



Privacy Impact Assessment for the VA IT System called:

# Electronic Health Record Modernization (EHRM) Defense Healthcare Management System Modernization (DHMSM) Train

## VA Central Offices (VACO)

# Electronic Health Record Modernization Integration Office (EHRM-IO)

Date PIA submitted for review:

May 22, 2023

System Contacts:

*System Contacts*

	Name	E-mail	Phone Number
Privacy Officer	Angela Pluff	Angela.Pluff@va.gov	315-263-3653
Information System Security Officer (ISSO)	Jeramy Drake	Jeramy.Drake@va.gov	509-956-8865
Information System Owner	Michael Hartzell	Michael.Hartzell1@va.gov	803-406-0112

## Abstract

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

The Electronic Health Record Modernization Defense Healthcare Management System Modernization Train system, EHRM DHMSM Train, is a VA Pre-production (Pre-Prod) reciprocity system mirroring the DHMSM Train system, dedicated to training of end users of the Production EHR Core system. The EHR Core along with other Millennium ancillary applications, solutions, and platforms, collectively referred to as the Federal EHR system, enhances patient care and provider effectiveness, enables the application of standardized workflows, integrated healthcare delivery, data standards and interoperability for improved and secure electronic exchange of patient health records among participating Federal partners, namely DoD, VA, Department of Homeland Security (DHS) U.S. Coast Guard (USCG), and Department of Commerce's National Oceanic and Atmospheric Administration (NOAA). A single, common EHR helps create a more seamless health care experience for service members transitioning from active duty to Veteran status. When fully implemented, the Federal EHR system will benefit over 9 million Veterans and their qualified family members, increasing their access to care and improving health outcomes.

## Overview

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

### 1 General Description

- A. *The IT system name and the name of the program office that owns the IT system.*  
The full name of this VA reciprocity system is The Electronic Health Record Modernization (EHRM) Defense Healthcare Management System Modernization (DHMSM) Train system, EHRM DHMSM Train, which is owned by the Electronic Health Record Modernization Integration Office (EHRM-IO).
- B. *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*  
By launching a modern EHR system and creating a seamless health care experience, the EHRM program enables VA to fulfill its mission to improve the delivery of quality health care to Veterans, enhance the provider experience and promote interoperability with the Department of Defense and community care providers. This system is a training module and an integrated part of the overall new Federal EHR system, dedicated to end user training before and during early days of deployment of the new EHR system in each and all VA sites.
- C. *Indicate the ownership or control of the IT system or project.*  
The VA reciprocity system, in essence, is a Federal Information Security Modernization Act (FISMA) compliance shell mirroring the source DoD system, DHMSM Train, which is owned and controlled by the Program Executive Office, Defense Healthcare Management Systems (PEO DHMS), an acquisition organization with a direct reporting relationship to the Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD-A&S) and administratively attached to the Defense Health Agency (DHA).

## 2. Information Collection and Sharing

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

Unlike the Production systems, this Pre-production system only uses, processes, stores a limited set of patient records, for training purpose, which can be ranged from a few hundreds to a few thousand records of Veterans and/or their beneficiaries. Those records will be completed removed/deleted once each training project is completed.

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

This Pre-Prod system contains a limited set of patient health record of Veterans and/or their beneficiaries with data elements to include personally identifiable information (PII)/protected health information (PHI) such as Social Security Number, DoD Electronic Data Interchange Personal Identifier (EDIPI) – the system default prime identifier, VA Integration Control Number (ICN), name, date of birth, mailing address, patient admission and discharge information, medical benefit and eligibility information, etc. The answer to question 1.1. provides a full list of key data elements used by the system. Meanwhile, the intended purpose(s) of use of each key data element can be found in the answer to question 2.1.

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

As a Pre-Prod training module, no information sharing takes place with this system.

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

DHMSM Train resides in the DHA-authorized Disaster Recovery site security boundary, at Oracle Health data center in Lee Summit, MO.

