Privacy Impact Assessment for the VA IT System called:

EHRM Defense Healthcare Management System Modernization (DHMSM) Test

VA Central Offices (VACO)

Electronic Health Record Modernization Integration Office (EHRM-IO)

eMASS ID #2105

Date PIA submitted for review:

October 8, 2024

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?".

The EHRM DHMSM – Test (Electronic Health Record Modernization Defense Healthcare Management System Modernization – Test) is a VA Pre-Production reciprocity (*) system mirroring the "source" DHMSM Test, dedicated to various testing functions of both existing and new capability before deployment in the Production environments. The EHRM DHMSM - Test consists of two (2) domains referred to as Mock and Cert, residing in the same Federal Enclave that hosts the Production Federal Electronic Health Record (Federal EHR) environments. Mock is used to test major/significant upgrades to primary clinical applications. Cert is used to test routine patches and minor upgrades/changes prior to their installation/deployment in the Production environments. 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, and 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.

*(*Notes: Reciprocity is an agreement between organizations to accept one another's security assessment results in order to reuse system resources or to accept each other's assessed security posture in order to share information – referenced National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 Revision 2, Dec 2018 - Risk Management Framework for Information Systems and Organizations - A System Life Cycle Approach for Security and Privacy).*

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?
The full name of this VA reciprocity system is EHRM Defense Healthcare Management System Modernization (DHMSM) Test system, EHRM DHMSM Test, which is owned by the VA Electronic Health Record Modernization Integration Office (EHRM-IO).

B. What is 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 Testing module is an integrated part of the new Federal EHR system, dedicated to various types of testing for existing and new applications before deployment in the Production environments.

C. Who is the owner 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 Test, 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. 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?

Unlike the Production systems, this Pre-production system only collects, processes and temporarily stores a limited set of patient records for testing purposes which can range from a few hundred to a few thousand medical records of Veterans and/or their beneficiaries. These records will be completely removed/deleted once the testing project is completed.

E. What is 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 the patient health records of Veterans and/or their beneficiaries with both demographic and medical care data elements. The answer to question 1.1. provides a full list of data elements potentially 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. What information sharing conducted by the IT system? A general description of the modules and subsystems, where relevant, and their functions.

This Pre-Prod Testing module only "shares" or "receives" data from the DHMSM EHR Core, also within the DHA-authorized and controlled Federal enclave. Both are considered "external" to the conventional VA IT network and system boundary.

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

3. Legal Authority and SORN

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

The legal authority to operate the system is stated in 10 U.S. Code § 1104 - Sharing of health-care resources with the Department of Veterans Affairs, as well as 38 U.S. Code § 8111 - Sharing of Department of Veterans Affairs and Department of Defense health care resources. 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 Federal Register (FR) 85, 62406, on October 2, 2020 (https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf). A biennial review of the said SORN was conducted by the VHA Privacy Office in late 2022 without any change recommended. For cross referencing purpose, the legal authority for the

source system is DoD SORN EDHA-07, Military Health Information System, published in FR 85, 36190, on June 15, 2020.

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.

4. System Changes

J. *Will 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. *Will 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 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://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: Electronic Data Interchange Personal Identifier (EDIPI) as the prime identifier and medical record number (MRN), date of death, guardian name and contact information, employment information, education information, veteran dependent information, service-connected rating and disabilities, criminal background information.
**Specify type of Certificate or License Number (e.g. Occupational, Medical, or Education.*
***Depend on the test objectives, a set of relevant data elements shall be selected to facilitate testing activities*

PII Mapping of Components (Servers/Database)

The system consists of 1 key component (servers/databases/instances/applications/software/application programming interfaces (API). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by the 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 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
N/A	N/A	N/A	N/A	N/A	N/A

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

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 testing purpose, limited data set is sourced from the Production DHMSM EHR Core system to the designated Pre-prod testing environment for various types of testing of existing and new applications.

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 testing purpose, limited data set is sourced from the Production DHMSM EHR Core system to the designated Pre-prod testing environment.

1.2c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?
No new information is created by the system.

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?
For testing purpose, limited data set is sourced/loaded from the Production DHMSM EHR Core system to a testing project container within the Pre-Prod DHMSM Test environment.

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?
Not applicable – The system is not subject to the Paperwork Reduction Act.

