Privacy Impact Assessment for the VA IT System called:

OA and L Remote Order Entry System (ROES) Assessing

VA Central Office

VA National Acquisition Center

Date PIA submitted for review:

July 14, 2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Shevonna Planer	Shevonna.Planer@va.gov	708-786-7804
Information System Security Officer (ISSO)	D. Scott Lewis	scott.lewis1@va.gov	708-786-5144
Information System Owner	Kevin Quitmeyer	kevin.quitmeyer@va.gov	303-273-6251

Abstract

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

OA and L Remote Order Entry System (ROES) is used for ordering health care products and services through the Denver Logistics Center (DLC). ROES is used by designated clinical services at all medical centers and outpatient clinics, including Audiology and Speech Pathology Service, Prosthetics & Sensory Aids Service, and Home Telehealth Service. Items commonly ordered through ROES include hearing aids; hearing aid accessories and batteries; prosthetic items; assistive devices; Home Telehealth messaging devices and related peripherals; and services associated with all these items. ROES allows authorized medical facility users to enter requests and perform other actions in managing patient care consistent with their clinical practices. When an order is placed, patient-specific demographic and eligibility information from the patient database on the originating VA medical center VistA system is collected and incorporated into records within the ROES system.

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.
Remote Order Entry System (ROES); VA National Acquisition Center

B. The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.
Support VHA Supply activities for patient care purposes.

C. Indicate the ownership or control of the IT system or project.
Denver Logistics Center

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.
Two million individuals; and Veterans and Dependents

E. A general description of the information in the IT system and the purpose for collecting this information.
Patient full name, Social Security Number, date of birth, Department of Defense (DoD) status (active duty/retired), and address (optional).

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

Veteran's Health Administration(VHA) Prosthetic and Sensory Aids Program (113), VA Decision Support System, VA Enrollee Healthcare Projection Model and VA Financial Services Center(FSC) Electronic Data Interchange(EDI) System.

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.

VHA Electronic Health Record EHR system: same controls are used. Both locations use the same source data within the DLC system Denver Logistics Center in Golden, Colorado.

3. Legal Authority and SORN

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

SORN Veterans health Information Systems and Technology Architecture (VISTA) records-VA (79VA10). Also, collection and use are authorized under the Veterans Benefit Act, Title 38, USC Section 7301(a). In addition, VA has been delegated the authority to manage Federal Supply Service (FSS) Schedule 65 contracts and contracts for the portion of Schedule 65 that pertains to medical equipment by the General Services Administration. Within the VA Acquisition and Logistics program, the DLC has authority to establish contracts and manage associated records for designated VHA clinical programs. Products and services are provided based on entitlements set forth in VHA Handbook 117

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?

N/A. The system does not currently use cloud technology

D. System Changes

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

No

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

No

Section 1. Characterization of the Information

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

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

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

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

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

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

- ☒ Name
- ☒ Social Security Number
- ☒ Date of Birth
- ☐ Mother's Maiden Name
- ☒ Personal Mailing Address
- ☐ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☐ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☐ Financial Information
- ☐ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers*
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☐ Medications
- ☐ Medical Records
- ☐ Race/Ethnicity
- ☐ Tax Identification Number

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

Department of Defense (DoD) Status (Active Duty/Retired)

PII Mapping of Components (Servers/Database)

Remote Order Entry System consists of 4 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 **Remote Order Entry System** 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
Veterans Health Administration (VHA) Prosthetic and Sensory Aids Program (113) (VistA Prosthetics Package)	Yes	Yes	Name (last, first), SSN of patients for whom products have been ordered.	Prosthetics to maintain records of prosthetic appliances issued to Veteran.	PIV-only access, required Annual Privacy/Rules of Behavior Training
VA Decision Support System (DSS)	Yes	Yes	SSNs of Veterans receiving care from the clinical programs	For use in VHA management decision making for future health care needs	PIV-only access, required Annual Privacy/Rules of Behavior Training

			served by ROES.		
VA Enrollee Healthcare Projection Model (VSSC)	Yes	Yes	SSNs of Veterans receiving care from the clinical programs served by ROES.	For use in VHA management decision making for future health care needs	PIV-only access, required Annual Privacy/Rules of Behavior Training
VA Financial Services Center (FSC) Electronic Data Interchange (EDI) System	Yes	Yes	Last name, SSN (Last 4 only)	To exchange purchase transactions with vendors.	Contract restrictions, Business Associate Agreements in place.

