Privacy Impact Assessment for the VA IT System called:

Health Data Repository II Azure Cloud

Veteran's Health Administration (VHA)

Enterprise Portfolio Management Division

(EPMD)

2416

Date PIA submitted for review:

6/12/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Phillip Cauthers	Phillip.Cauthers@va.gov	503-721-1037
Information System Security Officer (ISSO)	Louis McCrutchen	Louis.McCrutchen@va.gov	202-461-8872
Information System Owner	Paul Arnold	Paul.Arnold@va.gov	727-310-5193

Abstract

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

The Health Data Repository (HDR II AC) is a data repository of clinical information that resides on one or more independent platforms and is used by clinicians and other personnel to facilitate longitudinal patient-centric care. The Health Data Repository (HDR II AC) is a data repository of clinical information that resides on one or more independent platforms and is used by clinicians and other personnel to facilitate longitudinal patient-centric care.

Overview

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

1 General Description

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

Enterprise Portfolio Management Division (EPMD) owns Health Data Repository II AC (HDR II AC).

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

HDR II AC provides a repository of clinical information normally residing on one or more independent platforms for use by clinicians and other personnel in support of Veteran-centric care. The data are derived from legacy, transaction-oriented systems and organized in a format to support clinical decision-making in support of health care, independent of physical location or patient information. HDR II AC will hold individual patient medical records that delineate all aspects of a Veteran's clinical care across the continuum within the VHA. Storage and retrieval of data from Veterans Health Information Systems and Technology Architecture (VistA) to the repository is in real-time. HDR II AC accesses all VistA systems (159 systems). HDR II AC provides the back-end services and does not include a user interface.

The HDR II AC system includes a number of services, such as: Clinical Data Service (CDS), Pathways, Federated Patient Data Service (FPDS) and Aggregate Read Service (ARS) to provide clinical and non- clinical data from a federation of VistA systems, as well as enabling storage and retrieval of Home Telehealth (HTH) data from the HDR II AC database. The Data Federation Design Pattern (DFDP) facilitates parallel access to the data sources and aggregation of data retrieved from the various data sources. HDR II AC integrates with the Identity Management System (IdM) to obtain corresponding local identifiers when a national identifier is supplied on a Read request and uses this information to determine the VistA systems from to extract data.

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

VA owned and VA operated.

2. Information Collection and Sharing

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

The expected number of individuals whose information is accessible through HDR II AC increases as new VA patients are added to VistA, currently there are over 2 million records stored in VistA. The typical client or affected individual is any Veteran utilizing the VA's labs, allergy clinics, or outpatient pharmacy.

The number of individuals varies at any given time, but information on ALL VA patients that have allergy, lab and outpatient pharmacy data in VistA, may also be present in HDR II AC.

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

HDR II AC will hold individual patient medical records that delineate all aspects of a Veteran's clinical care across the continuum within the VHA. Storage and retrieval of data from Veterans Health Information Systems and Technology Architecture (VistA) to the repository is in real-time. HDR II AC accesses all VistA systems (159 systems)

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

The HDR II AC system includes a number of services, such as: Clinical Data Service (CDS), Pathways, Federated Patient Data Service (FPDS) and Aggregate Read Service (ARS) to provide clinical and non- clinical data from a federation of VistA systems, as well as enabling storage and retrieval of Home Telehealth (HTH) data from the HDR II AC database. The Data Federation Design Pattern (DFDP) facilitates parallel access to the data sources and aggregation of data retrieved from the various data sources. HDR II AC integrates with the Identity Management System (IdM) to obtain corresponding local identifiers when a national identifier is supplied on a Read request and uses this information to determine the VistA systems from to extract data.

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

HDR II AC is operating the VAEC Azure Cloud all data is encrypted.

3. Legal Authority and SORN

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

SORN 24VA10A7 / 85 FR 62406 "Patient Medical Records-VA" https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf. Authority for maintenance of the system: Title 38, United States Code, Sections 501(b) and 304.

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 SORN does not require amendment at this time.

4. System Changes

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

No

K. *Will the completion of this PIA could potentially result in technology changes?*

No

Section 1. Characterization of the Information

The following questions are intended to define the scope of the information requested and collected as well as the reasons for its collection as part of the program, IT system, or technology being developed.

