Privacy Impact Assessment for the VA IT System called:

# Enabling Technologies for Rapid Learning Health Systems

# Office of Research & Development (ORD) Massachusetts Veterans Epidemiology Research and Information Center (MAVERIC)

# Cooperative Studies Program (CSP)

# Office of Research and Development (ORD)

# Veterans Health Administration (VHA)

# #1807

Date PIA submitted for review:

2/29/2024

System Contacts:

| | Name | E-mail | Phone Number |
|---|---|---|---|
| Privacy Officer | Nora Begley | Nora.Begley2@va.gov | 857-203-5924 |
| Information System Security Officer (ISSO) | Stuart E. Chase | Stuart.chase.va.gov | 410 340-2018 |
| Information System Owner | Nicholas Best | Nicholas.best.va.gov | 857-364-5581 |

## Abstract

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

Enabling Technologies for Rapid Learning Health Systems (ENTHRALL) is a data platform that aggregates patients' longitudinal clinical history with molecular profile data and displays this information in summary table and dashboard views for providers, in order to inform clinical decisions. The database will serve as a knowledge base for providers (e.g., results of prior treatment, etc.) when encountering similar cases. A key functionality of ENTHRALL is trial matching. Finding clinical trials for oncology patients is an important aspect of clinical care especially those with metastatic diseases. The platform will include curated data about clinical trials that the patient may be eligible for, based on information in the patient's medical history. The system categorization is Moderate.

## 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. What is the IT system name and the name of the program office that owns the IT system?*

Enabling Technologies for Rapid Learning Health Systems and the program office that owns the system is Office of Research & Development (ORD) - Massachusetts Veterans Epidemiology Research and Information Center (MAVERIC) & Cooperative Studies Program (CSP) Coordinating Center - Boston, MA.

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

The ENTHRALL (Enabling Technologies for Rapid Learning Health Systems) platform enables workflow, data capture, search, role management and reporting capability in the clinical setting. The functionality is aimed to aid healthcare personnel with their workload and supply efficiency especially regarding data management. An example of an ENTHRALL system is Oncology Application (OncApps), an application that aggregates patients' longitudinal clinical history with molecular profile data, and displays this information in summary, table, and dashboard views for providers, to inform clinical decisions. Another key functionality is trial matching (MPACT), finding clinical trials for oncology patients is an important aspect of clinical care especially those with metastatic diseases. Other examples, include PASI (lung cancer screening focus), CSP2017 (call center workflow), PROGRESS (prostate cancer screening), VA-Io (facilitating

enrollment), MOAlmanac (genomic almanac), Tumor Board (multi-disciplinary tumor board data management), GBM/RareCancers (workflow quality improvement), Geriatric (frailty scoring to aid in cancer treatment decision for geriatric patients), RandRobbins (assigns clinical trial labels to patients based on an algorithm), and the TrialTracker (tracking the status of LOIs and Trial statuses). ENTHRALL employs development tools approved by the Technical Reference Model [TRM].

*C. Who is the owner or control of the IT system or project?*

ENTHRALL is owned and operated by the VA.
Veterans Health Administration (VHA), Office of Research and Development (ORD), Cooperative Studies Program (CSP), Massachusetts Veterans Epidemiology Research and Information Center (MAVERIC), Boston VA Healthcare Informatics.

*2. Information Collection and Sharing*

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

The expected number of individuals whose information is stored in the system is less than 100,000.
The typical affected individual are Veterans who have been diagnosed with cancer and the VA employees involved in the healthcare of such Veterans (i.e., doctors, nurses, technical support, etc.).

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

The system will collect personally identifiable information (PII) and personal health information (PHI) of Veterans. This includes, but is not limited to, Race/Ethnicity, Gender, Addresses, Dates, Phone numbers, Personal Emails, Social Security Numbers, Medications, Medical record numbers, Integrated Control Number (ICN), etc.
The purpose for collecting this information is to aid in clinical trial matching (automatically identifying patients that fit criteria of clinical trials), tumor board management (tracking changes in patient status), and generally supporting healthcare workers by improving workflow processes with automation.

