Privacy Impact Assessment for the VA IT System called:

Electronic Health Record Modernization (EHRM) Defense Healthcare Management System Modernization (DHMSM) Electronic Health Record (EHR) Core

VA Central Offices (VACO)

Electronic Health Record Modernization Integration Office (EHRM-IO)

Date PIA submitted for review:

September 15, 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 (EHRM) Defense Healthcare Management System Modernization Electronic Health Record Core, EHRM DHMSM EHR Core, is a VA reciprocity system mirroring the DHMSM EHR Core, comprising the widely used state-of-market Millennium EHR platform developed, maintained, managed, and hosted by Oracle Health, formerly Cerner Corporation. The DHMSM 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) Electronic Health Record Core, EHRM DHMSM EHR Core, which is owned by the VA 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.

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 EHR Core, including the Millennium platform, 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.

This is a mission-critical system collects, processes, and distributes EHR longitudinally across the Military Health System (MHS), VA, TRICARE, and Veterans Health Administration (VHA) network of service providers, Federal, and State agencies for approximately 9.6 million DoD beneficiaries and 9.11 million VA healthcare enrollees, worldwide.

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

The system contains a consolidated health record for patients (Military Service Members, Veterans and beneficiaries) and includes 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.

All information sharing activities take place in the source DoD system, not the VA reciprocity one, as more details are provided in both section 4, Internal sharing/receiving, and section 5, External sharing/receiving and disclosures. However, the VA EHRM Reciprocity system has received from the DHMSM/DHA four out of five Risk Management Framework (RMF) core documents as defined by the Committee on National Security System Instruction CNSSI 1254, August 2016, which includes the System Security Plan (SSP), the Security Assessment Report (SAR), the Plan of Action and Milestones (POA&M), and the DHA Authority to Operate (ATO) Decision Memo, dated Feb 25, 2022. The VA Reciprocity mirrors the information and system security categorization High impact level, in accordance with DoDI 8510.01, RMF for DoD Systems, dated July 17, 2022, and the Memorandum of Understanding between DoD and VA for Authority to Operate (ATO) Reciprocity, referencing NIST SP 800-37 and NIST SP 800-53, dated Jan 24, 2018. Such reciprocity will enable secure interoperability and information sharing and help to ensure a seamless experience for our military service members as they transition from active duty to veteran status.

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.

Millennium EHR, the heart of DHMSM EHR Core, is a suite of several systems ancillary to the EHR, centrally resides in the DHA-authorized Federal enclave inside Oracle Health data center in Kansas City, MO, and concurrently runs in more than 100 parent DoD Military Treatment Facilities (MTFs), five (5) VA Medical Centers (VAMC's), and more than 100 USCG sites. As of the end of fiscal year 2023, five (5) VHA local facilities/sites have completed their conversion from VistA to the new EHR system. These facilities are the Mann-Grandstaff VAMC (Spokane, Washington State-WA), the Jonathan M. Wainwright Memorial VAMC (Walla Walla, WA), the Central Ohio VA Health Care system (Columbus-OH), the White City, Oregon (OR) VAMC, and the Roseburg OR VAMC. The same set of NIST SP 800-53 Rev.4 security and privacy controls in place with the DHMSM EHR Core are deployed with the VA reciprocity system. The DHA

Medical Community of Interest (Med-COI) network is deployed to safeguard and continuously monitor data traffic interfacing with both the Federal enclave and all the DoD and VA sites where the Federal EHR system is deployed. Both DoD and VA have adopted and implemented the Risk Management Framework (RMF) as recommended by NIST SP 800-37 Rev. 2, RMF for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, December 2018, and outlined in their respective Agency policies, DoD Instruction 8510.01, Risk Management Framework for DoD Systems, July 19, 2022, and VA Directive 6500, VA Cybersecurity Program, February 24, 2021.