1.1 What information is collected, used, disseminated, created, or maintained in the system?

Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy- Protected Information. For additional information on these information types and definitions, please see VA Directives and Handbooks in the 6500 series (https://vaww.va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

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

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1. It must also match the information provided in question 3.4 of the PTA.

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

☒ Name	☒ Personal Mailing Address	☐ Personal Fax Number
☒ Social Security Number	☒ Personal Phone Number(s)	☒ Personal Email Address
☒ Date of Birth		☒ Emergency Contact Information (Name, Phone
☒ Mother's Maiden Name		

Number, etc. of a different individual)
☐ Financial Information
☐ Health Insurance Beneficiary Numbers Account numbers
☐ Certificate/License numbers[1]
☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers

☒ Medications
☒ Medical Records
☒ Race/Ethnicity
☐ Tax Identification Number
☐ Medical Record Number
☒ Gender
☐ Integrated Control Number (ICN)

☐ Military History/Service Connection
☐ Next of Kin
☐ Other Data Elements (list below)

Other PII/PHI data elements:

HDR II AC also facilitates access to additional clinical and non-clinical information through its services, including: Allergies, Vital Signs, Lab results, Appointments, Exam Requests, Exams, Census, Activities of Daily Living (ADL), Disease Management Protocols (DMP), and VistA Virtual Patient Record (VPR) which accesses the full VistA patient clinical record (Problem List, Orders, TIU Documents, Immunizations, Radiology, Consults, etc.).

PII Mapping of Components (Servers/Database)

HDR II AC consists of **4** key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by HDR II AC and the reasons for the collection of the PII are in the table below.

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

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	**Does this system collect PII? (Yes/No)**	**Does this system store PII? (Yes/No)**	**Type of PII (SSN, DOB, etc.)**	**Reason for Collection/ Storage of PII**	**Safeguards**
Health Data Repository (HDR II AC) DB and Clinical Data Services (CDS)	Yes	Yes	Social Security Number, Name, Address received in HL7 messages,	Allergy and medication data required for supporting medication order checks;	VA Network only access that requires VPN access and 2 factor authentications through a

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

			stored temporarily. Only Name loaded into database., Clinical data	Lab and Vitals data to support personal health record	trusted interconnect gateway
Pathways	Yes	Yes	Social Security Number, Name, Address received in HL7 messages, stored temporarily. Only Name loaded into database., Appointments and exam data	Veteran data required to process claims	VA Network only access that requires VPN access and 2 factor authentications through a trusted interconnect gateway
Federated Patient Data Service (FPDS)	Yes	Yes	SSN, Name, Address received in HL7 messages stored temporarily/ Only name loaded in database	Used for extending care to Veterans through VA call centers	VA network only access that requires VPN access and 2 factor authentications through a trusted interconnect gateway

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?

HDR II AC retrieves data from VistA Systems, Department of Defense and Home Telehealth.

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.

• Stores and retrieves clinical data in the HDR II AC database from VistA systems, limited specifically to: Lab results, Vital Signs, Allergies, Allergy Assessments, and Outpatient Pharmacy Medications
• Stores Home Telehealth data in the HDR II AC database, limited specifically to: Vitals, Activities of Daily Living (ADL VR-12) surveys, Patient Satisfaction Surveys, Disease Management Protocols (DMP), and Census Reports
• Aggregates Census and Survey report data and creates reports retrieved by the HTH client
• Stores and retrieves clinical data in the HDR II AC database from the DoD, specifically limited to Allergies and Outpatient Pharmacy Medications
• Retrieves Veteran medical record data real-time from VistA systems where the Veteran has visited.

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

No

1.3 How is the information collected?

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.3a This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technologies used in the storage or transmission of information in identifiable form?

The data in HDR II AC is being collected via electronic transmission through HDR II AC services. HDR II AC receives data from VistA through VIE-VistA Interface Engine (soon to be eMI-enterprise Messaging Infrastructure), from CHDR II AC-Clinical/Health Data Repository for active dual consumers, and from HTH-Home Telehealth.
HDR II AC receives DoD messages from Clinical Health Data Repository (CHDR II AC).
HDR II AC is directly connected to DoD.