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?

Information used by the Remote Order Entry System comes from 2 resources: the individual requiring a medical device and the respective EHR system in use at a particular VHA facility (VistA/Computerized Patient Record System (CPRS) or Cerner Millennium electronic health record system). Information provided directly by the individual include: Personal email address, personal mailing address updates, if the patient chooses to provide it. Information imported from VistA/CPRS include: Patient name, Social Security Number, date of birth, and eligibility.

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.

n/a

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?

Electronically collected using VistA/CPRS electronic health records or Cerner Millennium electronic health record system application program interfaces. If the Veteran initiates contact with the Denver Logistics Center, they may provide updated information via telephone, email, or pre-printed battery and accessory cards when checking the status of an order.

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.

An application user feedback is solicited during the order process to verify that information in the record is correct. Individuals can check the accuracy of the record when placing an order online via va.gov, via telephone, via email or pre-printed mail-in card. It will be checked periodically, as patients check or are asked.

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

SORN Veterans Health Information Systems and Technology Architecture (VistA) records-VA(79VA10)

Collection and use are authorized under the Veterans Benefit Act, Title 38, USC Section 7301(a). In addition, VA has been delegated the authority to manage Federal Supply Service (FSS) Schedule 65 contracts and contracts for the portion of Schedule 65 that pertains to medical equipment by the General Services Administration. Within the VA Acquisition and Logistics program, the DLC has authority to establish contracts and manage associated records for designated VHA clinical programs. Products and services are provided based on entitlements set forth in VHA Handbook 117.

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

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

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

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

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

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

<u>Principle of Data Quality and Integrity:</u> 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: The Remote Ordering Entry System (ROES) contains personal identifying information (PII) on Veterans and their dependents. There is a risk that if this information were breached or otherwise accessed without authorization, delivery of care to the individuals could be interrupted.
Mitigation: Management, operational and technical security controls are employed. All personnel must use, disclose, or request PII to the minimum amount necessary required to perform their specific job functions and to accomplish the intended purposes of the use, disclosure, or request. Personnel must only access the PII needed to perform their official duties.

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.

DoD status (active duty/retired)

Name – Used to address and identify the Veteran or dependent receiving medical equipment.
Personal Mailing Address – Used to deliver products to Veteran or dependent.
Date of Birth – Used to identify the Veteran or dependent receiving medical equipment.
Phone Number – Used for customer service
purposes.
Social Security Number – Used to identify the Veteran or dependent receiving medical equipment.

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

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

The transactional procurement records can be rolled up into sales reports on a medical center, VISN or national basis.
This is not reported on an individual basis.
ROES can provide a number of ad hoc reports as follows:
Sales summary by VISN/Facility
Prosthetics and Sensory Aids Service (PSAS) sales summary by VISN/Facility/BOC
Commodity sales by Facility/Service
Order detail by Commodity/Facility
Sales summary by Commodity/Eligibility
Sales summary by Facility/Obligation
VA Decision Support System (DSS) uses information to determine capitation levels for patients who are treated in the audiology, telehealth, and prosthetics programs. Reports are provided monthly.
VA Enrollee Healthcare Projection Model uses information to project and anticipate patient workloads into the future for the VHA healthcare system. Reports are provided semiannually.

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.

New records of transactions are recorded and will be placed in the individual's existing record. A transactional record of the prescribed item will be placed in the individual's record. The newly-created information will be accessible to Government employees (with a need to know, in performance of their official duties) who make determinations about their health care delivery and provide ancillary services.