3. Legal Authority and SORN

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

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. The legal authority to collect data pursuant to the Privacy Act of 1974 is stated in both VA SORN 24VA10A7, Patient Medical Records-VA, published in FR Vol. 85, No. 192, on October 2, 2020, and SORN 114VA10 – The Revenue Program – Billing and Collections Records-VA, published in FR Vol.86, No. 14, on Jan 25, 2021. A biennial review of the SORN's was conducted by the VHA Privacy Office in 2022 without any change recommended. For cross-reference purposes, the applicable DoD SORN is EDHA-07, Military Health Information System, published in Federal Register (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 necessary following the decision made by the VA AO on March 23, 2023, concurring an Authorization to Operate (ATO) under reciprocity with [the] Defense Health Agency (DHA) [AO] with corresponding Authorization Termination Date (ATD) of March 23, 2025.

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

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

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

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

- ☒ Name
- ☒ Social Security Number
- ☒ Date of Birth
- ☒ Mother's Maiden Name
- ☒ Personal Mailing Address
- ☒ Personal Phone Number(s)
- ☒ Personal Fax Number
- ☒ Personal Email Address
- ☒ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☒ Financial Information
- ☒ Health Insurance Beneficiary Numbers Account numbers
- ☒ Certificate/License numbers* (Occupational, Medical and Education)
- ☐ 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)

Additional data elements included in the DHMSM EHR Core system: DoD Electronic Data Interchange Personal Identifier (EDIPI), Death certification information to include Date of Death, Guardian name and contact information, Employment Information, Veteran Dependent Information, Service-connected rating and disabilities, Criminal background information, medical record elements including PAMPI- Problems, Allergies, Medications, Procedures, Immunizations

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

PII Mapping of Components (Servers/Database)

The EHRM DHMSM EHR Core system consists of 5 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
Millennium (including 724 Downtime Viewer Mid-Tier, VitalsLink, TrackCore, Bridge Medical, AudBase)	Yes	Yes	EDIPI, ICN, SSN, name, 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, internet protocol (IP) address numbers, medications, medical records, race/ethnicity, tax identification number, gender, military history/service connection, next-of-kin, death certificate information, guardian name and contact information, employment information, veteran dependent information, service-connected rating and disabilities, criminal background information.	Treatment, Payment, Health care operations and administration	Security Hash Algorithm (SHA-256), Transport Layer Security (TLS), virtual private network (VPN) tunnel

(VA) Data Syndication	Yes	Yes	EDIPI, ICN, SSN, date of birth, mother's maiden name, mailing address, zip code, phone number(s), 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, race/ethnicity, gender, guardian name and contact information, next of kin, death certificate information, military history and service connection, employment information, veteran dependent information, education information, service-connected rating and disabilities, criminal background information, medications, medical records (PAMPI)	Health care operations and administration	Security Hash Algorithm (SHA-256), TLS, VPN tunnel
3M 360 Encompass (360e)	Yes	Yes	EDIPI, name, date of birth, race/ethnicity, date of death, gender, financial information, medical records	Revenue cycle solution to process, enrich, and enhance medical coder productivity in health information management	HyperText Transfer Protocol Secure (HTTPS) TLS
Clairvia	Yes	Yes	Name, date of birth, EDIPI, ICN, mailing address, phone number(s), email address, Personal Identity Verification (PIV) card number, user credentials. Patient demographic (Name, Birth Date, Gender	Clinical care operations & administration/ facility-wide planning; workforce scheduling, forecasting	HTTPS TLS

			Patient medical record (medications, lab value, admission, discharge, transfer)	care resource supply & demand, care team device assignment	

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?

