Privacy Impact Assessment for the VA IT System called:

# Collaborative Health Outcomes Information Registry (CHOIR)

## Veterans Health Administration

## Pain Management, Opioid Safety, Prescription Drug Monitoring Program (PMOP)

## eMASS ID #2521

Date PIA submitted for review:

12/05/2024

System Contacts:

*System Contacts*

| | Name | E-mail | Phone Number |
|---|---|---|---|
| Privacy Officer | Nancy Katz-Johnson | Nancy.Katz-Johnson@va.gov | 203-535-7280 |
| Information System Security Officer (ISSO) | Craig Heitz | Craig.Heitz@va.gov | 612-267-2301 |
| Information System Owner | Mark Mehelis | Mark.Mehelis@va.gov | 925-794-9117 |

## Abstract

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

Collaborative Health Outcomes Information Registry provides a mechanism for patients to complete a self-assessment regarding their current medical condition. A report is generated that will become part of their patient record. The system engine uses the data provided by the patient to generate information that is used by the provider to determine a diagnosis and/or therapies.

## Overview

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

*1 General Description*

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

The Collaborative Health Outcomes Information Registry is an implementation of the National Institute of Health common fund program Patient Reported Outcomes Management Information System (PROMIS). The Pain Management, Opioid Safety, and Prescription Drug Monitoring Program working group under the direction of the Executive Director for Pain Management is leading this effort to implement the tools within its pain clinics. The system is used to collect Patient Reported Outcomes using a scientifically validated computer adaptive testing engine which allows the system to collect high-fidelity information about the patient without requiring them to complete entire scientifically validated instruments. The outputs are used by providers to assist in their diagnosis, therapies, and documentation of patients and their diagnosis. The system is hosted in a single location using a single data structure with logical means of implementing HIPPA controls. When fully implemented, it will contain information regarding any pain clinic patients in the VA system (approximately 10,000).

*B. Who is the owner or has control of the IT system or project? If the system has an eMASS entry, ensure this information matches with the eMASS entry.*

This is a VA Owned and VA Operated system. The Pain Management, Opioid Safety, Prescription Drug Monitoring (PMOP) is the owner of the system through its Program Management Office – Veteran Integrated Pain Record (VIPR). The system registry in eMASS is #2521

*2. Information Collection and Sharing*

*C. Indicate the expected number of individuals whose information is stored in the system and include a brief description of the typical client or affected individual?*

We expect to have the information of 10,000 individuals stored in this system. The typical client will be a Veteran or dependent who is referred to the Pain clinics. The secondary record will be the clinical staff who provide the services to the Veterans.

| Check if Applicable | Demographic of Individuals |
|---|---|
| ☒ | Veterans or Dependents |
| ☒ | VA Employees |
| ☒ | Clinical Trainees |
| ☒ | VA Contractors |
| ☐ | Members of the Public/Individuals |
| ☐ | Volunteers |

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

The system will collect contact, identity verification, login, and personal health information of the patient in response to prompts from the system and staff login and contact information. The purpose of this is to then calculate the probability of a particular diagnosis, identify potential therapies, and assist the provider in documenting the encounter with the patient.

*E. What information sharing is conducted by the IT system? A general description of the modules and components, where relevant, and their functions.*

The system manually transfers information with Veterans Health Information Systems and Technology Architecture (VISTA) by manually transferring the History of Present Illness (HPI) note and system generated report by CHOIR to the patients record for use by the provider at time of the appointment. At a future date the system will use Office of Information Technology interfaces to electronically send these items into VISTA (or its successor). Additionally, the system will obtain appointment information and veteran profile from VISTA (Office of Information Technology (OIT) Services ) for patients and providers which will be used to automate certain data collection needs for the providers.

*F. Are the modules/subsystems only applicable if information is shared?*

No

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

The system is hosted at a single data center instance within the VA. All sites using the system use the single instance and as such, the PII is maintained in the same manner for all sites.

*3. Legal Authority and System of Record Notices (SORN)*

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

Title 38, United States Code, Sections 501(b) and 304
24VA10A7 / 85 FR 62406, *Patient Medical Records – VA*
https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pd

*H. What is the SORN?*

24VA10A7 / 85 FR 62406, *Patient Medical Records – VA*
https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pd

*I. SORN revisions/modification*

None

*I. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval.*

No

*4. System Changes*

J. *Will the business processes change due to the information collection and sharing?*

☒ Yes
☐ No
if yes,
The system will allow clinics to obtain information from patients with the least amount of intrusion into the clinics work and allow the veteran to provide high-fidelity information about their current situation and outcomes through the use of an electronic data collection system. Existing processes require the patient to complete these assessments on paper or in a static electronic form.