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

No information is collected on a form.

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.

Data checked for completeness is done at the application level by VistA and other HDR II AC client applications, and not at the HDR II AC database level.

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

Data checked for completeness is done at the application level by VistA and other HDR II AC client applications, and not at the HDR II AC database level.

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

Legal authority for operating the system is: SORN 24VA10A7 / 85 FR 62406 "Patient Medical Records-VA" https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf. Authority for maintenance of the system: Title 38, United States Code, Sections 501(b) and 304.

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: HDR II AC has access to Personally Identifiable Information (PII). If this information were breached or accidentally released to inappropriate parties or the public, it could result in personal and/or emotional harm to the individuals whose information is contained in the system.

Mitigation: Master Patient Index (MPI) has scrambled PII for all test accounts used by HDR II AC. Any communication of patient records are handled with encryption.

Section 2. Uses of the Information

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

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

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

PII/PHI Data Element	Internal Use	External Use
Name	Used to identify the Veteran medical record for real-time access and treatment	Not used
SSN	Used to identify the Veteran medical record for real-time access and treatment	Not used
DOB	Used to verify the identity of the Veteran	Not used
Mother Maiden Name	Used to verify the identity of the Veteran	Not used
Mailing Address	Used to verify the identity of the Veteran	Not used
Zip Code	Used to verify the identity of the Veteran	Not used
Phone Number	Used to contact Veteran.	Not used
Email Address	Used for correspondence with Veteran.	Not used
Emergency Contact Information	Used for emergency contact.	Not used
Current Medications	Used to record current health and medical conditions of the Veterans. Both VA and DoD medications for Active Dual Consumer (ADC) patients are collected. HDR II AC provides real- time drug-drug, drug-allergy, etc. alerts to the provider treating the Veteran.	Not used
Previous Medical Records	Used to review the history of health and medical conditions of the veterans such as: problems, allergies, diagnosis, therapeutic	Not used

	procedures, X-rays, laboratory tests, and operations.	
Race/Ethnicity	Used to verify identify of Veteran.	Not used
Gender	Used to verify identify of Veteran.	Not used

2.2 What types of tools are used to analyze data and what type of data may be produced?
These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

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

HDR II AC is a real-time system, it does not utilize tools to analyze data but allows Corporate Data Warehouse (CDW) to extract specific Census date from the HDR II AC database for the purpose of analysis and reporting.

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.

HDR II AC is a real-time system, it does not utilize tools to analyze data but allows Corporate Data Warehouse (CDW) to extract specific Census date from the HDR II AC database for the purpose of analysis and reporting.

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?

Encryption

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

SSNs are encrypted, not loaded in the database and only available to certain users.

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

Servers are restricted to only the IP addresses in our whitelist. This whitelist is considered pre-authentication and goes through a process before they are allowed access to HDR II AC

services. This process for gaining access has been documented and begins at the Project Manager. Data owner must approve their access before their server IP addresses are put into the whitelist. They are also the ones that can have entries removed from the whitelist.

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?

- Infrastructure admins manage all active directory accounts. Accounts are provisioned only upon a VA form 9957 or appropriate USD ticket.
- Guest/anonymous and temporary accounts are not allowed.
- Temporary accounts and "need-to-know" changes aren't applicable. For terminations and transfers, the VA form 9957 process makes sure all access changes are handled.
- Account deletions are done SDM ticket or VA form 9957.
- The VA form 9957 process covers expected usage, necessary access, etc.
- Account reviews are not performed.

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

The minimum-security requirements for HDR II AC's high impact system covers 17 security-related areas with regards to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas 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. The HDR II AC application team has implemented the required security controls based on the tailoring guidance of National Institute of Standards and Technology (NIST) Special Publication 800-53 and VA directives or handbooks. VA Records Management Policy and the VA Rules of Behavior recorded in the Talent Management System (TMS), a VA annual training system, govern how veterans' information is used, stored, and protected.

2.4c Does access require manager approval?