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

The system shares PII and PHI (such as names, race, ethnicity, dates, social security numbers, etc.) with the Veterans Health Administration (VHA) Corporate Data Warehouse (CDW) via custom code and Microsoft SQL Server Integration Service (SSIS) packages. The CDW is the standard repository provided by the VA that contains all PHI and PII of all Veterans.

The system shares PII and PHI (such as names, race, ethnicity, dates, social security numbers, contact info, medications, medical records, etc.) with the Veterans Health Administration (VHA) National Precision Oncology Program (NPOP) via custom code and Microsoft SQL Server Integration Service (SSIS) packages. NPOP is a specialized subset of CDW that contains more detailed cancer-related data.

The system shares PII and PHI (such as names, race, ethnicity, dates, social security numbers, contact info, medications, medical records, etc.) with the Veterans Health Administration (VHA) Capital Region Readiness Center (CRRC) Martinsburg, WV facility via custom code. CRRC Martinsburg provides the resources necessary to develop and host the ENTHRALL information system.

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

The system is only operated from the Capital Region Readiness Center (CRRC) Martinsburg, WV facility. All resources and operations necessary for the system is provided by this facility.

*3. Legal Authority and SORN*

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

SOR Number/Federal Register Citation: 24VA10A7 / 85 FR 62406
System Title: Patient Medical Records-VA
https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf
Federal Register / Vol. 85, No. 192 / Friday, October 2, 2020 / Notices, Page 62407
AUTHORITY FOR MAINTENANCE OF THE SYSTEM:
Title 38, United States Code, Sections 501(b) and 304.

SOR Number/Federal Register Citation: 172VA10 / 86 FR 72688
System Title: VHA Corporate Data Warehouse-VA
https://www.govinfo.gov/content/pkg/FR-2021-12-22/pdf/2021-27720.pdf
Federal Register/Vol. 86, No. 243/Wednesday, December 22, 2021/Notices, Page 72689
AUTHORITY FOR MAINTENANCE OF THE SYSTEM:
Title 38, United States Code, Section 501.

*B. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?*

Whether the implementation of this PIA will change business processes is not applicable because the ENTHRALL automates a current business process. ENTHRALL does not modify the system and is utilizing current approved infrastructure.

*4. System Changes*

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

No

*B. Will 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. 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
- ☒ 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) Address Numbers
- ☒ Medications
- ☒ Medical Records
- ☒ Race/Ethnicity
- ☐ Tax Identification Number
- ☒ Medical Record Number
- ☒ Gender
- ☒ Integrated Control Number (ICN)
- ☐ Military History/Service Connection
- ☐ Next of Kin
- ☒ Other Data Elements (list below)

Other PII/PHI data elements collected by ENTHRALL:

- VA Employee Names
- VA Employee Work Emails

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

**PII Mapping of Components (Servers/Database)**

Enabling Technologies for Rapid Learning Health Systems (ENTHRALL) consists of one key components (database). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Enabling Technologies for Rapid Learning Health Systems 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 3.9 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 |
|---|---|---|---|---|---|
| • ENTHRALL<br>• CSP2017<br>• ONCAPP<br>• PASI<br>• VABIO<br>• ProGRESS | **Yes** | **Yes** | • Names<br>• Race/Ethnicity<br>• Gender<br>• Addresses. All geographical subdivisions smaller than a state<br>• Dates. All elements of dates (except year). For dates directly related to an individual.<br>• Phone numbers<br>• Personal Emails<br>• Work Emails<br>• Social Security Numbers<br>• Medications<br>• Medical record numbers<br>• Integrated Control Number (ICN)<br>• Other unique identifying number, characteristic, or code (generated by the identified components/databases). | The purpose for collecting this information is to aid in clinical trial matching (automatically identifying patients that fit criteria of clinical trials), tumor board management (tracking changes in patient status), and generally supporting healthcare workers by improving workflow | PIV Enforcement. The VA enforces two-factor authentication by enforcing smartcard logon requirements. PIV cards are issued to employees, contractors, and partners in accordance with HSPD-12. The Personal Identify Verification (PIV) Program is an effort directed and managed by |

| | | | | | |
|---|---|---|---|---|---|
| | | | | processes with automation. | the Homeland Security Presidential Directive 12 (HSPD-12) Program Management Office (PMO). IT Operations and Services (ITOPS) Solution Delivery (SD) is responsible for the technical operations support of the PIV Card Management System. |

**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?*

- Veterans Health Administration (VHA) Corporate Data Warehouse (CDW).
- Veterans Health Administration (VHA) National Precision Oncology Program (NPOP).