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 - Limited set of data is loaded to designated testing environment, depending on the test objectives. This Pre-Prod environment would be configured to mirror the Prod environments/systems being tested, including data accuracy testing capability where needed.

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 Pre-Prod system does not use commercial aggregator to check information accuracy.

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. Title 38, United States Code (U.S.C.): i) Chapter 5, § 501(b) Veterans Benefits, ii) Chapter 73, §7301(a) Veterans Health Administration – Organization and Functions, and iii) § 8111, Sharing of Department Veterans Affairs and Department of Defense Health Care Resources. The applicable VA System of Record Notice (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). The VA and DoD jointly re-signed a Memorandum of Understanding (MOU) on June 18, 2024 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 <u>PRIVACY IMPACT ASSESSMENT: Characterization of the information</u>

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

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

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

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

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

<u>Principle of Data Quality and Integrity:</u> Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?

This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

Privacy Risk: A risk may arise if patient data used in certain tests is accessed or disclosed without proper authorization.

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 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 (in Testing Cases)	External Use
Name	to identify the patient during appointments and in other forms of communication	Not used
Date of Birth	to identify age and confirm patient identity	Not used
Mother's Maiden Name	to confirm patient identity	
Personal Mailing Address	for communication, billing purposes and calculate travel pay	Not used
Personal Phone Number(s)	for communication, confirmation of appointments and conduct Telehealth appointments	Not used
Personal Email Address	for communication, including the patient portal secure communication.	Not used

PII/PHI Data Element	Internal Use (in Testing Cases)	External Use
Personal Fax Number	to send forms of communication and records to business contacts, Insurance companies and health care providers.	Not used
Emergency Contact Information	(Name, Phone Number, etc. of a different individual): used in emergent situations such as medical emergencies.	Not used
Financial Information	to calculate co-payments and VA health care benefit eligibility	Not used
Health Insurance Beneficiary Numbers/ Account Numbers	to communicate and bill third party healthcare plans	Not used
Certificate/License Numbers	For patients/individuals – Driver License, Birth Certificate, Marriage Certificate, etc. are used in various cases to verify identity, age, eligibility & benefits	Not used
Internet Protocol (IP) Address Numbers	for configuration and network connections	Not used
Race/Ethnicity	for patient demographic information and for indicators of ethnicity-related diseases	Not used
Tax Identification Number (TIN)	to verify user/patient identity and financial/taxation/eligibility status	Not used
Gender	to identify patient demographic, type of medical care/provider and medical tests required in healthcare operations	Not used
Internal Control Number (ICN)	back-up/legacy identifier for user/record verification purpose.	Not used
Military history/service connection	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	Not used
Next of Kin	in emergent cases such as medical emergencies, or in cases of patient incapacity i.e. unable to make decisions for themselves	Not used
Electronic Data Interchange Personal Identifier (EDIPI) as Medical Record Number (MRN)	the prime identifier/ medical record number to confirm/verify patient identity	Not used
Date of Death	a critical data point in healthcare and being valuable for not only the use cases noted in the U.S. Core Data for Interoperability (USCDI) but also for appropriate care coordination as well	Not used
Guardian Information	Name, contact info of the guardian(s) for use in healthcare operations when patient is unable to make decisions for themselves	Not used
Employment Information	to determine employment/benefit eligibility and for veteran contact, financial verification.	Not used

PII/PHI Data Element	Internal Use (in Testing Cases)	External Use
Education Information	patient wellness education information helps improve care quality, financial sustainability, ability to diagnose diseases, and reduce or prevent errors	Not used
Veteran Dependent Information:	to determine benefit support and as an emergency contact person	Not used
Service-connected Rating and Disabilities	to determine VA health care eligibility and treatment plans/programs	Not used
Criminal Background Information	to determine employment eligibility and during VA Police investigations	Not used
Medications	full or partial history of past and present drugs taken by a patient in different forms/ways (pills, injections, or inhalers), either over the counter or prescribed, along with notes of their effectiveness and side effects, would be helpful to diagnose, treat, cure, or prevent disease in the future	Not used
Medical Records - PAMPI	for continuity of health care, typically includes elements such as Problems, Allergies, Medications, Procedures, Immunizations (PAMPI)	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?
N/A – By design, this Pre-Prod environment does not provide data analysis capability.

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 Pre-Prod system does not create or make available new or previously unutilized information about individuals.

