropriate contracts to ensure new acquisitions include Federal Desktop Core Configuration (FDCC) settings and products of information technology providers operate effectively using them. Link to VA Handbook 6500.6: Contractors must take approved VA security training and sign the VA Rules of Behavior document Located in VA Handbook 6500.6 Appendix C

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.

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 via the VA Talent Management System.

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:* 23-Jun-2023
3. *The Authorization Status:* 1-year ATO
4. *The Authorization Date:* 10-Mar-2023
5. *The Authorization Termination Date:* 09-Mar-2024
6. *The Risk Review Completion Date:* 02-Mar-2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* High

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.***

Not Applicable

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)*

The REFDOC web-based application system is hosted by the VA Enterprise Cloud (VAEC) and is identified as an IaaS.

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.*

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.

NA

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.

NA

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).

NA

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.

MICHAEL HARTMANN

Digitally signed by MICHAEL HARTMANN
Date: 2023.09.01 06:55:00 -06'00'

Privacy Officer, Michael Hartmann

KIMBERLY KEENE

Digitally signed by KIMBERLY KEENE
Date: 2023.09.12 08:00:47 -04'00'

Information System Security Officer, Kimberly Keene

Tony L. Sines 167047

Digitally signed by Tony L. Sines 167047
Date: 2023.09.08 12:48:55 -05'00'

Information System Owner, Tony Sines

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).

- Department of Veterans Affairs Veterans Health Administration NOTICE OF PRIVACY PRACTICES
- 79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records – VA (12/23/2020)
- 172VA10, VHA Corporate Data Warehouse – VA (12/22/2021).

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