A majority of the information is collected or created directly from the patients and inputted by individual users and clinical staff. For example: items such as name, social security number, date of birth, mailing address, personal phone number, etc. are collected from the patient on healthcare enrollment forms, such as VA Form 10-10EZR – Health Benefits Update Form, as part of healthcare business operations. Military service member information, such as dates of service, branch of service, type of discharge is collected by the DoD with cross-verification performed by the Veterans Benefits Administration (VBA). In the case of a Veteran with a disability directly connected to their military service, the VBA may also provide service-connected disability ratings and information related to applicable disabilities (date granted, type of disability, overall percentage of combined disabilities). In cases where a Veteran has applied for a service-connected disability, but has not applied for VHA healthcare benefits, VBA will provide patient's profile to facilitate the Compensation and Pension exam. Information can also be collected electronically from individuals/patients through their secure account in the patient portal. During the period of transitioning from the legacy EHR system, the Veterans Information Systems and Technology Architecture (VistA), to the Federal EHR or (Oracle Health/Cerner) Millennium, EHRM-IO has designed and deployed a data migration management program to continuously i) migrate data extracted from the VistA instance of approximately 130 VA health care facilities locations/sites (VX130) into both the Corporate Data Warehouse (CDW) system and the HealtheIntent data platform (locates in the EHRM DHMSM High Assurance Clinical Application Service (HA/CAS) Production Reciprocity ATO package), and ii) syndicate data from the Federal EHR system (Millennium) generated from health care activities taken place at the five (5) VA health care facilities/sites already completed their conversion from VistA to the new EHR system, back to the VA/VHA legacy systems outside the Federal enclave.

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.

Beside sourcing information directly from individuals/patients, the Federal EHR system collects information from other sources such as VX130 by means of data migration as mentioned in 1.2 above, to ensure continual healthcare operations, management, interoperability.

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

The Millennium EHR platform is considered the authoritative source of clinical data of the Federal EHR 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?

Information is collected both directly from individuals via VA Form 10-10EZR – Health Benefits Update Form, and electronically from other sources such as by means of the data migration process.
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.

The current VA Form 10-10EZR is registered under OMB Control Number 2900-0091, expires on June 30, 2024. (https://www.va.gov/vaforms/medical/pdf/VA%20Form%2010-10EZR.pdf)

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.

Information obtained directly from the patient is assumed to be accurate. Information may be verified with other Federal agencies (DOD, SSA and IRS) to confirm eligibility or benefits. Should conflicting information exists, it will be documented and verified prior to further use. Furthermore, individuals have the right to obtain access to their records and request correction to them when necessary (see Section 7 for additional information). Patient demographics as well as income verification matching are completed by automated tools. Practitioners review and sign all treatment information and Business Office/Health Information Management Service (HIMS) reviews data obtained and assists with corrections.

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.

The system does not use commercial aggregator for data accuracy verification purpose.

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 two applicable (2) VA System of Record Notices are i) SORN 24VA10A7, Patient Medical Records-VA, published in FR Vol. 85, , on October 2, 2020 (https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf), and ii) SORN 114VA10 – The Revenue Program – Billing and Collections Records-VA, published on Jan 25, 2021 (https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01541.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. To perform their respective missions, including processing of claims and delivery of benefits, each Department needs timely access to PII/PHI held by the other Department. On October 9, 2019, the VA Deputy General Counsel for General Law (02GL) issued an Opinion Memorandum, addressing the VA Assistant Deputy Under Secretary for Health Informatics (10A7), on the subject of "Cerner VA/DoD Common Record". The answer to Question A states that, VA and DoD may "own a single, electronic instance of the 'common record' in Cerner Millennium under the Privacy Act" because the two departments may simultaneously own, have jurisdiction of, and exercise control over identical data. In compliance with the Federal Information Security Modernization Act of 2014, Pub. L. 113-283, aka FISMA Reform, the system must receive a security authorization to operate, or an ATO, given by a senior VA authority official or an AO. In this management decision, acting on behalf of the VA, the AO would explicitly accept the risk to agency operations including mission, functions, image, or reputation, agency assets, individuals, etc. based on the implementation of an agreed-upon set of security and privacy controls defined by Directive 6500, VA Cybersecurity Program. Question C of the afore-mentioned Oct 9,2019 Opinion Memorandum has led to the publication of SORN 24VA10A7 (to replace the old SORN 24VA10P2) on October 2, 2020, in the Federal Register Vol. 85, No. 192.

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 an unauthorized individual 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 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
- Social Security Number: In case the prime identifier is not available, this element is used as a historical patient identifier and as a resource for verifying income information with the Social Security Administration
- 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 MyHealtheVet 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 part 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.
- Tax Identification Number: used for user identification and financial/taxation transaction verification purposes.
- 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.
- Death Certificate Information: used to determine date, location, and cause 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.
- Veteran Dependent Information: used to determine benefit support and as an emergency contact person.
- 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.