## 3. Legal Authority and SORN

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

The legal authority to collect data pursuant to the Privacy Act of 1974 is stated in VA SORN 24VA10A7, Patient Medical Records-VA, published in FR 85, 62406, on October 2, 2020. For cross referencing purpose, the legal authority for the source system is DoD SORN EDHA-07, Military Health Information System, published in Federal Register (FR) 85, 36190, on June 15, 2020. The authority to operate the system is stated in 38 U.S. Code § 8111 - Sharing of Department of Veterans Affairs and Department of Defense health care resources, as well as 10 U.S. Code § 1104 - Sharing of health-care resources with the Department of Veterans Affairs.

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

The afore-mentioned VA SORN has been modified and published following an Opinion Memorandum on “common record” issued by the VA Deputy General Counsel for General Law (02GL) on October 9, 2019. More detail can be found in answer to question 1.5. No SORN amendment or revision is expected.

D. System Changes

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

No change to existing business processes is expected as result of this PIA completion.

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

The completion of this PIA will not result in any technology change of the underlined reciprocity system.

## 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://vawww.va.gov/vapubs/>). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.

This question is related to privacy control AP-1, Authority To Collect, and AP-2, Purpose Specification.

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

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

- |  |  |  |
|--|--|--|
| <input checked="" type="checkbox"/> Name                     | <input checked="" type="checkbox"/> Emergency Contact Information (Name, Phone Number, etc. of a different individual) | <input checked="" type="checkbox"/> Vehicle License Plate Number           |
| <input type="checkbox"/> Social Security Number              | <input checked="" type="checkbox"/> Financial Information  | <input checked="" type="checkbox"/> Internet Protocol (IP) Address Numbers |
| <input checked="" type="checkbox"/> Date of Birth            | <input checked="" type="checkbox"/> Health Insurance Beneficiary Numbers   | <input checked="" type="checkbox"/> Medications                            |
| <input checked="" type="checkbox"/> Mother's Maiden Name     | <input checked="" type="checkbox"/> Certificate/License numbers* Occupational, Medical, and Education                  | <input checked="" type="checkbox"/> Medical Records                        |
| <input checked="" type="checkbox"/> Personal Mailing Address |  | <input checked="" type="checkbox"/> Race/Ethnicity                         |
| <input checked="" type="checkbox"/> Personal Phone Number(s) |  | <input type="checkbox"/> Tax Identification Number                         |
| <input checked="" type="checkbox"/> Personal Fax Number      |  | <input checked="" type="checkbox"/> Medical Record Number                  |
| <input checked="" type="checkbox"/> Personal Email Address   |  | <input checked="" type="checkbox"/> Gender                                 |

- Integrated Control Number (ICN)
- Military History/Service Connection

- Next of Kin
- Other Data Elements (list below)

Additional data elements included in the system: DoD Electronic Data Interchange Personal Identifier (EDIPI), Date of death, Guardian name and contact information, Employment Information, Education information, Veteran Dependent Information, Research medical statistics, Service-connected rating and disabilities, Criminal background information.

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

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

The system consists of 0 (zero) key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by the EHR Core system and the reasons for the collection of the PII are in the table below.

**Note:** Due to the PIA being a public facing document, please do not include the server names in the table. **The first table of 3.9 in the PTA should be used to answer this question.**

*Internal Database Connections*

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
N/A			N/A		N/A

**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?*

For training purpose, limited data set is sourced from the Production DHMSM EHR Core system to the designated Pre-prod training environment for simulation and training of new users.

*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.*

For training purpose, limited data set is sourced from the Production DHMSM EHR Core system to the designated Pre-prod training environment for simulation and training of new users.

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

No new information is created by the DHMSM Train.

### **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?*

Limited data set is sourced/collected from the Production DHMSM EHR Core system and loaded to the designated Pre-prod training environment for simulation and training of new users.