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?

Physical security of storage media, encryption, secure transmission protocols

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

Pattern recognition to block Social Security Numbers from being sent via unencrypted means.

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

No additional measures are necessary to meet the requirements of OMB M-06-15

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?

Need to know; in performance of official duties

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

Yes

2.4c Does access require manager approval?

Yes. Local ROES Site Supervisor

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

The Sensitive Patient indicator used in ROES is the same in VistA. When a staff member accesses a record marked "sensitive," ROES checks the indicator and presents the same user notification and the logging of access when the record is viewed.

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

All VA employees are required to complete annual training in order to maintain access to the Remote Order Entry System. These trainings are the VA Privacy and Information Security Awareness

training, which includes agreeing to the VA Rules of Behavior and the annual Privacy and HIPAA training.

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*

Name, Social Security Number, personal mailing address, order history, eligibility, and order-specific medical information.

3.2 How long is information retained?

*In some cases VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. **For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods**. The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented. If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

Information in the Remote Order Entry System (ROES) is kept in accordance with VHA Records Control Schedule (RCS) 10-1 Destroy 6 years, 3 months after the creation date of the purchase order or 6 years, 3 months after the last entry in file.

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

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

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

Yes, the Remote Order Entry System (ROES) operates under the Department of Veterans Affairs, Veterans Health Administration (VHA), Record Control Schedule (RCS) 10-1 (March 2017).

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

the Remote Order Entry System (ROES) operates under the Department of Veterans Affairs, Veterans Health Administration (VHA), Record Control Schedule (RCS) 10-1 (March 2017).
http://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.

Electronic records are destroyed in accordance with VHA Records Control Schedule (RCS) 10-1 and VA's media sanitization program, VA Handbook 6500.1.
http://www.va.gov/vhapublications/rcs10/rcs10-1.pdf
https://www.va.gov/vhapublications/publications.cfm?pub=8

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.

When there is a need for records containing PII to be used for testing, such as when introducing new applications or application functionality, the application or enhancement is first assessed for its usage of PII. If usage involves output or transmission of PII as part of the testing, then

additional controls measures are implemented to ensure test recipients are limited to as few as reasonable, and that they are informed, prior to testing, of their obligation to protect the privacy and security of test information. Testing is closely monitored to ensure usage of PII is limited to only that necessary to perform the test procedure.
PII is used for training purposes only when completion of the training without exposing PII is not possible. When PII is exposed in the course of delivery of training, participants are reminded of their obligation to protect the information. If participants are not able to comply with VA Rules of Behavior regarding PII and protected information, they are excused from the training while PII is used.
Research studies or requests which require usage of PII within the system are first subject to approval by senior officials and/or VHA Patient Care Services (PCS), whichever is applicable based on the data content requested by the study. No research data is provided without the necessary Independent Review Board (IRB) and PCS approvals.

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: The longer information is retained, the greater the risk that the information could be compromised or otherwise breached.

Mitigation: The Remote Order Entry System retains only the information necessary to ensure continuity of care and provide veterans and their dependents with the necessary service to maintain their medical equipment. Additionally, ROES carefully follows the retention time frames laid out in VA Veterans Health Administration RCS 10-1 and destroys the files following the procedures discussed question 3.4 when the retention period has expired.

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 (VHA) Prosthetic and Sensory Aids Program (113)	Patient care delivery	Name (last, first), SSN of patients for whom products have been ordered.	Electronically
VA Decision Support System	The information is shared for purposes of aggregate data	SSNs of Veterans receiving care from the clinical programs served by ROES.	Electronically

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*
	analysis and management decision support.		
VA Enrollee Healthcare Projection Model	The information is shared for purposes of data analysis and projections affecting VA resource allocation in upcoming years.	SSNs of Veterans receiving care from the clinical programs served by ROES.	Electronically
VA Financial Services Center (FSC) Electronic Data Interchange (EDI) System	The information is shared for translation to American National Standards Institute (ANSI) standard EDI transaction sets.	Last Name, SSN (Last 4 only).	Electronically

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: There is a risk that the data may be shared with an unauthorized VA program or IT system or exposed to programs or individuals without a valid need to know.