Authorized users of the system can use Discern Reporting Portal for statistics and analysis purposes to create many types of general reports that provide a better understanding of patient care and needs. These reports are used by the staff and management to identify, track and trend performance in a variety of areas including access, patient satisfaction, financial indicators, and many others. Patient and employee data are analyzed on an as-needed basis with tools relevant to the task at hand upon official authorization. This data is never placed into the record of any patient, but is often saved as part of staff performance such as: the number of patients enrolled, provider capacity, staffing ratios, new primary care patient wait-times, etc. for Veterans established with a Patient Care Aligned Team (PACT), beneficiary travel summary/benefits, workload and cost resources for various services, i.e., mental health, primary care, home dialysis, fee services, etc., daily bed management activity, coding averages for outpatient/inpatient encounters, satisfaction of healthcare experience of patients (SHEP) data as it pertains to customer satisfaction regarding outpatient/inpatient services, unique patient trends, clinic wait times, etc.

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.

Clinicians and some administrative staff can add new episodes of care/encounters to an existing record of a patient or create a new patient record. In general, access to the newly created patient record, or to an existing record, is granted based on the need-to-know principle for treatment, payment and healthcare operations.

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?

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 the need-to-know basis, commensurate to their user role in the system.

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

The system follows a strict user provisioning, identification and authentication process, 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. It's also captured in the Privacy managed Functional Categories process and verified filed in the employee's personnel files annually per 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.

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

Access to system functions, including to patient PII/PHI are monitored by P2 Sentinel, an auditing tool used for privacy and compliance monitoring.

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

1. Medical record folder or Consolidated Health Record (CHR): contains all professional and administrative material necessary to document the episodes of medical care and benefits provided to individuals by the VA health care system; 2. Financial information; 3. System generated information. Information collected as listed in 1.1 that us retained by the system includes the following: 1) Name 2) Social Security Number 3) Date of Birth 4) Mother's Maiden Name 5) Mailing Address 6) Phone Number(s) 7) Fax Number 8) Email Address 9) Emergency Contact Information 9) Financial Information 10) Health Insurance Beneficiary Numbers/Account Numbers 11) Certificate/License numbers 12) Vehicle License Plate Number 13) Internet Protocol (IP) Address Numbers 14) Medications 15) Medical Records 16) Race/Ethnicity 17) Tax Identification Number 18) Gender 19) Integration Control Number (ICN) 20) Guardian name and contact information 21) Military and service history/connection 22) Next of Kin 23) EDIPI 24) Death Certificate Information 25) Employment information 26) Veteran dependent information 27) Education information 28) Medical statistics for research purposes containing PII/PHI. 29) Employment Information 30) Veteran Dependent Information 31) Service-connected Rating and Disabilities 32) Criminal Background Information

3.2 How long is information retained?

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

Medical records: since the system collects and stores both DoD and VA records, the longer retention period will be applied where there's a difference in record retention policy between the agencies. VA/VHA adheres to the VA/VHA Record Control Schedule RCS 10-1, https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf, item number 6000.2b. Accordingly, VHA patient medical records are retained for a total of 75 years after the last episode of care. Meanwhile, DoD/DHA record retention policy requires to keep the data for 100 years after the last episode of care; Financial records and IT system records: retention time varies between 1-7 years depending on the type/category of records as detailed in RCS10-1.

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.In addition, for the VHA records, the core system operates using two NARA approved retention schedules: Department of Veterans Affairs, VHA Records Control Schedule 10-1 January 2019 https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf• Department of Veterans Affairs, Office of Information & Technology Record Control Schedule 005-1 (August 3, 2009) https://www.oprm.va.gov/docs/RCS005-1-OIT-8-21-09.pdf

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

For the common record owned by VA, the VA RCS 10-1 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.

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 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. For VA controlled records, once the information retention period is met, Records Management and OIT will develop a plan for destruction per VA requirements in accordance with VA Directive 6371 Destruction of Temporary Paper Records, VA Directive 6500 VA Cybersecurity Program and VA Handbook 6500.1, Electronic Media Sanitization.