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

N/A

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

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

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

N/A

*1.4b If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.*

N/A

### **1.5 What specific legal authorities, arrangements, and agreements defined the collection of information?**

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

The authority for the system to collect, use, and disseminate information about individuals that is maintained in systems of records by federal agencies, in accordance with the code of fair information practices established by the Privacy Act of 1974, as amended, 5 U.S.C. § 552a. From DHA point of view, such authority is stated in System of Record Notification (SORN) EDHA-07, Military Health Information System, (<https://dpcl.d.defense.gov/Portals/49/Documents/Privacy/SORNs/DHA/EDHA-07.pdf>) published in Federal Register (FR) 85, 36190, on June 15, 2020. The correspondent VA SORN is 24VA10A7, Patient Medical Records-VA, published in FR 85, 62406, on October 2, 2020 (<https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf>). On March 13, 2014, the VA and DoD jointly signed a Memorandum of Understanding (MOU) for Sharing Personal Information to establish a framework governing inter-Departmental transfer of Personally Identifiable Information/Protected Health Information (PII/PHI) of beneficiaries who receive health care and/or other benefits from either Department.

#### **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:** Millennium, as part of the source DHMSM EHR Core system, collects PII for the purposes of healthcare treatment and management servicing Veterans, beneficiaries, and Military Service Members. The information is collected or created directly from the patients and inputted by authorized system users and clinical staff using various methods. Information is also collected



electronically through various secure data sharing mechanism as specified in section 1.3. Due to the highly sensitive nature of this data, there is a risk that, if the data was accessed by unauthorized individual(s) or otherwise breached, serious personal, professional, or financial harm may result for the individuals affected.

**Mitigation:** The Departments employ a variety of security measures to ensure that the information is not inappropriately accessed, 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. All security controls have been implemented in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 and applicable VA Directives. Privacy measures will include authority and purpose, accountability, audit and risk management, data quality and integrity, data minimization and retention, individual participation and redress, transparency, and use limitation; consistent with VHA Directive 1605.2, Minimum Necessary Standard for Access, Use, Disclosure, and Requests for Protected Health Information.

## Section 2. Uses of the Information

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

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

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

- Name: Used to identify the patient during appointments and in other forms of communication
- Date of Birth: Used to identify age and confirm patient identity
- Mother's Maiden Name: used to confirm patient identity
- Personal Mailing Address: used for communication, billing purposes and calculate travel pay
- Personal Phone Number(s): used for communication, confirmation of appointments and conduct Telehealth appointments
- Personal Fax Number: used to send forms of communication and records to business contacts, Insurance companies and health care providers
- Personal Email Address: used for communication, including the patient portal MyHealthVet secure communication
- Emergency Contact Information (Name, Phone Number, etc. of a different individual): used in cases of emergent situations such as medical emergencies.
- Financial Information: used to calculate co-payments and VA health care benefit eligibility
- Health Insurance Beneficiary Numbers/Account Numbers: used to communicate and bill third-party Health care plans



- Certificate/License numbers: (specifying types such as occupational, educational, medical) used to track and verify legal authority to practice medicine and licensure for health care workers in an area of expertise.
- Internet Protocol (IP) Address Numbers: used for configuration and network connections. Network Communication allows information to be transferred from one Information Technology System to another.
- Medications: used within the medical records for health care purposes/treatment, prescribing medications and allergy interactions.
- Medical Records: used for continuity of health care
- Race/Ethnicity: used for patient demographic information and for indicators of ethnicity-related diseases.
- Medical Record Number: this data element is replaced by/combined with the prime identifier EDIPI, which is used to identify individual/record.
- Gender: is used to identify patient demographic, type of medical care/provider and medical tests required in healthcare operations
- Integration Control Number (ICN): The VA ICN is used as a back-up identifier for user/record verification purpose
- Military history/service connection: Used to evaluate medical conditions that could be related to location of military time served. It is also used to determine VA benefit and health care eligibility.
- Next of Kin: Used in cases of emergent situations such as medical emergencies. Used when patient expires and in cases of patient incapacity.
- Electronic Data Interchange Personal Identifier (EDIPI): is the prime identifier/ medical record number and is used for patient identity and internal VA user authentication
- Date of Death: indicates the official date of death
- Guardian Name and Contact Information: used in healthcare operations when patient is unable to make decisions for themselves.
- Employment Information: used to determine VA employment eligibility and for veteran contact, financial verification
- Education information: used to record education level, graduation date.
- Veteran Dependent Information: used to determine benefit support and as an emergency contact person
- Research medical statistics: up on training objectives, users may need to be trained on health statistics for better understanding of risk factors for communities, monitoring diseases, or assessing quality and safety of health care
- Service-connected Rating and Disabilities: Used to determine VA health care eligibility and treatment plans/programs
- Criminal Background Information: used to determine employment eligibility and during VA Police investigations.