*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.*

ENTHRALL uses internal data sources available within the VA network to support healthcare workers with automated workflows, leading to quicker and more efficient healthcare of veterans.

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

ENTHRALL does create its own data, such as follow-up tasks for tumor boards, analyses, and reports. But it is currently not planned to become a source of information for use by other systems.

**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?*

The ENTHRALL system uses a mixture of automated scripts (custom code made with R, Python, SQL, etc.) and Microsoft SQL Server Integration Services (SSIS) packages to connect to the Corporate Data Warehouse (CDW) and the National Precision Oncology Program (NPOP) data sources.

*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?*

This is not applicable because ENTHRALL does not use paper documents.

**1.4 How will the information be checked for accuracy? How often will it be checked?**

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

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

The CDW and NPOP data sources have data accuracy checks that ENTHRALL is not involved in.
Data is pulled from the CDW and NPOP data sources into the ENTHRALL system once every day via automated scripts and SSIS packages to ensure accurate data.
Front-end users of ENTHRALL web applications check the data every day and will message the ENTHRALL development team of any data inaccuracies.

*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?*

This is not applicable to ENTHRALL.
ENTHRALL does not connect to any commercial aggregators of information at all.
ENTHRALL does not pass any information to any commercial entity.
ENTHRALL operates only within the internal VA network.

**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*

SOR Number/Federal Register Citation: 172VA10 / 86 FR 72688
System Title: VHA Corporate Data Warehouse-VA
https://www.govinfo.gov/content/pkg/FR-2021-12-22/pdf/2021-27720.pdf

Federal Register/Vol. 86, No. 243/Wednesday, December 22, 2021/Notices, Page 72689
AUTHORITY FOR MAINTENANCE OF THE SYSTEM:
Title 38, United States Code, Section 501.

**1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information**

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

**Privacy Risk:** ENTHRALL is a data platform that aggregates patients' longitudinal clinical history with molecular profile data. The database does contain PII Information; Unauthorized disclosure of this information would give visibility into an individual's Information and Health records. Additionally, it would violate the privacy act of 1974 and HIPAA. This may have a serious adverse effect on VA operations, assets, or individuals.

**Mitigation:** Mitigation measures include access control, awareness and training, audit and accountability, certification, accreditation, and security assessments, configuration management,

contingency planning, identification and authentication, incident response, maintenance, media protection, physical and environmental protection, planning, personnel security, risk assessment, systems and services acquisition, system and communications protection, and system and information integrity.

## 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 |
|---|---|---|
| Names | Used to identify the patient during appointments and in other forms of communication. | Not used |
| Race/Ethnicity | Used for patient demographic information and for indicators of ethnicity-related diseases. | Not used |
| Gender | Used for patient demographic information and for indicators of gender-related diseases. | Not used |
| Mailing Address | Used for communication, billing purposes and calculate travel pay. | Not used |
| Date of Birth | Used to identify age and confirm patient identity. | Not used |
| Phone Numbers | Used for communication, confirmation of appointments and conduct Telehealth appointments. | Not used |
| Patient Personal Emails | Used for communication, confirmation of appointments and conduct Telehealth appointments. | Not used |
| VA Employee Work Emails | Used to identify users and track their application usage within the information system. | Not used |
| Social Security Numbers | Used as a patient identifier and as a resource for verifying income Information with the Social Security Administration. | Not used |
| Medications | Used within the medical records for health care purposes/treatment, prescribing medication, and allergy interactions. | Not used |

| | | |
|---|---|---|
| Medical Record Numbers | Used to identify a patient within the medical record system without using their social security number as their identifier. Also used for continuity of health care. | Not used |
| Integrated Control Number | Used to identify a patient within the medical record system without using their social security number as their identifier. Also used for continuity of health care. | Not used |

**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?*

ENTHRALL supports phenotyping capabilities, including natural language processing, from patients' medical records.
Additionally, it displays scoring metrics and performs ranking based on patient's existing medical information.