K. *Will the technology changes impact information collection and sharing?*

☒ Yes
☐ No
if yes,
The system will simplify the process for VA clinicians to obtain full featured measures of patients while impacting the patient as little as possible. The system takes both the submitted

information from the patient and other data (appointment and veteran profile) to generate a standardized History of Present Illness (HPI) note that can either be manually entered into VISTA or electronically via an OIT generated service. Finally, the tool creates a report intended for the provider to provide them with a longitudinal view of the patient and visually represent trends in the patients reported outcomes.

## 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 Information 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. It must also match the information provided in question 3.4 of the PTA.*

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
- ☐ **Full** Social Security Number
- ☐ **Partial** Social Security Number
- ☒ Date of Birth
- ☐ Mother's Maiden Name
- ☐ Personal Mailing Address
- ☒ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☒ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a Different Individual)
- ☐ Financial Information
- ☐ Health Insurance Beneficiary Numbers Account Numbers
- ☐ Certificate/License Numbers[1]
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP)

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

Address Numbers
☐ Medications
☐ Medical Records
☐ Race/Ethnicity
☐ Tax Identification Number
☐ Medical Record Number
☐ Gender/Sex
☒ Integrated Control Number (ICN)
☐ Military History/Service Connection
☐ Next of Kin
☐ Date of Death
☐ Business Email Address
☐ Electronic Data Interchange Personal Identifier (EDIPI)
☒ Other Data Elements (List Below)

Other PII/PHI data elements: PHI Provided by Patient in Response to Prompts, SSOi Security Identification Number (SECID), Identification Number, VA Email Address

**1.2 List 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?*

- The system collects PHI from the patient as part of the application function.
- The system obtains appointment and demographic data from VISTA

*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.*

The appointment data is needed to determine the necessary action the system must make to ensure the patient is receiving email or text notifications in a timely manner (prior to appointment). Furthermore, the system needs to be able to determine if the patient has been seen by the pain clinic previously (within certain frames) to order the correct type and number of measures.

Veteran Profile information is needed so that the system can attempt to contact the patient using the latest contact information.

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

Yes, the system creates information such as a score for each individual computer adaptive measure, History of Present Illness note, reports, and data analysis.

**1.3 Methods of information collection**

*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?*

Yes, the information that the CHOIR system receives from VISTA regarding the appointment is identifiable so that the system can make determinations on the appropriate actions based on who the patient is and if they are new or returning to the Pain clinic. This automation allows the clinic staff to spend more time providing medical services and less time managing the system.

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

No, the information collected by the system is not form based and uses a computer adaptive technology originally developed by the National Institute of Health Common Fund program Patient Reported Outcomes Management Information System (PROMIS).

**1.4 Information checks for accuracy, and how often will it be checked.**

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

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

The information captured by the system and generated by the system is intended to be used as a tool to assist the provider in determining a diagnosis and potential therapies. The system stores name, date of birth, phone numbers, email addresses, security identification number, and integrated control numbers. This data is received from the electronic health record via VA internal services. The storage allows the system to provide continuity between appointment events and to return data electronically or manually back to the health record. While accuracy is important, the provider should be again using this to discuss with the patient their care and any current or past issues and this acts as validation of the data. The engine that is used by the system is validated by Stanford University against known good version prior to its inclusion in any new releases of the CHOIR software.

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

No, a commercial aggregator for this information does not exist.

**1.5 Identify the specific legal authorities, arrangements, and agreements that defined the collection of information.**

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

The legal authority for collecting information is as follow: USC Title 5 Section 552a, is also known as the Privacy Act of 1974, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals maintained in systems of records by federal agencies. The Act requires agencies to restrict the collection of relevant information, ensure accuracy, and inform individuals about the purpose and authority for collecting their information.