Infrastructure admins manage all active directory accounts. Accounts are provisioned only upon a VA form 9957 or appropriate USD ticket.

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

Audit logs are part of the HDR II AC product every request is logged.

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

Servers are restricted to only the IP addresses in our whitelist. This whitelist is considered pre-authentication and goes through a process before they are allowed access to HDR II AC services. This process for gaining access has been documented and begins at the Project Manager. Data owner must approve their access before their server IP addresses are put into the whitelist. They are also the ones that can have entries removed from the whitelist.

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*

- Name
- Social Security Number
- Date of Birth
- Mother's Maiden Name
- Mailing Address
- Phone Numbers
- Email Address
- Current Medications
- Previous Medical Records
- Race/Ethnicity

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.*

The HDR II AC retention process is based upon the Department of Veterans Affairs Record Control Schedule 10-1, revised January 2021. Data will be retained in HDR II AC until 3 years after last episode of care. It will then be converted to the HDR II AC archived system but will be retrievable if/when the patient returns for further treatment. Data in the archived system will be retained 75 years after the Veteran's last episode of care.

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?

HDR II AC records are retained in accordance with Department of Veterans Affairs Privacy Act of 1974, System of Records 24VA10A7 / 85 FR 62406 "Patient Medical Records-VA" https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf. Disposition authority is approved by the Archivist of the United States under, VHA Records Control Schedule (RCS 10–1), Chapter 6, 6000.1d (N1–15–91–6, Item 1d) and 6000.2b (N1–15–02–3, Item 3). RCS 10-1: https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

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

VHA Records Control Schedule (RCS 10–1), Chapter 6, 6000.1d (N1–15–91–6, Item 1d) and 6000.2b (N1–15–02–3, Item 3).
RCS 10-1: https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

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

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

"Health information stored on electronic media is maintained for 75 years after the last update and then destroyed in accordance with VA Directive 6500 – Media Sanitization, which states that "data with a security categorization of 'high' must be destroyed." VA Directive 6500 describes in detail how destruction will take place to include Disposal, Clearing, Purging and Destroying.

HDR II AC records are destroyed in accordance with VA Directive 6500.

Under the jurisdiction of VHA, it is VA policy that all Federal records contained on paper, electronic, or other medium are properly managed from their creation through their final disposition, in accordance with Federal laws, the General Records Schedule (GRS) and VHA Records Control Schedule (RCS) 10-1. The GRS can be found at www.archives.gov. VA Directive 6300, Records and Information Management contains the policies and responsibilities for VA's Records and Information Management program. VA Handbook 6300.1, "Records Management Procedures", Section 3.2, contains mandatory procedures for the proper management of eliminating data at the end of the retention period. Procedures are enforced by Records Management Staff and VA Records Officers.

Paper documents may be shredded or burned, and record destruction is documented in accordance with NARA guidelines. Selected destruction methods for other data media comply with NCSC-TG-025 Version-2/VA Policy. Other IT equipment and electronic storage media are sanitized in accordance with procedures of the NSA/Central Security Service Media Declassification and Destruction Manual and certified that the data has been removed or that it is unreadable. Certification identifies the Federal Information Processing (FIP) item cleared. FIP equipment is not excessed, transferred, discontinued from rental or lease, exchanged, or sold without certification.

The disposition authority is documented in Record Control Schedule 10-1, Section XLIII-1 and XLIII-2. Disposition instructions and procedures for electronic media are documented in NCSC-TG-025 Version- 2/VA Policy, VA Form 0751, and Information Technology Equipment Sanitization Certificate.

No records are disposed/destroyed without the approval of the facility's Record Control Manager. All records are disposed of in accordance with VA Policy and disposition authority (RCS 10-1). Archived and retired records are maintained in accordance with VA Policy.

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.

Master Patient Index (MPI) has scrambled PII for all test accounts used by HDR II AC. Any communication of patient records is handled with encryption.