*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.*

The ENTHRALL system is not an official system of record, it aids clinicians and coordinators with their daily workflow by presenting existing patient information in a specific way.
Any new data or information produced from analysis by ENTHRALL can be consistently reproduced with code.

**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?*

Advanced Encryption Standard (AES) 256 safeguards are in place, servers are stored in a secured environment and managed with restricted access controls.

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

Access and control to ENTHRALL is provided through PIV enforcement. Criteria, procedures, controls, and responsibilities regarding access is documented through PIV login.

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

Controls are in place to assure that the information is handled in accordance with the uses described above to include mandatory online information security and Privacy and HIPAA training; face-to-face training for all incoming new employees conducted by the Information System Security Officer and Privacy Officer; and regular audits of individuals accessing sensitive information to ensure information is being appropriately used and controlled.

**2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.**

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

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

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

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

*2.4a How is access to the PII determined?*

Access is requested through a SharePoint document and approved/declined by the program manager. Access and control to ENTHRALL is protected with PIV enforcement.

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

Criteria, procedures, controls, and responsibilities regarding access is documented via 3rd party tools with enterprise licenses like Microsoft Teams, SharePoint, and GitHub repositories. Access to documentation is protected with PIV enforcement.

*2.4c Does access require manager approval?*

Access to PII/PHI is reviewed and approved by the program manager.

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

Access requests to use the ENTHRALL information system are recorded via SharePoint documents. These documents can also be exported and audited

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

The same training for clinical staff (i.e., clinicians/nurses) to access CPRS and CAPRI is applicable here.

## 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 following information is retained by the system:
Names
Race/Ethnicity
Gender
Mailing Addresses
Birth Dates
Patient Phone numbers
Patient Personal Emails
VA Employee Work Emails
Social Security Numbers
Medications
Medical record numbers
Integrated Control Number (ICN)

**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.*

Patient medical records are retained for a total of 75 years after the last episode of care. Department of Veterans Affairs Record Control Schedule (RCS)10-1, Part Three, Chapter Six-Healthcare Records, Item 6000.1a. and 6000.1d.
https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

**3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)?**
*An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the*

*proposed schedule, the VA records officer will notify the system owner. Please work with the system Privacy Officer and VA Records Officer to answer these questions.*
*This question is related to privacy control DM-2, Data Retention and Disposal.*

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

Yes

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

Department of Veterans Affairs Record Control Schedule (RCS)10-1, Part Three, Chapter Six-Healthcare Records, Item 6000.1a. and 6000.1d.

**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.*

Sanitization of electronic media authorized for destruction (or upon system decommission), will be carried out in accordance with VA Directive 6500 (January 23, 2019), VA Cybersecurity Program, Policy, Protect Function, Media Sanitization, sections a-m.
https://www.va.gov/digitalstrategy/docs/VA_Directive_6500_24_Jan_2019.pdf
This affects electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, etc. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destructio. Additionally, this system follows Field Security Service (FSS) Bulletin #176 dated April 9, 2014 for Media Sanitization Program, SOPs - FSS - All Documents as well as FSS Standard Operating Procedures (SOP) MP-6 Electronic Media Sanitization."

Paper documents are destroyed to an unreadable state in accordance with the Department of Veterans' Affairs VA Directive 6371 (October 29, 2010), DESTRUCTION OF TEMPORARY PAPER RECORDS.
https://www.vendorportal.ecms.va.gov/FBODocumentServer/DocumentServer.aspx?DocumentId=505240&FileName=VA251-12-R-0228-003.PDF

**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.*

VA Directive 6500 mandates that Systems under development should not process "live data" or do any real processing in which true business decisions will be based. Test data used to test and develop systems, that have not yet undergone security Assessment and Authorization (A&A), must be de-identified.