**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: The collection ties with the purpose of the underlying mission of the organization and its enabling authority.*

*Principle of Minimization: The information is directly relevant and necessary to accomplish the specific purposes of the program.*

*Principle of Individual Participation: The program, to the extent possible and practical, collects information directly from the individual.*

*Principle of Data Quality and Integrity: VA policies and procedures must ensure that personally identifiable information is accurate, complete, and current.*
*This 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 system collects, processes, and retains PII and PHI on Veterans and on Members of the Public. If this information was breached or accidentally disclosed to inappropriate parties or the public, it could result in personal and financial harm to the individuals impacted and adverse negative effect to the VA.

**Mitigation:** Data collected, processed, and retained will be protected in accordance with VA Handbook 6500 and FIPS 140-2 encryption and data in-transit protection standards. All systems and individuals with access to the system will be approved, authorized, and authenticated before access is granted. VA annual privacy and security training compliance will be enforced for all VA employees, contractors, and vendors.

## Section 2. Uses of the Information

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

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

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

| PII/PHI Data Element | Internal Use | External Use |
|---|---|---|
| Name | Identification | Not Used |
| Date of Birth | Determine Age Related Needs | Not Used |
| Personal Phone Number(s) | Not Used | Send Notifications to Patient |
| Personal Email Address | Not Used | Send Notifications to Patient |
| Integrated Control Number (ICN) | Identification and Communication With Other VA Systems | Not Used |
| PHI Provided by Patient in Response to Prompts | Generate Scores, History of Present Illness, and Reports | Not Used |
| SSOi Security Identification Number (SECID) | Identification | Not Used |
| Identification Number | Identification | Not Used |
| VA Email Address | Not Used | Send Notifications to Provider |

**2.2 Describe the types of tools 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.*

The system uses a validated implementation of the National Institute of Health Patient Report Outcomes Management Information System (PROMIS). The system uses the response of the patient to validated measures in calculating probabilities of the patients likely hood of a particular diagnosis. The system has a set threshold that once exceeded allows the system to discontinue asking questions as it relates to that particular measure.

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

The system collects the answers from the patient and uses these to determine a probability of diagnosis. The system has a set threshold that it needs to be confident in the probability and will ask questions in different dimensions and based on the additional answers, calculates a new probability. This process is repeated until the set threshold is met or exceeded upon which it ceases to ask questions for that measure. The data is then used to create a History of Present Illness note in plain text. Additionally, the data is presented in a consolidated report that includes longitudinal display of scores of the patient for the provider to then use as part of their determination of care.

*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.*

Upon completion of a set of prescribed measures, the system creates both a History of Present Illness (HPI) note and consolidated report that is used by the provider to assist them in deciding regarding the patient's diagnosis or types of therapies.

**2.3 How the information in the system is 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 in transit is encrypted using VA approved Transport Layer Security (TLS) and cryptography algorithms.

*2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs? (refer to PTA question 3.8).*

This system does not collect, processes, or retain Social Security Numbers.

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

- VA approved encryption such as FIPS 140-2 or current version, Transparent Data Encryption (data at rest), Virtual disk and volume encryption and File/folder encryption
- Intrusion Detection and Protection Systems (IDPS)
- Firewall rulesets

- Endpoint security to scan for malware other threats to confidentiality and integrity
- Physical and logical access control mechanisms
- Change control processes
- Reverse proxy for internet accessible site

**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?*

Users have access to the PII that is stored in CHOIR as a right of access outlined in the VHA Notice of Privacy Practices (NoPP). The data is transferred as a History of Present Illness note and summary reports to the electronic health record (VISTA ). Access to PII is determined by the location clinic that the user is currently assigned to and provides services at. The user administrator at the location or a supporting user administrator confirms each user with the location/clinic management prior to approval. The user application is responsible for assigning users to the appropriate user roles to limit access for different parts of the application and assuring PII safeguards as documented in the user manual, technical manual, and system design document.

*2.4b Are criteria, procedures, controls, and responsibilities regarding access documented? How are the documented, i.e. Policy, SOP, other. And where is this documentation located?*

The criteria, procedures, controls, and responsibilities regarding access are documented in the Governance, Risk, and Compliance tool and in the access control document AC VIPR Account Control Standard Operating Procedure (SOP).

*2.4c Does access require manager approval?*

Yes

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

Yes

*2.4e Who is responsible for assuring safeguards for the PII as identified in eMASS?*

The Information System Owner is responsible for documenting and assuring the safeguards are implemented as described in eMASS.