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: There is a risk that the information maintained by HDR II AC could be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached

Mitigation: To mitigate the risk posed by information retention, HDR II AC adheres to the disposition authority approved by the Archivist of the United States. When the retention date is reached for a record, the individual's information is carefully disposed of. The individual's information is carefully disposed of following the procedures listed in 3.4.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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***
VistA (Veterans Health Information Systems and Technology Architecture)	Clinical Data Services (CDS)	Lab results, Vital Signs, Allergies, Allergy Assessments, and Outpatient Pharmacy Medications	Electronically pulled from VistA thru VAMC thru E-VIE (EnterpriseVistA InterfaceEngine) thru JMS(Java MessageService) Queuesthru CDS (ClinicalData Services)Message Mediator
HTH (Home TeleHealth)	Clinical Data Services (CDS)	Vitals, Surveys, DMPs& Census	Electronically pulled from HTH thru Socket Adapter, thru JMS Queues, thru CDS Message Mediator.
MHV (My Health*e*Vet)	Clinical Data Services (CDS)	VistA Allergies & Lab, HTH Vitals, DoD Allergies	Electronically pushed from HDR II AC DB service thru CDS
RDI (Remote Data Interoperability)	Clinical Data Services (CDS)	VistA and DoD Allergies and OP	Electronically pushed from HDR II AC DB service thru CDS

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***
CRM (Customer Relationship Management)	Clinical Data Services (CDS)	Vista Exams, Requests, & Appointments	Electronically pushed from HDR II AC DB service thru CDS thru Pathways
eBenefits	Clinical Data Services (CDS)	VistA Exams, Requests, & Appointments	Electronically pushed from HDR II AC DB service thru CDS thru Pathways
MHV (My Health*e*Vet)	Clinical Data Services (CDS)	VistA Appointments	Electronically pushed from HDR II AC DB service thru CDS thru Pathways
Mobile Health	Clinical Data Services (CDS)	VistA Appointments	Electronically pushed from HDR II AC DB service thru CDS thru Pathways
Production VistA Instances	Clinical Data Services (CDS)	Log Sensitive Patient Access	Electronically pulled from VistA to HDR II AC DB service thru JMS Queues thru CDS
Cerner EHR	Clinical Data Services (CDS)	Allergies, Outpatient Medications	Electronically pulled from Cerner to HDR II AC DB service thru JMS Queues thru CDS
One VA Pharmacy	Clinical Data Services (CDS)	VistA Pharmacy Data	Electronically pushed from HDR II AC DB

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*
			service thru CDS
VA Profile	Clinical Data Services (CDS)	VistA Pharmacy Data	Electronically pushed from HDR II AC DB service thru CDS thru Pathways
CHDR	Clinical Data Services (CDS)	Allergy, pharmacy	Electronically pulled from VistA to HDR DB service thru CDS
DVP	Clinical Data Services (CDS)	TIU	Electronically pulled from VistA to HDR DB service thru CDS
Mocha	Clinical Data Services (CDS)	Pharmacogenetic	Electronically pushed from HDR DB service thru CDS
PATS-R	Clinical Data Services (CDS)	Vista user, appointment, audio car, facility consult, visit data, document, med, lab, order, radiology, consult, nonvamed, encounter, problem, immunization, flags, diagnosis, non veteran employee, pharmacy, patient alert list, allergy, facility,	Electronically pulled from VistA to HDR DB service thru CDS and pathways
SF-CCCM	Clinical Data Services (CDS)	Allergy, appointment, visit, document, med, lab, order, radiology, consult, nonvamed, encounter, problem, immunization, flags, demographics, patient movement, exam request,	Electronically pulled from VistA to HDR DB service thru CDS

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*
		exam, facility, consults, vista patient remarks, vista user, womens health, TIU	
VAHC	Clinical Data Services (CDS)	Allergy, appointment, visit, document, med, lab, order, radiology, consult, nonvamed, encounter, problem, immunization, flags, demographics, patient movement, exam request, exam, facility, consults, vista patient remarks, vista user, womens health, outpatient Rxs, TIU	Electronically pulled from VistA to HDR DB service thru CDS
VBAAP	Clinical Data Services (CDS)	TIU, vital sign observation, allergy, appointment, consult, CPT, document, education, exam, factor, image, immunization, lab, med, OBS, order, patient, POV, problem, procedure, PTF, skin, surgery, visit, vital,	Electronically pulled from VistA to HDR DB service thru CDS
Vet-HOME	Clinical Data Services (CDS)	User Alerts	Electronically pulled from VistA to HDR DB service thru CDS

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: There is a risk that data contained in the Virtual VA may be shared with unauthorized individuals or that authorized individuals may share it with other VA Internal unauthorized individuals.