## **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.*

N/A – this is a Pre-Prod Training system.

*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.*

N/A - this is a Pre-Prod Training system.

### **2.3 How is the information in the system secured?**

*These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.*

*2.3a What measures are in place to protect data in transit and at rest?*

Data at rest is encrypted using Security Hash Algorithm SHA-256; data in transit uses Transport Layer Security (TLS) 1.2 cryptographic protocol.

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

Data at rest and data in transit is protected with SHA-256 and TLS 1.2.

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

This Pre-Prod system is protected with the same set of security and privacy controls implemented for the Production systems. The system complies to requirements set forth by OMB Memorandum M-06-15, Safeguarding Personally Identifiable Information, by means of obtaining an ATO from the DHA AO, a proof of FISMA Reform compliance. Among more than 400 security and privacy controls implemented, there are controls implemented to address security awareness and training requirements for the system users, personnel security, physical security, auditing and monitoring, and cybersecurity/privacy incident response.

### **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 of the system are authorized to access to PII based on a need-to-know basis in the performance of their official job duties, commensurate to their user role in the system.

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

Even though being a Pre-Prod system, DHMSM Train follows the same strict policy and procedures for user provisioning, identification and authentication as applicable to a Production environment, documented in the account management standard operating procedure, which covers criteria, procedures, roles and responsibilities, and applicable security controls in accordance with NIST SP 800-53 Rev 4.

2.4c Does access require manager approval?

User access to the system does require direct supervisor/manager approval, similar to the procedure applied to a Production system.

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

Network and system auditing, monitoring controls are in place, in accordance with applicable DoD and VA cybersecurity policies.

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

The System Owner is ultimately responsible for assuring safeguards for the PII collected by and stored in the system.

## **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*

A copy of a limited set of patient PII/PHI is sourced/collected and used during training, then will be completely removed from the environment once the training session is ended.

### **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.*

A copy of a limited set of patient PII/PHI is sourced/collected and used during training, then will be completely removed from the environment once the training session is ended – following VA RCS-10-1.

### **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, all records are stored within the boundary defined by the DHA and VHA SORN's detailed in section 1.5 – for the VHA records, RCS10-1 (<https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf>) is used.

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

For the common record owned by VA, the VA RCS10-1 schedule, line item 6000.2b – Electronic Final Version of Health Record, is applied (<https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf>).

### **3.4 What are the procedures for the elimination or transfer of SPI?**

*Explain how records are destroyed, eliminated or transferred to NARA at the end of their mandatory retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc.? This question is related to privacy control DM-2, Data Retention and Disposal.*

Applicable VA and DoD procedures will be followed to destroy, eliminate, or transfer of the common records in the system at the end of their mandatory retention period.

### **3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?**

*Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.*

The Pre-Prod Training system does not use PII for research or testing. Even though this is a training system, users must comply with access control, personnel security, awareness and training, and auditing requirements as if it were a Prod system. Only copy of a limited set of PII is used for training simulation purpose hence privacy risk is minimized.

### **3.6 PRIVACY IMPACT ASSESSMENT: Retention of information**

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

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

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

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

*Principle of Data Quality and Integrity: Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?*

*This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.*

Follow the format below:

**Privacy Risk:** The risk of letting the (source DoD) system holding certain types of VA data beyond the length of time (years, or months) mandated by applicable provision outlined in VHA Records Control Schedule 10-1 can arise in the case of common records shared among two, and now four Federal agency partners. Further complication may arise when different standards applied to different partners co-exist for the same type of data or share records.

**Mitigation:** Ensure/validate that PII is completely removed/purged once each training project is ended. Since only copy of a limited set of PII is used for training simulation purpose hence privacy risk is minimized.