## Section 3. Retention of Information

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

**3.1 What information is retained?**

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

The system retains all of the information that is collected and generated. Additionally, the generated data and reports are transferred to the electronic health record to ensure it is available to the provider in a timely manner.

**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 https://www.archives.gov/records-mgmt/grs? This question is related to privacy control DM-2, Data Retention and Disposal.*

Per SORN 24VA10A7: POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: In accordance with the records disposition authority approved by the Archivist of the United States, paper records and information stored on electronic storage media are maintained for seventy-five (75) years after the last episode of patient care and then destroyed/or deleted. VHA Records Control Schedule (RCS 10–1), Chapter 6.

**3.3 The retention schedule 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. Please work with the system VA Records Officer to answer these questions.*
*This question is related to privacy control DM-2, Data Retention and Disposal.*

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

Yes

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

Data within the system is retained until its decommissioning or is migrated to a replacement system. The data that is transferred to the system of record is held in accordance with the records disposition authority approved by the Archivist of the United States, paper records and information stored on electronic storage media are maintained for seventy-five (75) years after the last episode of patient care and then destroyed/or deleted. VHA Records Control Schedule (RCS 10–1), Chapter 6.

**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 is not removed from CHOIR. The status of the Veteran can be changed but policy is to never remove a record. Data is retained until the system is decommissioned or migrated to a new replacement system. CHOIR is not a system of record and data is stored on Database servers operated by OI&T. If the system is decommissioned destruction or migration will be handled by OI&T with support from the CHOIR team as needed.

**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.*

All Information Technology (IT) system and application development and deployment is handled by the CHOIR program office. The CHOIR Program Management Office (PMO) does test the system for VHA operations prior to deployment and Personally Identifiable Information (PII) / Personal Health Information (PHI) may be used for that Alpha or Beta testing at the facility-level per VHA policy. In addition, VHA may need to train staff on functionality in the new or modified IT system. Training, including on IT systems, is part of health care operations and per VHA policy, PII and PHI may be used for that training purpose. However, VHA must minimize the use of PII and PHI in training presentations or materials per VA policy. In case human subject research was intended to be covered by this control, VA Research investigators may use PII for VA Institutional Review Board (IRB)- approved research and there is no effort to minimize the use of PII for research. Controls for protecting PII used for testing, training and research are often security controls if the PII is electronic. When paper PII, reasonable safeguards for protecting the PII are to be employed.

**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 Privacy Officer (PO) 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: The project retains only the information necessary for its purpose, additionally, the PII is retained only for as long as necessary and relevant to fulfill the specified purposes.*

*Principle of Data Quality and Integrity: The PIA should describe 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 contained in the system will be retained for longer than is necessary to fulfill the VA mission. Potential impact is that the data is exposed to users without need.

**Mitigation:** The system manages the risk as described in section 3.4.

## Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

**PII Mapping of Components**

4.1a **Collaborative Health Outcomes Information Registry** consists of five (5) key components (servers/databases/instances/applications/software/application programming interfaces (API)). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **Collaborative Health Outcomes Information Registry** 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 server names in the table. The first table of 3.9a in the PTA should be used to answer this question.

*Internal Components Table*

| **Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI** | **Does this system collect PII? (Yes/No)** | **Does this system store PII? (Yes/No)** | **Type of PII (SSN, DOB, etc.)** | **Reason for Collection/ Storage of PII** | **Safeguards** |
|---|---|---|---|---|---|
| Web Server | Yes | No | • Name<br>• Integrated Control Number (ICN)<br>• Date of Birth | To enable authorized personnel to view patient information and assist in completion of assessments. | Transmittal: HTTPS (TLS), TCP/IP Protocols |

**4.1b List internal organizations information is shared/received/transmitted, the information shared/received/transmitted, and the purpose, and how the information is transmitted.**

**NOTE: Question 3.9b (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*

| ***IT system and/or Program office. Information is shared/received with*** | ***List the purpose of the information being shared /received with the specified program office or IT system*** | ***List PII/PHI data elements shared/received/transmitted.*** | ***Describe the method of transmittal*** |
|---|---|---|---|
| VHA VistA | A user with HIPPA compliant access will manually transfer information into VISTA. System will transition to using services from OI&T to electronically transfer the data into VISTA and associate it with the patient and provider. | • Name<br>• Integrated Control Number (ICN)<br>• PHI Provided by Patient in Response to Prompts<br>• Identification Number | HTTPS (TLS), TCP/IP Protocols |

**4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure**

*Discuss the privacy risks associated with the sharing of information within the VA network 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 in this section.).*

*This question is related to privacy control UL-1, Internal Use.*
Follow the format below:

**Privacy Risk:** There is very little risk in transmitting, viewing, and uploading the data from Collaborative Health Outcomes Information Registry to the electronic health record. Information may be compromised through shoulder surfing which may result in a breach of confidentiality. When transferring data via an electronic means, this risk becomes even smaller.