- Per the HIPAA Privacy laws, data that has been de-identified is no longer defined as PII. The PO can personally assure that the data has been properly de-identified or the VA form 10- 250 can be used for this assurance.
- Systems that are in development (pilot, proof-of-concept, or prototype) should not be attached to VA networks without first being assessed and authorized.
- Healthcare Portal (i.e. MyHealthyVet, etc.) provides encryption through secure messaging for compliance with FIPS 140-2 policy. Additionally, the Healthcare Portal enrollment process supports verifying a subject's identity before allowing access to the application for increased authentication.
- Mobile media must follow the encryption standards as set forth in the ESO Data and Media Protection SOP.

ENTHRALL uses the following techniques to minimize risk to privacy when using PII/PHI for research, testing, and training:

- Requiring yearly certification of the privacy training courses within the VA Talent Management System (TMS 2.0) for all ENTHRALL personnel and users, such as the VA Privacy and Information Security Awareness and Rules of Behavior.
- Maintaining separate environments for research and operational projects.
- Maintaining separate environments (SQL databases and servers) for development, testing, and production data.
- Hosting all environments within the internal VA network. ENTHRALL is not accessible from outside the internal VA network.
- Managing and logging access requests to ENTHRALL via SharePoint documents.
  CSPCC Boston - Help Desk - Access Request (sharepoint.com)
  ENTHRALL Access Request Form (sharepoint.com)
- Enforcing login to environments with PIV credentials.

**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:**

Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious harm may result for the individuals affected.

**Mitigation:**

ENTHRALL employs a variety of security measures designed to ensure that the information is not inappropriately disclosed or released. These measures include access control, awareness and training, audit and accountability, certification, accreditation, and security assessments, configuration management, contingency planning, identification and authentication, incident response, maintenance, media protection, physical and environmental protection, planning, personnel security, risk assessment, systems and services acquisition, system and communications protection, and system and information integrity.
Employees complete the Privacy and HIPAA Focused training as well as the VA Privacy and Information Security Awareness & Rules of Behavior training annually. The VA enforces two-factor authentication by enforcing smartcard logon requirements. PIV cards are issued to employees, contractors, and partners in accordance with HSPD-12. The Personal Identity Verification (PIV) Program is an effort directed and managed by the Homeland Security Presidential Directive 12 (HSPD-12) Program Management Office (PMO). IT Operations and Services (ITOPS) Solution Delivery (SD) is responsible for the technical operations support of the PIV Card Management System.

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

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

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

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

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

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

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

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

*Data Shared with Internal Organizations*

| ***List the Program Office or IT System information is shared/received with*** | ***List the purpose of the information being shared /received with the specified program office or IT system*** | ***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*** | ***Describe the method of transmittal*** |
|---|---|---|---|
| Veterans Health Administration Corporate Data Warehouse | ENTHRALL is a data platform that aggregates patients' longitudinal clinical history with molecular profile data, and displays this information in a summary view | • Names<br>• Race/Ethnicity<br>• Gender<br>• Addresses. All geographical subdivisions smaller than a state<br>• Dates. All elements of dates (except year) for dates directly related to an individual. | • SQL Server Integration Services (SSIS) packages using OLE DB and ADO.NET database connections transfer data to local instance in Martinsburg, WV. |

| *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* |
|---|---|---|---|
| | | • Patient Phone Numbers<br>• Patient Personal Emails<br>• VA Employees Work Emails<br>• Social Security Numbers<br>• Medications<br>• Medical record numbers<br>• Integrated Control Number (ICN)<br>• Other unique identifying number, characteristic, or code (generated by the identified components/databases). | • Custom scripts written in Python and R languages using ODBC Driver 17 for SQL Server database connections transfer data to local instance in Martinsburg, WV. |
| Veterans Health Administration National Precision Oncology Program (NPOP) Database | ENTHRALL is a data platform that aggregates patients' longitudinal clinical history with molecular profile data, and displays this information in a summary view | • Names<br>• Addresses. All geographical subdivisions smaller than a state<br>• Dates. All elements of dates (except year) for dates directly related to an individual.<br>• Patient Phone Numbers<br>• Social Security Numbers<br>• Medical record numbers<br>• Integrated Control Number (ICN)<br>• Other unique identifying number, characteristic, or code (generated by the identified components/databases). | • SQL Server Integration Services (SSIS) packages using OLE DB and ADO.NET database connections transfer data to local instance in Martinsburg, WV.<br>• Custom scripts written in Python and R languages using ODBC Driver 17 for SQL Server database connections transfer data to local instance in Martinsburg, WV. |