Mitigation: Everyone who accesses the information is subject to VA Privacy and Information Security policies. Only the information necessary for the program to perform its function is shared.

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***

Department of Defense (DoD) clinical healthcare providers	Information is received from DoD providers as they request patient care products that are available through ROES and VA/DLC contracts. Providers enter information in the application and select products needed for the active duty patients and some dependents. VA sensitive information is not shared with DoD.	Information received consists of patient name, Social Security Number, date of birth, DoD status (active duty/retired), and address (optional). In the application, DLC contract product descriptions, pricing, etc., are available for selection and order entry. VA sensitive information is not shared/transmitted to DoD.	Executive Order 9397, 32 CFR 505.4(a)(b); VA national contracts for healthcare items; VA InterAgency Acquistions Guidance and Procedures Memorandum 2013-06 Direct Acquisition (6.1) allows DoD to purchase from VA contracts; DoD Memorandum	The VA grants authorized DoD clinical providers remote access directly to the ROES system so that they may enter/view records in ROES. An account is created for DoD users in addition to their Identity and Access Management (IAM) registration. Those granted DoD access to ROES must submit a security agreement and training is made available to them. VA Training reciprocity

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum Of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.
Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.
This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

Privacy Risk: There is a risk that information shared outside the Department for authorized purposes may be exposed by that entity.

Mitigation: Contracts with commercial suppliers of healthcare products include provisions to ensure the suppliers comply with VA privacy and security policies and Rules of Behavior. Suppliers are explicitly instructed as to their usage of the information solely for the purpose of fulfilling their contract to the Department for provision of healthcare products and services.

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.

Yes, ROES does not collect anything outside what's covered by VHA Notice of Privacy Practices (NOPP). As stated in the NOPP, "We may use and disclose your health information for treatment or to provide health care services. Treatment may include: prescriptions for medications, supplies and equipment; and electronic information exchange. The NOPP is available on VA's Web site at https://www.va.gov/vhapublications/publications.cfm?pub=8

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

N/A

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

https://www.va.gov/vhapublications/publications.cfm?pub=8

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.

Yes, individuals have the right to decline to provide information to the ROES system without penalty or denial of service.

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.

Yes, the process is outlined in the VHA Notice of Privacy Practices (NOPP). We may use or disclose your health information for any purpose based on a signed, written authorization you provide us. If we were to use or disclose your health information for marketing purposes we would require your signed written authorization. In all other cases, we will not use or make a disclosure of your health information without your signed, written authorization, unless the use or disclosure falls under one of the exceptions described in the NOPP. When we receive your signed written authorization we will review the authorization to determine if it is valid, and then disclose your health information as requested by you in the authorization.

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

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

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

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

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

Privacy Risk: There is a risk that a Veteran or other member of the public may not know that the Remote Order Entry System (ROES) exists or that it contains records about them.

Mitigation: ROES mitigates this risk by providing the individuals direct notice of the system and its information collection practices via the means mentioned in question 6.1.

Section 7. Access, Redress, and Correction

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

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

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

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

Staff has been provided training that queries are to be directed to the Government Information Specialist, 708-786-5146 or to NACFOIA@va.gov. Individuals may make written requests for their information. For matters of customer service, the individuals would speak to Customer Service representatives. Please send a written request, to your VHA health care facility Privacy Officer. The Privacy Office at the DLC does not maintain VHA health records, nor past military service health records. For a copy of your military service health records, please contact the National Personnel Records Center at (314) 801-0800. The Web site is http://www.archives.gov/veterans/military-service-records/medical-records.html.

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

N/A

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

ROES is contained in a Privacy Act System of Records.