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 source DoD system does not use PII for research, testing or training. These purposes of use are carried out by other Prod or Pre-Prod ATO packages in the Federal enclave that specialize on testing, or training. PII can be used in research studies approved by the VA Institutional Review Board (IRB).

Certain types of testing maybe conducted for new or modified applications or information systems prior to deployment. The usage of PII/PHI in those tests, if any, must comply with the Federal Regulations listed below.

- 38 U.S.C. 5702 -researcher(s) must submit a written request to the Record Management officer in charge, stating purpose and duration of using the records for
- 38 U.S.C. 5701 applicable to names and addresses
- 38 U.S.C. 7332, applicable to Drug Abuse, alcohol Abuse, HIV Infection, and Sickle Cell Anemia Records; HIPAA Privacy Rule; Privacy Act of 1974, and
- 38 CFR 1.488 - Reseach activities - subject to the provisions of 38 U.S.C. 5701, 38 CFR 1.500–1.527, the Privacy Act (5 U.S.C. 552a), 38 CFR 1.575–1.584 and the following paragraphs, patient medical record information covered by §§ 1.460 through 1.499 of this part may be disclosed for the purpose of conducting scientific research.

As part of health care operations, VHA may need to train staff on functionality of new/modified IT systems. If PII is used in training materials, applicable VA/VHA directives must be followed.

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. Records held longer than required are at greater risk of being inappropriately released or breached.

Mitigation: By consistently reviewing and 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 risks 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 and an 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***
Veterans Health Administration (VHA) • Clinical Imaging/Radiology – Central VistA Image Exchange (CVIX) • Ambulatory • Behavioral Health • Advanced Care & Ancillaries • Logistics & Supply Chain • Laboratory • Telehealth (Video Visit) • Dental • Pharmacy • Community Care • Revenue Cycle Management • Case Management	Clinical Care, Health care operations and management	EDIPI, ICN, SSN, name, 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, internet protocol (IP) address numbers, medications, medical records, race/ethnicity, tax identification number, gender, military history/service connection, next-of-kin, death certificate information, guardian name and contact information, employment information, veteran dependent information, service-connected rating and disabilities, criminal background information.	Medical Community of Interest (Med-COI) network Health Level (HL) 7 - OPENLink or Orion Rhapsody Secure file transfer protocol (SFTP) Hypertext transfer protocol secure (HTTPS) Transmission Control Protocol/Internet Protocol (TCP/IP)
Veterans Benefits Administration (VBA) • Veterans Benefit Management System (VBMS) • Eligibility	Eligibility verification, claims & benefits processing	EDIPI, ICN, SSN, name, 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, internet protocol (IP)	Med-COI HL7 HTTPS

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*
		address numbers, medications, medical records, race/ethnicity, tax identification number, gender, military history/service connection, next-of-kin, death certificate information, guardian name and contact information, employment information, veteran dependent information, service-connected rating and disabilities, criminal background information.	
Office of Information & Technology (OI&T) • Identity & Access Management • VA data centers • VA Enterprise Cloud (VAEC) • Data Access Service (DAS) • Veterans Data Integration and Federation Enterprise Platform (VDIF-EP) • Workforce & Operations	Clinical Care, Health care operations and management	EDIPI, ICN, SSN, name, 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, internet protocol (IP) address numbers, medications, medical records, race/ethnicity, tax identification number, gender, military history/service connection, next-of-kin, death certificate information, guardian name and contact information, employment information, veteran dependent information, service-connected rating and disabilities, criminal background information.	Med-COI HL7 SFTP TCP IP HTTPS
Electronic Health Record Modernization Integration Office	Clinical Care, Health care operations	EDIPI, ICN, SSN, name, date of birth, mother's maiden name, personal mailing address, personal	Med-COI HL7 SFTP