## 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.*

<i>List the Program Office or IT System information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</i>	<i>Describe the method of transmittal</i>
N/A	N/A	N/A	N/A

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

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

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

Follow the format below:

**Privacy Risk:** A privacy risk may arise when highly sensitive controlled unclassified information (CUI) including PII is accidentally disclosed in training sessions.

**Mitigation:** Ensure only relevant CUI/PII elements are included in the copy of limited data set designed and intended for use in training projects.

## **Section 5. External Sharing/Receiving and Disclosure**

The following questions are intended to define the content, scope, and authority for information sharing external to VA, which includes Federal, State, and local governments, and the private sector.

**5.1 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?**

**Is the sharing of information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.**

**NOTE: Question 3.10 on Privacy Threshold Analysis should be used to answer this question.**

*Identify and list the names of any Federal, State, or local government agency or private sector organization with which information is shared.*

*For each interface with a system outside VA, state what specific data elements (PII/PHI) are shared with each specific partner.*



What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.

This question is related to privacy control UL-2, Information Sharing with Third Parties

*Data Shared with External Organizations*

<i>List External Program Office or IT System information is shared/received with</i>	<i>List the purpose of information being shared / received / transmitted with the specified program office or IT system</i>	<i>List the specific PII/PHI data elements that are processed (shared/ received/ transmitted) with the Program or IT system</i>	<i>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</i>	<i>List the method of transmission and the measures in place to secure data</i>
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.

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:** VA patient data is now collected and retained in a shared database as part of the Federal EHR may expose to certain privacy/security risks such as unauthorized access or being used for purposes other than the stated purpose and use of the original collection.

**Mitigation:** Beside the 2014 MOU signed between the then-Secretaries of DoD and VA, the two agencies have entered into several inter-agency MOA, MOU/ISA, in line with the NIST recommended Risk Management Framework (RMF) and applicable OMB Memoranda, CNSSI, DoD and VA policies and procedures to ensure data safeguarding and information privacy controls are implemented as having designed to prevent and/or detect violation or compromise situations, maintaining an acceptable risk level for the operating systems, both in Prod and Pre-Prod environments.

## 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.*

Since data used in this Pro-Prod Train module is sourced from the Prod EHR Core system, the same privacy control sets applicable to the Prod system will be used for the Pre-Prod. With reference to the “Notice” requirements, beside the SORN publication in the Federal Register in October 2020 as having mentioned in 1.5, the current publication of the VHA Notice of Privacy Practices (NOPP) can be found in the VHA webpage, <http://www.va.gov/health/>, under the “Resources” section. A copy of the NOPP must be provided to a patient/Veteran in person when they present for services. Alternatively, a copy of the most recently distributed NOPP will be mailed to eligible veterans every 3 years by the VHA.

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

The latest publication of the VHA Notice of Privacy Practices (NOPP) can be found in the VHA webpage, <http://www.va.gov/health/>, under the “Resources” section. All users of the MyHealthVet patient portal can also access the same NOPP publication when logging in their account in the portal.

A copy of the NOPP must be provided to a patient/Veteran in person when they present for services. Alternatively, a copy of the revised/latest NOPP will be mailed to eligible veterans every 3 years by the VHA.

*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.*

VHA is required by law to maintain the privacy of Veterans/patients protected health information and to provide the Veterans/patients with notice of VHA legal duties and privacy practices. Beside the publication of the System of Record Notice in the Federal Register, the VHA Notice of Privacy Practice outlines the ways in which VHA may use and disclose Veterans/patients health information without their permission as required or permitted by law. For VHA to use or disclose Veterans/patients health information for any other purposes, VHA is required to get the Veteran's/patient's permission in the form of a signed, written authorization. The latest NOPP digital publication can be found in the Resources section of the VHA webpage (<http://www.va.gov/health/>) A copy of the NOPP must be provided to a patient/Veteran in person at the time they are admitted for services at a VHA health care facility. Alternatively, a copy of the revised/latest NOPP will be mailed to eligible veterans every 3 years by the VHA.