| *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 Martinsburg Data Center, WV | ENTHRALL is a data platform that aggregates patients' longitudinal clinical history with molecular profile data, and displays this information in a summary view | • Names<br>• Race/Ethnicity<br>• Gender<br>• Addresses. All geographical subdivisions smaller than a state<br>• Dates. All elements of dates (except year) for dates directly related to an individual.<br>• Patient Phone Numbers<br>• Medications<br>• Patient Personal Emails<br>• VA Employees Work Emails<br>• Social Security Numbers<br>• Medical record numbers<br>• Integrated Control Number (ICN)<br>• Other unique identifying number, characteristic, or code (generated by the identified components/databases). | • Web applications developed using ODBC Driver 17 for SQL Server database connections to query and modify data in local instance in Martinsburg, WV. |

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

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

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

Follow the format below:

**<u>Privacy Risk:</u>**

The ENTHRALL front-end web applications are only accessible to authorized users that have submitted an Access Request Form via SharePoint document. The Access Request Form will determine what content the users can see. Web app functionality is limited based on what level of permissions the authorized user has. The patient data viewable by authorized users is further limited by the user's primary VA site and other VA sites relevant for their workflow. Where possible, the last 4 SSN will be used instead of full SSN. The risk for unauthorized users to access PII/PHI and viewing patients not relevant to their workflow is minimal.

The possible risks for unauthorized users to access PII/PHI comes from:

- The personnel involved in the process of reviewing, approving, and granting access to users may mistakenly authorize the wrong user and grant users the wrong level of permissions or VA site access.
- A malicious entity may steal the PIV card and associated PIN of an authorized user and login to the ENTHRALL information system or front-end web app.

**Mitigation:**

Maintain PIV enforcement for access control of PII/PHI for users to view patients at their own VA site and use last 4 SSN where possible. Enforce completion and up-to-date certification of privacy training (such as the Rules of Behavior training) within the VA Talent Management System (TMS) for all ENTHRALL staff.

## 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*** |
|---|---|---|---|---|
| | | No information is shared/received to outside VA. | | |
| | | | | |

## 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:**

No information is shared/received to outside VA.

**Mitigation:**

No information is shared/received to outside VA.

## 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.*

SORN reference 172VA10A7 (VHA Corporate Data Warehouse-VA).
Notice of Privacy Practices, effective date 9-30-2019 (NOPP_IB163 final 7-17-19). Version Date: October 1, 2021 **Page 18 of 30**

https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=8928
https://www.oprm.va.gov/docs/Current_SORN_List_12_3_2021.pdf

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

Department of Veterans Affairs
Veterans Health Administration
NOTICE OF PRIVACY PRACTICES
Effective Date: September 30, 2022
https://www.va.gov/files/2022-10/10-163p_%28004%29_-Notices_of_Privacy_Practices-_PRINT_ONLY.pdf

*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.*

The Notice of Privacy Practices explains the VHA collection and use of protected information. A signed acknowledgement of having read and understood the NOPP is part of the individual's electronic file. When the NOPP is updated, all VHA beneficiaries receive a mailed copy.

**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.*

SORN reference 172VA10A7. Notice of Privacy Practices, effective date 9-30-2019 (NOPP_IB163 final 7-17-19).

Information is needed to administer benefits to veterans and other potential beneficiaries. While an individual may choose not to provide information, this may prevent them from obtaining services and benefits.

**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.*

SORN reference 24VA1087 and 172VA10A7. Notice of Privacy Practices, effective date 9-30-2019 (NOPP_IB163 final 7-17-19).
Individuals must submit a request in writing to their facility Privacy Officer. The request must state what information and/or to whom the information is restricted and must include their signature and date of the request. Individuals may also request to Opt-Out of the facility directory during an inpatient admission. If the individual chooses to opt-out, no information on the individual is given out.