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*
(EHRM-IO) •EHRM High Assurance Clinical Application Service (HA-CAS) • Forward Deployed Service Set (FDSS) • EHRM Skyvue • Multi-Purpose Clinical Platform (M-PCP) • EHRM Audiology • EHRM iAccess Kiosk • EHRM Tracking Board Kiosk • EHRM HemaTrak Blood Label Printing Service	and management	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, internet protocol (IP) address numbers, medications, medical records, race/ethnicity, tax identification number, gender, military history/service connection, next-of-kin, death certificate information, guardian name and contact information, employment information, veteran dependent information, service-connected rating and disabilities, criminal background information.	TCP IP HTTPS

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 DHMSM EHR Core is not considered locating within the conventional VA system boundary and does not introduce any "systematic" privacy risk associated with the sharing of information within VA/VHA.

Mitigation: N/A

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.
This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

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

Department of Defense (DoD) • DoD Dependent Eligibility & Enrollment Reporting System (DEERS) • Clinical (or Health) Data Repository (CHDR) • Patient Engagement	Sharing health care resources in supporting of clinical care, health care operations and management	Patient ID (EDIPI, SSN) demographics, eligibility, Other Health Insurance (OHI), user credentials, PAMPI - Problems, Allergies, Medications, Procedures, Immunizations	38 U.S. Code § 8111 - Sharing of VA & DoD health care resources; DoD & VA MOU on Sharing of PII, March 13, 2014	Med-COI HL-7 SFTP TCP IP HTTPS
Oracle Health (formerly Cerner Government Services) Clinical Application Service – Value Added Network CAS/VAN • Interfacing State Immunization Registries via CAS/VAN	Treatment, payment, Healthcare operations & management, immunization querying & reporting	Patient ID (EDIPI, SSN) demographics, eligibility, Other Health Insurance (OHI), user credentials, PAMPI - Problems, Allergies, Medications, Procedures, Immunizations (includes Unsolicited Update to Vaccination Record – VXU)	Sub-contractor Business Associate Agreement (Oracle Cerner - EHRM-IO) Jul 11, 2023	HL-7 SFTP TCP IP HTTPS

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: Patient medical records may be exposed to certain privacy/security risks such as unauthorized disclosure, unauthorized access or being used for purposes other than the purpose(s) stated at original collection time.

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 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. Mitigation by means of security and privacy controls such as access controls, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information integrity, security assessment and authorization, incident response, risk assessment, planning and maintenance, accountability, audit and risk management, data quality and integrity, data minimization and retention, individual participation and redress, transparency and use limitation. Criteria, procedures, controls, and responsibilities regarding access are well documented as part of the system ATO process in accordance with NIST SP 800-53 Rev 4 and VA Handbook 6500 – Risk Management Framework for VA Information Systems – VA Information Security Program. Standing letters for information exchange, business associate agreements and memorandums of understanding between agencies and VA are managed and monitored closely by the VA Office of Information Security (OIS), VHA Privacy Office and VHA Health Care Security (HCS) to ensure protection of information.

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.

Besides the SORN publications in the Federal Register in October 2020 and January 2021 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 a 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.

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.

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 above.

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

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

Yes, individuals 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 10-10EZR – Health Benefits Update Form. 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 10-10EZR 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%20Form%2010-10EZR.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.

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: There is a risk that 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 NOPP when Veterans apply for benefits and every three years thereafter to include any changes made to the notice. Additionally, NOPPs are provided to non-Veteran beneficiaries at each episode of care and periodic monitoring is performed to check that the signed NOPP acknowledgment form has been scanned into the beneficiaries' electronic health record. Additional mitigation is provided by making the System of Record Notices (SORNs) and PIA available for review online, as discussed in question 6.1 and the Overview section of this PIA.

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, MyHealtheVet, 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. 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 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.

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 process. To ensure data accuracy and maintain quality of care, patients are encouraged to actively review and verify information included in their health records. veteran or other VAMC patient who is enrolled in MyHealthevet can use the system to make direct edits to 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.
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 unrelated to your care. 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.

Access to the of Cerner Millennium roles is determined by the user's manager/supervisor (accountable individual) and the Using Service for the purposes of performing official assigned duties. 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). Access to the applicable EHR/Millennium roles is determined by the user's manager/supervisor (accountable individual) and the Using Service for the purposes of performing official assigned duties. 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. Access to the VA OEHRM program is restricted to VA employees and contractors who must complete both the Privacy and HIPAA Focused and Information Security training. 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?