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?
Even though currently no SSN use case exists, this Pre-Prod system employs the same set of security and privacy controls selected and implemented for Prod environments where SSN is processed/retained. Particularly, data at rest and data in transit is safeguarded with SHA-256 (Secure Hash Algorithm 256 bit) cryptographic solutions meeting Transport Layer Security (TLS) protocol version 1.2 requirements.

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?
Minimum necessary access to PII is determined by the user's manager/supervisor (accountable individual) and using service for the purposes of performing official assigned duties. Users of the system are authorized 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?

This Pre-Prod system follows the same strict policy and procedures for user provisioning, identification & authentication, as applicable to a Production system or environment, as 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 and VHA Directive 1605.2, Minimum Necessary Standard for Access, Use, Disclosure, and Requests for Protected Health Information.

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 and processed by 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 in designated tests, then will be completely removed from the environment once the test is completed. Particularly, as listed in 1.1., the data elements temporarily retained by/in a test case could include some or all of the followings: EDIPI as prime identifier and MRN, VA ICN, name, date of birth, mother's maiden name, mailing address, phone number, fax number, email address, emergency contact information, financial account information, health insurance beneficiary numbers or account numbers, certificate/license numbers, internet protocol (IP) address numbers, medications, medical records, race/ethnicity, TIN, gender, guardian name and contact information, next of kin name and contact information, military and service history, employment information, veteran dependent information, education information, service-connected rating and disabilities, criminal background information, data of death.

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 testing, then will be completely removed from the environment once the test is completed – following VA RCS10-1 guidelines and post-validation data reset schedules.

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. Reference line item 6000.2.a.(2) – Interim Electronic Source Information.

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

For the common record owned by VA, the VA RCS10-1 (https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf) schedule is applied. However, DoD record retention schedule(s) and disposition procedure will be applied to the records that DoD controls and deems having its ownership on them. Reference line item 6000.2.a.(2) – Interim Electronic Source Information.

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/DoD procedures will be followed to delete/eliminate the common records in the system once testing is completed and applicable RCS 10-1 record retention requirements are met.

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.

This Pre-Prod system does not use PII for research or training. The system is designed for the sole purpose of testing. Users must comply with awareness and training requirements as if it were a Prod system. Additionally, same sets of Prod system access control, personnel security, and auditing have been implemented.

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 Federal agency partners of the Federal EHR. Further complication may arise when different standards applied to different partners co-exist for the same type of data or share records. Records held longer than required are at greater risk of being inappropriately released or breached.

Mitigation: By consistently reviewing, validating/accounting for all types of VA owned data/records housed in the source systems, then executing data syndication workflows/techniques to syndicate those data types/records back to the legacy VA systems such as Corporate Data Warehouse (CDW), one of the potential risk of data loss can be addressed. However, to completely remove/purge the VA owned data out of this DoD system once it reaches its designated data retention time, more inter-agency workflows, effective joint-operation taskforce, may need to be employed.

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***
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: The source system, DHMSM Test, is outside of VA system boundary and does not introduce any "systematic" privacy risk associated with the sharing of information within VA/VHA.

Mitigation: No mitigation is required since no systematic privacy risk exists.

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***

Defense Health Agency (DHA)/ DHMSM EHR Core	Data testing/ validation	EDIPI/MRN, ICN, name, date of birth, mother's maiden name, mailing address, phone number, fax number, email address, emergency contact information, financial account information, health insurance beneficiary numbers or account numbers, certificate/license numbers, internet protocol (IP) address numbers, medications, medical records, race/ethnicity, TIN, gender, guardian information, next of kin information, military and service history, employment information, veteran dependent information, education information, service-connected rating and disabilities, criminal background information, date of death	MOU between DoD and VA for Sharing of Personal Information, 6/18/2024; SORN 24VA10A7, Patient Medical Records-VA, 10/02/2020	Medical Community of Interest (Med-COI) Secure File Transfer Protocol (SFTP) Hypertext transfer protocol secure (HTTPS) Transmission Control Protocol/Internet Protocol (TCP/IP)

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: VA patient data is now collected and retained in a shared database as part of the Federal EHR and may be exposed to certain privacy/security risks, even in the context of a Pre-Prod environment, such as unauthorized access or being used for purposes other than the purpose(s) stated at original collection time.