Individuals can request further limitations on other disclosures. A veteran, legal guardian or court appointed Power of Attorney can submit a request to the facility Privacy Officer to obtain information.

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

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

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

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

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

**<u>Privacy Risk:</u>**
Individuals are unaware of the process to amend health records.

**Mitigation:**
Notice is provided through the Notice of Privacy Practices, which is provided to patients upon enrollment and upon revision.

## 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.***

Individuals have a right of access under the Privacy Act of 1974. Individuals may request a copy of their records and receive an Accounting of Disclosures through the Health Information Management Service.

*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 is not applicable to ENTHRALL.
ENTHRALL 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 not applicable to ENTHRALL.
ENTHALL is a Privacy Act system.

**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 may contact facility Privacy Officer for Amendment Request.
Individuals are required to provide a written request to amend or correct their records to the appropriate Privacy Officer or System Manager as outlined in the Privacy Act SOR. Every Privacy Act SOR contains information on Contesting Record Procedure which informs the individual who to contact for redress.
Veterans are informed of the amendment process by many resources to include the VHA Notice of Privacy Practice (NOPP) which states: 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 Version Date: October 1, 2021 Page 35 of 58
File a "Statement of Disagreement"
Ask that your initial request for amendment accompany all future disclosures of the disputed health information.

**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.*

Through the Notice of Privacy Practices, individuals are notified of process to amend health information and request restriction.

**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.*

Redress is provided thru Amendment and Restriction processes.
Individuals are required to provide a written request to amend or correct their records to the appropriate Privacy Officer or System Manager as outlined in the Privacy Act SOR. Every Privacy Act SOR contains information on Contesting Record Procedure which informs the individual who to contact for redress.

**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:**

Includes inaccurate health information such as demographics, medical information, sex, age, medications, etc. 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:**

Individuals have a right to request amendment and restriction of use of information contain within the ENTHRALL system.
VA Cooperative Studies Program Coordinating Center (CSPCC) Boston mitigates the risk of incorrect information in an individual's records by authenticating information when possible, using the resources discussed in question 1.5. Additionally, staff verifies information in medical records and corrects information identified as incorrect during each patient's medical appointments.
As discussed in question 7.3, the NOPP, which every enrolled Veteran receives every three years or when there is a major change. The NOPP discusses the process for requesting an amendment to one's records.
VA Boston's Release of Information (ROI) office is available to assist Veterans with obtaining access to their health records and other records containing personal information.
The Veterans' Health Administration (VHA) established MyHealtheVet program to provide Veterans remote access to their medical records. The Veteran must enroll and have access to the premium account to obtain access to all the available features. In addition, VHA Directive 1605.01 Privacy and Release of Information establishes procedures for Veterans to have their records amended where appropriate.

## 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?*

The control and access to ENTHRALL is controlled and maintained by PIV enforcement. Individuals receive access to the Area VA Cooperative Studies Program Coordinating Center (CSPCC) Boston by gainful employment in the VA or upon being awarded a contract that requires access to the Area systems. Upon employment, the Office of Information & Technology (OI&T) creates computer and network access accounts as determined by employment positions assigned. Users are not assigned to software packages or network connections that are not part of their assigned duties or within their assigned work area. VA Area Boston requires access to the GSS be requested using the local access request system. VA staff must request access for anyone requiring new or modified access to the GSS. Staff are not allowed to request additional or new access for themselves.

*8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?*

Access is requested utilizing Electronic Permission Access Area Boundary (ePAS). Users submit access requests based on need to know and job duties. Supervisor, ISSO and OI&T approval must be obtained prior to access granted. These requests are submitted for VA employees, contractors and all outside agency requests and are processed through the appropriate approval processes. Once access is granted, individuals can log into the system(s) through dual authentication, i.e., a PIV card with a complex password combination. Once inside the system, individuals are authorized to access information on a need-to-know basis.
Strict physical security control measures are enforced to ensure that disclosure to these individuals is also based on this same principle. Generally, VA file areas are locked after normal duty hours and the facilities are protected from outside access by the Federal Protective Service or other security personnel. Access to computer rooms at VA Area Boston is generally limited by appropriate locking devices and restricted to authorized VA IT employees. Access to information stored on automated storage media at other VA locations is controlled by individually unique passwords/codes. Access by Office of Inspector General (OIG) staff conducting an audit, investigation, or inspection at the health care area, or an OIG office location remote from the health care area, is controlled in the same manner.
Access to the Area Boston working and storage areas is restricted to VA employees who must complete both the HIPAA and Information Security training. Specified access is granted based on the employee's functional category. Role based training is required for individuals with significant information security responsibilities to include but not limited to Information System Security (ISSO), local Area Manager, System Administrators, Network Administrators, Database Managers, Users of VA Information Systems or VA Sensitive Information.