**Mitigation:** The VA Rules of Behavior are required to be signed by all personnel prior to accessing any VA related equipment according to VA Directive and Handbook 6500. Only authorized users have access. Role-based access for VA activity is restricted by least privilege account management. Penalties are executed to the full extension of the law if a breach in confidentiality is determined.

## 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 List the external organizations (outside VA) that information shared/received. and information shared/received, and the purpose, and how the information transmitted and what measures are taken to ensure it is secure.**

**The sharing of information outside the agency must be compatible with the original collection. The sharing must be covered by an appropriate routine use in a SORN. If not covered, 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 IT System or External Program Office information is shared/received with*** | ***List the purpose of information being shared / received / transmitted*** | ***List the specific PII/PHI data elements that are processed (shared/received/transmitted)*** | ***List agreements such as: Contracts, MOU/ISA, BAA, SORN. 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 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure**

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

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

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

Follow the format below:

**Privacy Risk:** There is no external sharing.

**Mitigation:** There is no external sharing.

## 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 The notice provided to the individual before collection of the information. Please provide a copy and/or screen shot of a web notice of the notice as an Appendix-A 6.1 on the last page of the document. (A notice may include a posted privacy policy, a Privacy Act notice on forms, notice given to individuals by the sources system, or a system of records notice published in the Federal Register.) If notice was not provided, explain why.**

*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 Provide the Privacy Notice provided to the public by this system or any source systems. Include a copy of the notice in Appendix A of the PIA, the Federal Register citation, or Privacy Statement from collection of information such as forms or surveys.*

As a tool used by VHA staff, Privacy Notices for CHOIR collection are commensurate with VHA's own Privacy Notices. During the course of VHA operations, notice is provided in the following ways, as explained in further detail below:
1. VHA Notice of Privacy Practice (NOPP)
2. This Privacy Impact Assessment (PIA)
3. Applicable System of Record Notice (SORN)
4. Written notice on all VA forms

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

This Privacy Impact Assessment (PIA) also serves as notice as required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means." (Privacy Impact Assessments (PIA) - Privacy)

Notice is also provided in the Federal Register with the publication of the System of Record Notice 24VA10A7 / 85 FR 62406, *Patient Medical Records – VA.* The information is for Collaborative Health Outcomes Information Registry use only and is stated in the Privacy Notice.

*6.1b If notice was not provided, explain why.*

Notice was provided as stated in 6.1a.

*6.1c Provide how the notice provided at the time of collection meets the purpose of use for this system.*

CHOIR notice is adequate as it is aligned with VHA's own notice practices as described in 6.1a.

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

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

The CHOIR application is provided PII/PHI from the EHR system of record which implements the federal regulations that apply to Standards for Privacy of Individually Identifiable Health Information (Individual Participation IP-1 Consent control of the VA Information Security Reference Guide - Page 158). Any patient can decline to be followed by the pain clinic staff utilizing the CHOIR clinical operational program. The Facility Directory Opt-Out Overview for staff members responsible for disclosure directs to the Opt-Out Fact Sheet detailing steps necessary to allow for opt-in or opt-out. The patient is not penalized or denied service if they choose to opt-out.

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

*This question is directed at whether an individual may provide consent for specific uses, or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent.*

Information is used, accessed, and disclosed in accordance with the Privacy Act, 5 USC 552a, Title 38 USC 5701, Confidential Nature of Claims, Title USC 7332 and the HIPAA Privacy Rule 45 CFR.

Individuals are provided with a copy of the Notice of Privacy Practices that indicates when information will be used without their consent and when they will be asked to provide consent.