Mitigation: Beside the MOU for Sharing Personal Information recently revised and signed in June 2024 between DoD and VA, the two agencies have entered into several inter-agency MOA, MOU/ISA, in line with the 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 Pre-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, besides the SORN publications 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 is provided to Veteran upon enrollment and a revised/latest NOPP mailed to eligible veterans every 3 years by the VHA. A copy of the NOPP must be provided to non-Veteran/humanitarian patients in person when they present for services.

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

A notice specific for this system is not provided as the collection of data occurs under the EHR Core system and therefore this requirement has been met as specified under that system. For the EHR Core system, 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.

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.

Notification is provided for the system that directly collects information from individuals, which is the EHR Core system. The Notice of Privacy Practice (NOPP) is a document which explains the collection and use of protected information to individuals applying for VHA benefits. The NOPP (Appendix A) is provided when the Veteran enrolls or when updates are made to the NOPP, copies are mailed to all VHA beneficiaries (every 3 years). Employees and contractors are required to review, sign and abide by the National Rules of Behavior on an annual basis, that outlines the requirements and expectations for appropriate use of Veteran PHI/PII maintained in VA systems. In addition to NOPP distributions are the SORN publications in the Federal Register in October 2020 as mentioned in 1.5.

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

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

Yes, as outlined in the NOPP for the EHR Core system. The individuals do have an opportunity to decline to provide information at any time. However, 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/ or at this link 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, as outlined in the NOPP for the EHR Core system. Specifically, Right to Request Restriction: Veterans/patients do have the right to request that VHA not use or disclose all or part of their health information to carry out treatment, payment or health care operations, or that VHA not use or disclose all or part of their health information with individuals such as their relatives or friends involved in their care, including use or disclosure for a particular purpose or to a particular person. Reference the NOPP on how to submit a request for restriction. VHA, however, as a "Covered Entity" under the law, is not required to agree to such restriction, except in the case of a disclosure restricted under 45 CFR § 164.522(a)(1) (vi). This provision applies only if the disclosure of the Veteran's or patient's health information is to a health plan for the purpose of payment or health care operations and the Veteran's health information pertains solely to a health care service or visit which is paid out of pocket in full by the Veteran/patient. However, VHA is not legally able to accept an

out-of-pocket payment from a Veteran for the full cost of a health care service or visit. The Administration can only accept payment from a Veteran for co-payments. Therefore, this provision does not apply to VHA and VHA is not required or able to agree to a restriction on the disclosure of a Veteran's/patient's health information to a health plan for the purpose of receiving payment for health care services provided by VHA. Additionally, VHA is not able to restrict access to the patient health information by DoD providers with whom the patient has a treatment relationship. Lastly, Individuals have the right to consent to the use of their information. Individuals are directed to use the 10-5345 Release of Information (ROI) form describing what information is to be sent out and to whom it is being sent to. Patients have the right to opt-out of VA facility directories. Individuals can request further limitations on other disclosures. A veteran, guardian or court appointed Power of Attorney can submit a request to the facility Privacy Officer to obtain information.

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://department.va.gov/privacy/system-of-records-notices/ *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.***

This is not applicable to the data in the Test system as it is a copy of a limited data set of the data collected, accessed, used, maintained and stored in the EHR Core System. Individuals requesting to gain access to this information would request access to the original data maintained in the EHR Core system and would follow the procedures outlined in this section of the PIA for the EHR Core system.

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 but is a copy of a limited data set of the original records covered under the Privacy Act SORN and therefore not considered the final legal health record. As a result, request for access to the information would be for the data collected in the EHR Core system.

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.

This is not applicable to the Test system as it is a copy of a limited data set of the data directly collected, accessed, used, maintained, and stored in the EHR Core system. The procedures for correcting inaccurate or erroneous information are as specified under this section of the PIA for the EHR Core System. (To re-state here for EHR Core System: Right to Request Amendment of Health Information: Veterans/patients have the right to request an amendment (correction) of their health information in the Federal EHR system records if they believe it is incomplete, inaccurate, untimely, or irrelevant 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. A decision to approve or deny is made by the practitioner who entered the data and relayed to the Veteran in writing by the facility Privacy Officer. Appeal rights are provided if a request is denied. The goal is to complete any evaluation and determination within 30 business days. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned system of records, and the facility Privacy Officer, or designee, to be date stamped; and is filed appropriately.