*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.*

Human Resources notify Divisions, IT of new hires and their start date(s), through email. The Division that the person is going into fills out the local access form, Automated Systems Access Request form, with name, SSN and/or claim number, job title, division, and telephone number, along with marking the boxes on the form for application access the user will need on the computer system. This form starts at the Division level, is signed by the Division Chief, and Director, for signatures and then to IT for implementation.
•Individuals are subject to a background investigation before given access to Veterans' information.
•All personnel with access to Veterans' information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually AND Privacy and HIPAA Focused Training.

The procedures described above must be completed for all VA employees before they are granted access to ENTHRALL. To gain access to ENTHRALL, VA employees must submit an ENTHRALL Access Request Form SharePoint document. Each access request will be reviewed and approved by the ENTHRALL Project Manager before granting access to the user.

Users are assigned access to VA sites/stations so that they can only view data within their assigned sites. There are also multiple levels of permissions that can be granted to users, where each level allows users access to more functionality of ENTHRALL. Users may have more than one level of permission. The levels of permissions are described below:

- covid_nccaps_general
  COVID NCCAPS - General User Access with read & write capabilities.
- geriatric_general
  Geriatric App - General User Access with read & write capabilities.
- repop_general
  REPOP - General User Access with read & write capabilities.
- trial_matching_admin
  Trial Matching - Administrator Access with read & write capabilities. Can also see more details about clinics and filter by clinics.
- trial_matching_general
  Trial Matching - General User Access with read & write capabilities.
- tumor_board_admin
  Tumor Board - Administrator Access with read & write capabilities. Can also create and manage groups of users within Tumor Board.
- tumor_board_general
  Tumor Board - General User Access with read-only capabilities.
- tumor_board_member
  Tumor Board - Board Member Access with read & write capabilities.

**8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?**

*If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII. This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

No VA contractors will have access to the ENTHRALL. Only full-time VA employees will have access to ENTHRALL

**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.*

10176 VA Privacy and Security Information Training – TMS, renewed annually. 10203 Privacy and Security Awareness, ROB, renewed annually.

**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:* 4/10/2023
3. *The Authorization Status:* Authorization to Operate (ATO)
4. *The Authorization Date:* 6/19/2023
5. *The Authorization Termination Date:* 6/18/2024
6. *The Risk Review Completion Date:* 6/2/2023
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.***

ENTHRALL has an Authorization to Operate (ATO)

## 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.*

ENTHRALL 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.*

ENTHRALL 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.*

ENTHRALL 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).*

ENTHRALL does not use Robotics Process Automation (RPA)

## 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.**

NORA BEGLEY

Digitally signed by NORA BEGLEY
Date: 2024.03.12 10:15:10 -04'00'

**Privacy Officer, Nora Begley**

STUART CHASE

Digitally signed by STUART CHASE
Date: 2024.03.12 09:57:12 -04'00'

**Information System Security Officer, Stuart E. Chase**

NICHOLAS BEST

Digitally signed by NICHOLAS BEST
Date: 2024.03.12 11:05:45 -04'00'

**Information System Owner, Nicholas Best**

## APPENDIX A - HELPFUL LINKS

**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 Notice of Privacy Practices
VHA Handbook 1605.04: Notice of Privacy Practices
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=8928

**Privacy Act System of Records Notices (SORNs):**
Privacy Act System of Records Notices (SORNs) - Privacy
2021-27720.pdf (govinfo.gov)
https://www.oprm.va.gov/docs/Current_SORN_List_12_3_2021.pdf