Individuals or their legal representative may consent to the use or disclosure of information via a written request submitted to their facility Privacy Officer. Individuals also have the right to request a restriction to the use of their information. The written request must state what information and/or to whom the information is restricted and must include their signature and date of the request. The request is then forwarded to facility Privacy Officer for review and

processing. Individuals may also request to Opt-Out of the facility directory during an inpatient admission. If the individual chooses to opt-out, information is not disclosed from the facility directory unless otherwise required by law.

### 6.4 PRIVACY IMPACT ASSESSMENT: Notice

*Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your Privacy Officer (PO) 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: This is referring to sufficient notice provided to the individual.*

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

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

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

## Section 7. Access, Redress, and Correction

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

### 7.1 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 VA Public Access Link-Home (efoia-host.com) to obtain information about FOIA points of contact and information about agency FOIA processes.***

All data inquiries are to be addressed to the CHOIR Dev Support at VHAPHOVIPRDEVSUPPORT@va.gov. There are several ways a veteran or other beneficiary may access information about themselves. The Department of Veterans Affairs has created the MyHealthEVet program to allow online access to their medical records. More information on this program and how to sign up to participate can be found online at https://www.myhealth.va.gov/index.html. Veterans and other individuals may also request copies of their medical records and other records containing personal data from the medical facility's Release of Information (ROI) office. VHA Directive 1605.01, Privacy and Release of Information, Paragraph 7 outlines policy and procedures for VHA and its staff to provide individuals with access to and copies of their PII in compliance with the Privacy Act and HIPAA Privacy Rule requirements. VHA also created VA form 10-5345a for use by individuals in requesting copies of their health information under right of access. VA Form 10-5345a is voluntary but does provide an easy way for individual to request their records.

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

This system is not exempt from the access provisions of the Privacy Act.

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

This is a Privacy Act 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.*

The individual has the right to request amendment of erroneous information in accordance with the Privacy Act and HIPAA Privacy Rule. Any discrepancies are to be reported to CHOIR Dev Support for correction via VHAPHOVIPRDEVSUPPORT@va.gov.

**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.*

Individuals have access to the Notice of Privacy Practices which states the following relating to procedures for correcting their information: "Right to Request Amendment of Health Information". You have the right to request an amendment (correction) to your health information in our records if you believe it is incomplete, inaccurate, untimely, or unrelated to your care. You must submit your request in writing, specify the information that you want corrected, and provide a reason to support your request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains your information. If your request for amendment is denied, you will be notified of this decision in writing and provided appeal rights. In response, you may do any of the following:

- File an appeal.
- File a "Statement of Disagreement".
- Ask that your initial request for amendment accompany all future disclosures of the disputed health information.

**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.*

Formal redress is provided as indicated above.

**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 Privacy Officer (PO) to complete all Privacy Risk questions in this section).*

*Consider the following FIPPs below to assist in providing a response:*
*Principle of Individual Participation: The individual must be provided with the ability to find out whether a project maintains a record relating to them.*

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

*Principle of Individual Participation: The mechanism by which an individual is able to prevent information about them obtained for one purpose from being used for other purposes without their knowledge.*
*This question is related to privacy control IP-3, Redress.*

Follow the format below:

**Privacy Risk:** There is a risk that members of the public will not know the relevant procedures for gaining access to, correcting, or contesting their information.

**Mitigation:** The risk of incorrect information in an individual's records is mitigated by authenticating information when possible. Additionally, staff verifies information in medical records and corrects information identified as incorrect during each patient's medical appointments. The NOPP discusses the process for requesting an amendment to one's records.

## Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures. (Work with your ISSO to complete this section).

**8.1 The procedures in place to determine which users may access the system, must be 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?*

CHOIR inherits network security controls from the VA infrastructure. CHOIR requires the user to request access either directly in the system or via the clinical leadership. In all cases, users must be validated as having an association with the location/clinic in order to obtain a role that allows access to read patient data.

*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?*

CHOIR utilizes network security controls inherited from the VA infrastructure to ensure that only authorized users can access the VA network and CHOIR application. Furthermore, CHOIR implements additional authentication security controls to ensure users have the appropriate access to the software and corresponding data. CHOIR also contains auditing features that allow administrators and the Veteran Integrated Pain Record PMO the ability to

audit individual user actions and follow VA SOPs with respect to disciplinary action. Users from another agency would have to be validated as part of a clinic or location.