**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.*

To apply for enrollment in the VA health care system, all Veterans are required to fill out VA Form 10-10EZ. The information provided on this form will be used by VA to determine eligibility for medical benefits. The applicant is not required to disclose their financial information; however, VA is not currently enrolling new applicants who decline to provide their financial information unless they have other qualifying eligibility factors. If a financial assessment is not used to determine the applicant's eligibility for cost-free medication, travel assistance or waiver of the travel deductible, and the applicant chooses not to disclose personal financial information, the applicant will not be eligible for these benefits. More details and instruction for VA Form 10-10EZ can be found through the Resources section of the VHA webpage at [va.gov/health/](http://va.gov/health/) or at this link [https://www.va.gov/vaforms/medical/pdf/VA\\_Form\\_10-10EZ.pdf](https://www.va.gov/vaforms/medical/pdf/VA_Form_10-10EZ.pdf).

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

*This question is directed at whether an individual may provide consent for specific uses or the consent is given to cover all uses (current or potential) of his or her information. If specific consent*

is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent.

Yes, individuals have the right to consent to particular uses or disclosures of their health information of which VHA does not have other legal authority to disclose. Individuals are directed to use VA Form 10-5345, Request for and Authorization to Release Health Information, to consent to or authorize what health information can be released to whom and for what purpose. Consents to use the information would be processed through the original source system, the Prod DHMSM EHR Core system..

#### **6.4 PRIVACY IMPACT ASSESSMENT: Notice**

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

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

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

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

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

Follow the format below:

**Privacy Risk:** An individual may not receive notice that their information is being collected, maintained, processed, or disseminated by the VA prior to providing the information.

**Mitigation:** This risk is mitigated by the common practice of providing the VHA Notice of Privacy Practice (NOPP) when Veterans present for service. New NOPPs are mailed to the patients/Veterans every 3 years and periodic monitoring is performed to check that the acknowledgment form signed by patients have been scanned into electronic records. Additional mitigation is provided by making the System of Record Notices (SORNs) and NOPP available for review online.

([https://www.oprm.va.gov/privacy/systems\\_of\\_records.aspx](https://www.oprm.va.gov/privacy/systems_of_records.aspx) and <http://www.va.gov/health/> )

## **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.*

As having stated in the VHA NOPP, Veterans/patients have the right to review and obtain a copy of their health information by means of completing VA Form 10-5345a – Individuals' Request for a Copy of their Own Health Information, to the facility Privacy Officer of the VHA facility that provided or paid for their care. Form 10-5345a can be obtained from the facility webpage or the VA online repository at the link <https://www.va.gov/find-forms/about-form-10-5345a>. Additionally, Veterans/patients can gain access to their health record by enrolling in the VA patient portal, myHealthVet, at <https://www.myhealth.va.gov/index.html>

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

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.*

Not applicable. This 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.*

Right to Request Amendment of Health Information: Veterans/patients have the right to request an amendment (correction) of their health information in Federal EHR records if they believe it is incomplete, inaccurate, untimely, or unrelated to their care. A request in writing must be submitted to the facility Privacy Officer, specifying the information to be corrected, including a reason to support the request for amendment. Reference the VHA NOPP, which can be found in the Resources section of the VHA webpage (<http://www.va.gov/health/>.) Alternatively, a copy of the revised/latest NOPP will be mailed to eligible veterans every 3 years by the VHA.

## **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.*

The NOPP, outlining the procedure for Veterans/patients request amendment (correction) of their health information, is provided to the Veteran/patient at the time their information being collected and subsequently each time they are admitted for care service. If they enroll in the patient portal, a digital version of the NOPP is also available for their awareness. Alternatively, a copy of the latest NOPP will be mailed to all eligible veterans every 3 years by the VHA. Veterans/patients are expected to review and understand the said procedures as well as the NOPP in its completeness, so that they can properly exercise their rights. Particularly, the procedures also address the situation when a request for amendment is denied - Veterans/patients will be notified of such decision in writing and given information about their right to appeal the decision. In response, the Veterans/patients may do any of the following: file an appeal, file a “Statement of Disagreement” which will be included in their health record, or ask that their initial request for amendment accompany all future disclosures of the disputed health information. Reference the VHA NOPP, which can be found in the Resources section of the VHA webpage (<http://www.va.gov/health/>.)