With Millennium EHR at its heart, the DHMSM EHR Core system along with ancillary applications, solutions, and platforms, collectively referred to as the Federal EHR system, is currently accessed by

more than 160,000 authorized DoD, VA, and U.S. Coast Guard users such as doctors and nurses, according to data presented on the Federal EHRM Program Office website, www.FEHRM.gov.

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.

Nearly 400 VA positions have been mapped to predefined roles in the Oracle Millennium product. Each of those "Oracle roles" determines what 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 were defined at national level in the National Workshops by the National Councils and based on workflows. As having outlined in the methodology section of the URA SOP, ver. 1.5 document stated in section 8.1a, a secure URA library and URA list are created and stored on the site-specific page under the EHRM Facilities Implementation Center (EFIC) SharePoint workspace. The assigned local URAC in collaboration with URA Subject Matter Experts (SMEs) is ultimately responsible for those critical artifacts, particularly to ensure the integrity of the single source of truth URA list.

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.

Yes. The prime contractor/implementor contracted by VA since May 2018, Oracle Health Government Services, Inc., formerly Cerner Government Services, Inc., 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. The Subcontractor Business Associate Agreement (BAA) between EHRM-IO and CGS, originally signed on Sept 12, 2018, has been revised and fully signed on July 11, 2023. The terms and conditions of this Subcontractor BAA reflect the BAA revised and signed in May 2023 between the Veterans Health Administration (VHA), a Covered Entity-CE, and EHRM-IO, a Business Associate-BA. Contractor staff personnel who provide support to the Federal EHR system are required to complete annual VA Privacy and Information Security and Rules of behavior training via the VA Talent Management System (TMS). All contractors are vetted using the VA background investigation process and must obtain the appropriate level background investigation for their role. Contractors with systems administrative access are required to complete additional role-based training prior to gaining system administrator access. Generally, contracts are reviewed at the start of the initiation phase of acquisitions and again during procurement of option years by the

Contracting Officer, Information Security Officer, Privacy Officer, COR, Procurement Requestor/Program Manager and any other stakeholders required for approval of the acquisition. Contracts generally have an average duration of 1-3 years and may have option years stipulated in the original contract.

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 DHMSM EHR Core, specifically the Millennium EHR system, as having described in 8.1a, must read and acknowledge the VA National Rules of Behavior (ROB) or VA Contractor's 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 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?

Yes, A&A has been completed for the system.

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* June 13, 2022
3. *The Authorization Status:* VA AO concurred an Authorization to Operate (ATO) under Reciprocity with the DHA AO
4. *The Authorization Date:* March 23, 2023
5. *The Authorization Termination Date:* March 23, 2025
6. *The Risk Review Completion Date:* March 14, 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**

ID	Privacy Controls
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 M. PLUFF 143002

Digitally signed by ANGELA M. PLUFF 143002
Date: 2023.09.21 15:32:32 -04'00'

Privacy Officer, Angela Pluff

JERAMY DRAKE

Digitally signed by JERAMY DRAKE
Date: 2023.09.22 09:11:42 -07'00'

Information System Security Officer, Jeramy Drake

MICHAEL HARTZELL

Digitally signed by MICHAEL HARTZELL
Date: 2023.09.22 13:02:14 -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).

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

SORN 114VA10D, The Revenue Program – Billing and Collections Records-VA: https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01541.pdf

HELPFUL LINKS:

Record Control Schedules:

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

National Archives (Federal Records Management):

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

VA Form 10-10EZR – Health Benefits Update Form:

https://www.va.gov/vaforms/medical/pdf/VA%20Form%2010-10EZR.pdf

VHA Publications:

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

VA Privacy Service Portal:

https://department.va.gov/privacy/

SORN 24VA10A7, Patient Medical Records-VA:

https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

SORN 114VA10, The Revenue Program – Billing and Collections Records-VA:
https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01541.pdf