*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.*

User – able to manually add patients, order assessments, update data
Physician - able to manually add patients, order assessments, update data
Analyst – limited data viewing
System Administrator – No PII/PPHI access
User Administrator – No PII/PHI access

**8.2a. Will VA contractors have access to the system and the PII?**

CHOIR and the VA ensure that all personnel take annual security training and pass VA Privacy and Information Security Awareness training. All users of the CHOIR project team are required to sign a Rules of Behavior agreement prior to being given access to CHOIR systems. Additionally, the Rules of Behavior is required to be reviewed and signed annually by each user. Annual training for the National Rules of Behavior is performed through the Talent Management System (TMS). There are two versions of the National Rules of Behavior: one for VA employees and one for contractors. Definitions of VA employee and VA Contractor:

• VA Employees - VA employees are all individuals who are employed under title 5 or title 38, United States Code, as well as individuals whom the Department considers employees such as volunteers, without compensation employees, students, and other trainees.

• VA Contractors - VA contractors are non-VA users having access to VA information resources through a contract, agreement, or other legal arrangement and will have access to the system. Contractors must meet the security levels defined by the contract, agreement, or arrangement. Contractors must read and sign the Rules of Behavior and complete security awareness and privacy training prior to receiving access to the information systems.

Users agree to comply with all terms and conditions of the National Rules of Behavior by signing a certificate of training at the end of the training session.

**8.2b. What involvement will contractors have with the design and maintenance of the system?**

Contractors are used for the design and maintenance of the systems code base, troubleshooting system issues, and providing survey coordination services. The coordination services include the management of a locations appointments, assessments, and ensuring the information produced by the system is transferred to the EHRM.

**8.2c. Does the contractor have a signed confidentiality agreement?**

No

**8.2d. Does the contractor have an implemented Business Associate Agreement for applicable PHI?**

Yes

**8.2e. Does the contractor have a signed non-Disclosure Agreement in place?**
*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.*

The contract is reviewed yearly by the Veteran Integrated Pain Record (VIPR) Program Management Office (PMO). The access to the underlying system by the engineering support teams allows them to troubleshoot issues in a timely manner and identify roots causes. Survey Coordinators are providing direct support to the location/clinic and will need to be able to review records to ensure the system is working as expected and transfer reports and system generated notes to the EHRM.

**8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?**

*VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately. This question is related to privacy control AR-5, Privacy Awareness and Training.*

VA requires Privacy and Information Security Awareness & Rules of Behavior training to be completed on an annual basis. The Talent Management System offers the following applicable privacy courses: VA 10176: Privacy and Information Security Awareness and Rules of Behavior VA 10203: Privacy and HIPPA Training VA 3812493: Annual Government Ethics

**8.4 The Authorization and Accreditation (A&A) completed for the system.**

*8.4a If Yes, provide:*

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

IOC date 2/1/2025

## Section 9 – Technology Usage

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

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

*If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.* ***(Refer to question 1.8 of the PTA)***

No, the system does not use cloud technology.

**9.2 Does the contract with the Hosting 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 3.3.1 of the PTA)*** *This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

System does not use a Cloud Service Provider.

**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.*

System does not use a Cloud Service Provider.

**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.*

System does not use a Cloud Service Provider.

**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).*

System does not utilize Robotics Process Automation.

## 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.**

NANCY KATZ-JOHNSON

Digitally signed by NANCY KATZ-JOHNSON
Date: 2025.01.06 15:56:33 -05'00'

**Privacy Officer, Nancy Katz-Johnson**

CRAIG HEITZ

Digitally signed by CRAIG HEITZ
Date: 2025.01.14 14:16:06 -06'00'

**Information System Security Officer, Craig Heitz**

MARK MEHELIS

Digitally signed by MARK MEHELIS
Date: 2025.01.06 07:20:57 -08'00'

**Information System Owner, Mark L. Mehelis**

## APPENDIX A-6.1

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

1. Notice of Privacy Practice (NOPP): VHA Directive 1605.04 IB 10-163p (va.gov)

2. Privacy Impact Assessments (PIA):
   https://department.va.gov/privacy/privacy-impact-assessments/

3. 24VA10A7 / 85 FR 62406, *Patient Medical Records – VA*:
   https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

## HELPFUL LINKS:

**Records Control Schedule 10-1 (va.gov)**

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

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

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

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

**Notice of Privacy Practice (NOPP):**
VHA Directive 1605.04
IB 10-163p (va.gov)