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

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

Individuals are given a point of contact in Customer Service to update information. Customer service representatives also verify all information is up-to-date when making corrections. Customer Service may be reached via e-mail to dalc.css@va.gov or by calling (303) 215-5245. Customer Service Representatives are available Monday through Friday from 6:30 a.m. to 4 p.m. MT. Individuals may also use information listed in Section 7.1.

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.

Information about the processes for accessing and correcting personal information in the Remote Order Access System (ROES) is provided in the Veteran's Health Administration (VHA) Notice of Privacy Practices (NOPP). Individuals have the right to review and obtain a copy of your health information in our records. You must submit a written request to the facility Privacy Officer at the VHA health care facility that provided or paid for your care.
NOTE: Please send a written request, to your VHA health care facility Privacy Officer. The Denver Logistics Center does not maintain VHA health records, nor past military service health records. For a copy of your military service health records, please contact the National Personnel Records Center at (314)801-0800. The Web site is http://www.archives.gov/veterans/military-service-records/medical-records.html

.

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

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

The methods and procedures discussed in questions 7.1 and 7.2 are the only methods available for accessing and requesting edits to one's personal data in the Remote Order Entry System (ROES). Alternative methods are not available.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that the ROES system contains and uses inaccurate data, which could cause a variety of problems including, but not limited to medical devices not being delivered correctly (because contact information is incorrect) or denial of requests for devices (because eligibility data is incorrect).

Mitigation: By providing processes and procedures that allow individuals to access, review, and request changes to their personal information, the ROES system provides a means to verify and ensure the accuracy of patient data in the system.

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.

Office of Inspector General auditors were given "read only" access, on an as-needed basis. Clinicians are given full access. Patients do not have access to the system, but are able to request authorized re-supply items through va.gov request method. DoD – clinical provider, based on role in that Agency's health care system. A user self-service registration is used for account set up, which also includes acknowledgement of the DLC Security Agreement for gaining access to the system. Access is granted by the System Owner. The security agreement outlines training requirements, access level, and user permissions.

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?

DoD – clinical provider, based on role in that Agency's health care system. A user self-service registration is used for account set up, which also includes acknowledgement of the DLC Security Agreement for gaining access to the system. Access is granted by the System Owner. The security agreement outlines training requirements, access level, and user permissions

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.

Office of Inspector General auditors were given "read only" access, on an as-needed basis. Clinicians are given full access.

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.

Contractors who work within the DLC Distribution Management Division have access to data contained within the Remote Order Entry System (ROES). They have no involvement with the design and maintenance of the system. Vendors do not have access to ROES. Contracts are reviewed every six months by the Contract Officer Representative (COR) and the DLC subject matter experts.

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 individuals given access to ROES must complete the VA Privacy and Information Security Awareness training and agree to the VA Rules of Behavior. Department of Defense employees who have access to the system must take the DoD equivalent of this training before gaining access.

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:* 09/28/2022
3. *The Authorization Status:* Authority to Operate (ATO)
4. *The Authorization Date:* 12/02/2022
5. *The Authorization Termination Date:* 12/02/2023
6. *The Risk Review Completion Date:* 11/28/2022
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.***

N/A

Section 9 – Technology Usage

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

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

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

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

No

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.*

N/A

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

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

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

N/A

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

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

N/A

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

Robotic Process Automation is the use of software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. For example, will the

automation move or touch PII/PHI information. RPA may also be referred to as "Bots" or Artificial Intelligence (AI).

N/A

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

ID	Privacy Controls
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.

SHEVONNA PLANER

Digitally signed by SHEVONNA PLANER
Date: 2023.07.19 11:32:00 -05'00'

Privacy Officer, Shevonna Planer

Digitally signed by DUANE LEWIS
Date: 2023.08.03 12:46:53 -05'00'

Information System Security Officer, Scott Lewis

KEVIN L. QUITMEYER 248322

Digitally signed by KEVIN L. QUITMEYER 248322
Date: 2023.08.03 11:38:35 -06'00'

Information System Owner, Kevin Quitmeyer

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).

https://www.va.gov/vhapublications/publications.cfm?pub=8

.

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