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

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

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

The processes outlined in 7.2 and 7.3 are considered formal redress process. To ensure data accuracy and maintain quality of care, patients are encouraged to actively review and verify information included in their health records.

#### **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:** Individuals whose records contain incorrect or out-of-date information may be exposed to the risk of not receiving prescription medications, notification of appointments, or test results timely. Certain incorrect information in a patient medical record could result in improper diagnosis and treatments.

**Mitigation:** Various accuracy checks are designed and implemented in different workflows of the DHMSM EHR Core system. VHA built-in procedure requires staff verify information in patient medical records and correct information identified as incorrect during each patient's medical appointments. Staff are informed of the importance of maintaining compliance with VA Request of Information policies and procedures and the importance of remaining alert to information correction requests.

Internal processes are in place to address corrections when identified by individuals (employees) other than the Veteran through an administrative correction which is a remedial action by appropriate personnel with the authority to correct information previously captured by, or in, error regardless of who makes VHA aware of the error. Examples of items that can be handled as an administrative correction is incorrect date, association or linking data to wrong patient, or other designated clinical data items impacting the integrity of the record.

Individual patients have the right to request an amendment (correction) to their health information in VHA records if they believe it is incomplete, inaccurate, untimely, or irrelevant to their care as explained in the NOPP. The individuals must submit request in writing, specify the information that they want corrected, and provide a reason to support their request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains the patient's information or health records. Reference "Right to Request Amendment of Health Information" under VHA Notice of Privacy Practices (NOPP) (<https://www.va.gov/health/>)

## **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 User Role Assignment Standard Operating Procedure (URA SOP), version 1.5. dated December 15, 2022, developed and managed by the National User Role Access Coordinator (URAC) Lead, under the EHRM Office of Functional Champion (OFC) Deployment Manager, outlines the objectives, scope, methodology, timing and duration, tools and resources, roles and responsibilities, and procedure, to complete the conversion of user roles, including training, from the legacy EHR system (VistA) to the new one (Millennium EHR). While the Computerized Patient Record System (CPRS) in VistA, by design, has permission for each user that can be added, removed, and otherwise customized depending on the user's needs, the new EHR/Millennium uses several "roles" pre-defined by the vendor and set at the national level. Each user of the new system is assigned one or several role(s) that define their access right (authorization). The 'User Role Assignment' (URA) process is essentially to optimize the conversion of a user's legacy permission(s) to the available role(s) (equivalent to access rights) in Millennium. Once the role(s) for each user have been assigned, the local URAC(s) will follow the procedures documented in the EHRM Access Office Access Management Guide, to complete new user provisioning in Millennium. Concurrently, the local URAC(s) will monitor and ensure the user complete assigned training courses before the site go-live date.

*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?*

Beside system admins, only intended VA users can access the Training environment dedicated to VA users.

*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.*

In the context of a Pre-Prod Training environment for VA users, this Training system follows the similar user account management procedure (authorization, identification, and authentication configuration) applied to the Production EHR Core environment with limited time duration and different (Pre-Prod vs. Prod) system/environment.

**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.*

The prime contractor/implementor contracted by VA since May 2018, Oracle Health Inc., formerly Cerner Corp, is also one of the four core partners of the Leidos Partnership for Defense Health (LPDH) that was awarded the DoD MHS GENESIS contract in July 2015. Oracle Health is the developer, maintainer, deployment/implementation manager, and Federal enclave hosting facility/data center owner, of Millennium, the EHR system in the heart of the DHMSM EHR Core, the DoD system this VA EHRM Reciprocity system mirrors. On September 12, 2018 then Cerner Corp, signed a Subcontractor Business Associate Agreement (BAA) with the then Office of Electronic Health Record Modernization (OEHRM). The terms and conditions of this Subcontractor BAA reflect the terms and conditions of the BAA signed between the Veterans Health Administration (VHA), a Covered Entity-CE, and EHRM-IO, a Business Associate-BA, revised in May 2023. Accordingly, in order for the Subcontractor BA to provide the services identified in the Agreement scope, EHRM-IO as a BA will disclose PHI received from VHA, the CE, to Oracle Health, Subcontractor. Various terms and conditions governing Subcontractor's use and disclosure of the PHI owned by the CE are specified.