In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579. That is, VA must maintain in its records only such information about an individual that is accurate, complete, timely, relevant, and necessary. Lastly, individuals have the right to review and change their contact or demographic information at time of appointment or upon arrival to the VA facility and/or submit a change of address request form to the facility business office for processing).

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.

This is not applicable to the EHRM DHMSM Test system as it is a copy of a limited data set of data directly collected, accessed, used, maintained and stored in the EHR Core system. The procedures for notifying individuals of how they can correct their information are specified under this section of the PIA for the EHR Core system. To re-state here, 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 during enrollment and every three years thereafter. If they enroll in the patient portal, a digital version of the NOPP is also available for their awareness. 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/). Publications of the SORNs referenced in 1.5 are also a means of notification. Lastly, individuals are provided written notice of the amendment process in the written amendment acknowledgement and response letters.

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

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

The processes outlined in 7.2 and 7.3 are considered formal redress procedures for the data in the EHR Core system from which the information from this system is collected and used. To ensure data accuracy and maintain quality of care, patients are encouraged to actively review and verify information included in their health records. Veterans or other VAMC patients who are enrolled in MyHealthevet can use the system to make direct edits to their personal health record.

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: DMSM Test collects/processes copy of a limited data set of the EHR Core system; any risks associated with incorrect information would be associated with the live data in the EHR Core system.

Mitigation: – Mitigation efforts would default to the EHR Core system where the live data is stored.

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 workflow to request and manage access to the Pre-Prod Test system is similar to the one used for the Prod systems, as having been defined in the User Role Assignment Standard Operating Procedure (URA SOP), version 1.5 dated December 15, 2022, developed and managed by the EHRM Office of Functional Champion (OFC) Deployment Manager. Access to the VA EHRM program is restricted to VA employees and contractors who must complete both the VA Privacy and HIPAA Focused and Information Security training courses. Specified access is granted based on the employee/contractor functional category authorizing them to access information on a need-to-know basis based on least privilege and minimum necessary standards approved by supervisors.

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 administrators, only authorized VA users can access designated testing environments.

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 environment for VA users, the system follows the same user account management procedure applied to the Production environment. Nearly 400 VA positions have been mapped to predefined roles in the Oracle Millennium system platform. Each of those "Oracle roles" determines the level of access a user has in the patient's medical record. Each user needs to be assigned at least a primary role and an optional secondary role. The Oracle roles for the VA enterprise have been defined at national level in national workshops organized by relevant VA national councils and based on workflows.

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, 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 hosting facility/data center owner, of the Federal EHR system. The Subcontractor Business Associate Agreement originally signed on Sep 12, 2018, between Oracle Health Inc., then Cerner Corp, and EHRM-IO, has been revised and signed in July 2023, in accordance with the guidance provided by the VHA Directive 1605.5, Business Associate Agreements dated Nov 17, 2020.

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 Federal EHR 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 since they will have direct access to PHI in the Millennium system in particular, and the Federal EHR system in general. The curriculum of TMS courses identified and assigned to a user by the User Role Assignment (URA) process is to address different purposes other than privacy awareness & training.

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:* December 7, 2022
3. *The Authorization Status:* Authorization to Operate (ATO)
4. *The Authorization Date:* May 27, 2023
5. *The Authorization Termination Date:* September 30, 2025
6. *The Risk Review Completion Date:* May 1, 2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* HIGH

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

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

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.

ANGELA PLUFF

Digitally signed by ANGELA PLUFF
Date: 2024.10.24 08:40:53 -04'00'

Privacy Officer, Angela Pluff

JERAMY DRAKE

Digitally signed by JERAMY DRAKE
Date: 2024.10.23 10:51:43 -07'00'

Information System Security Officer, Jeramy Drake

MICHAEL HARTZELL

Digitally signed by MICHAEL HARTZELL
Date: 2024.10.24 07:51:11 -04'00'

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; screen shot of a website collection privacy notice).

In the http://www.va.gov/health/ webpage, the current PDF copy of the "VA Privacy Practices" is listed in the "Resources" section on the right.

SORN 24VA10A7, Patient Medical Records-VA: https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

HELPFUL LINKS:

Record Control Schedule
https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

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

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

VA Privacy Service Portal:
https://department.va.gov/privacy/

Notice of VA/VHA Privacy Practice
In the http://www.va.gov/health/ webpage, the current PDF copy of the "VA Privacy Practices" is listed in the "Resources" section on the right.