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

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

All eligible and authorized VA users of the system must read and acknowledge the VA general Rules of Behavior (ROB) pertaining to everyday behavior expected of Organizational Users, prior to gaining access to any VA/Federal information system or sensitive information. The rules are included as part of the annual VA Privacy and Information Security Awareness and Rules of Behavior (WBT) course, ID# 10176, which all VA network authorized users must complete via the VA's Talent Management System (TMS). After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the renew/refreshing privacy and security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system. The 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. System administrators are required to complete additional role-based training. Additionally, these users also need to complete course ID# 10203, HIPAA and Privacy training annually. The curriculum of TMS courses identified and assigned to a user by the URA process is to address different purposes other than privacy awareness & training. Depend on training objectives, additional courses may be assigned to new and existing users.

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

Yes, the DHMSM/DHA Cybersecurity division has completed an A&A for the source DHMSM Train system. As part of Reciprocity agreement between the agencies, VA won't need to repeat the A&A works. On May 27, 2023 the VA Authority Official (AO) concurred to grant Reciprocity

Authorization to Operate (ATO) for the system with the Authorization Termination Date (ATD) of September 30, 2025.

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* Dec 5, 2022
3. *The Authorization Status:* Authorized
4. *The Authorization Date:* May 27, 2023
5. *The Authorization Termination Date:* Sep 30, 2025
6. *The Risk Review Completion Date:* Jan 17, 2022
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* HIGH

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

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

N/A

## Section 9 – Technology Usage

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

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

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

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

No, the system does not use cloud technology.

### 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.

The system does not use cloud technology.

**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.*

The system does not use cloud technology.

**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.*

The system does not use cloud technology.

**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).*

The system does not utilize Robotics Process Automation.

## Section 10. References

### Summary of Privacy Controls by Family

*Summary of Privacy Controls by Family*

<b>ID</b>	<b>Privacy Controls</b>
<b>AP</b>	<b>Authority and Purpose</b>
AP-1	Authority to Collect
AP-2	Purpose Specification
<b>AR</b>	<b>Accountability, Audit, and Risk Management</b>
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
<b>DI</b>	<b>Data Quality and Integrity</b>
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
<b>DM</b>	<b>Data Minimization and Retention</b>
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
<b>IP</b>	<b>Individual Participation and Redress</b>
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
<b>SE</b>	<b>Security</b>
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
<b>TR</b>	<b>Transparency</b>
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
<b>UL</b>	<b>Use Limitation</b>

<b>ID</b>	<b>Privacy Controls</b>
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

**Signature of Responsible Officials**

**The individuals below attest that the information they provided in this Privacy Impact Assessment is true and accurate.**

---

**Privacy Officer, Angela Pluff**

---

**Information System Security Officer, Jeramy Drake**

---

**Information System Owner, Michael Hartzell**



## 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).

The current version of the VHA Notice of Privacy Practices (NOPP) can be found in the VHA webpage, <http://www.va.gov/health/>, under the “Resources” section.

## **HELPFUL LINKS:**

### **Record Control Schedules:**

<https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf>

### **General Records Schedule 1.1: Financial Management and Reporting Records (FSC):**

<https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf>

### **National Archives (Federal Records Management):**

<https://www.archives.gov/records-mgmt/grs>

### **VHA Publications:**

<https://www.va.gov/vhapublications/publications.cfm?Pub=2>

### **VA Privacy Service Privacy Hub:**

<https://dvagov.sharepoint.com/sites/OITPrivacyHub>

### **Notice of Privacy Practice (NOPP):**

[VHA Notice of Privacy Practices](#)

[VHA Handbook 1605.04: Notice of Privacy Practices](#)