Mitigation: The principle of need-to-know is strictly adhered to. Only personnel with a clear business purpose are allowed access to the system and the information contained therein.
HDR II AC clients are not end users but applications that the clinicians (end users) depend upon in delivering care to the Veterans. Centralized data centers are required as the clinicians that use our clients' products are located across the entire VA wide area network.

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***	***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***	***List the method of transmission and the measures in place to secure data***

	specified program office or IT system		***permit external sharing (can be more than one)***	
N/A	N/A	N/A	N/A	N/A

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

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

Follow the format below:

Privacy Risk: None

Mitigation: None

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.

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

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

Notice is also provided in the Federal Register with the publication of the SORN 24VA10A7 that applies to the information in this system. https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

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

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

6.1c Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

Notice has been provided as described in question 6.1a 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.

Information is requested when it is necessary to administer benefits to veterans and other potential beneficiaries. While an individual may choose not to provide information, this may prevent them from obtaining the benefits necessary to them. The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VHA an SSN (see 38 CFR 1.575(a)).

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.

Individuals are provided with a copy of the Notice of Privacy Practices that indicates when information will be used without their consent and when they will be asked to provide consent. Information is used, accessed and disclosed in accordance with the Privacy Act, 5 USC 552a, Title 38 USC 5701, Confidential Nature of Claims, Title USC 7332 and the HIPAA Privacy Rule 45 CFR.

Individuals or their legal representative may consent to the use or disclosure of information via a written request submitted to their facility Privacy Officer. Individuals also have the right to request a restriction to the use of their information. The written request must state what information and/or to whom the information is restricted and must include their signature and date of the request. The request is then forwarded to facility Privacy Officer for review and processing. Individuals may also request to Opt-Out of the facility directory during an inpatient admission. If the individual chooses to opt-out, information is not disclosed from the facility directory unless otherwise required by law.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your 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 Veterans' Health Administration and the local facilities prior to providing the information to the VHA.

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

(SORNs) and Privacy Impact Assessment (PIA) are also available for review online, as discussed in question 6.1.

Section 7. Access, Redress, and Correction

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

7.1 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 https://department.va.gov/foia/ to obtain information about FOIA points of contact and information about agency FOIA processes.***

Individuals do not come to HDR II AC to correct or access records. Whatever system/program enables an individual access is the system/program the individual will contact.

There are several ways a veteran or other beneficiary may access information about them. The Department of Veterans' Affairs has created the MyHealthEVet program to allow online access to their medical records. More information on this program and how to sign up to participate can be found online at https://www.myhealth.va.gov/index.html. Veterans and other individuals may also request copies of their medical records and other records containing personal data from the medical facility's Release of Information (ROI) office.

VHA Directive 1605.01, Privacy and Release of Information, Paragraph 7 outlines policy and procedures for VHA and its staff to provide individuals with access to and copies of their PII in compliance with the Privacy Act and HIPAA Privacy Rule requirements. VHA also created VA form 10-5345a for use by individuals in requesting copies of their health information under right of access.VA Form 10-5345a is voluntary but does provide an easy way for individual to request their records.

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

The system is not exempt from 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?

The system falls under Privacy Act SORN 24VA10A7 "Patient Medical Record-VA"

7.2 What are the procedures for correcting inaccurate or erroneous information?

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed? If the correction procedures are the same as those given in question 7.1, state as much. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Individuals are required to provide a written request to amend or correct their records to the appropriate Privacy Officer or System Manager as outlined in the Privacy Act SORN. Every Privacy Act SORN contains information on Contesting Record Procedure which informs the individual who to contact for redress. Further information regarding access and correction procedures can be found in the notices listed in Appendix A. The VHA Notice of Privacy Practices also informs individuals how to file an amendment request with VHA.

7.3 How are individuals notified of the procedures for correcting their information?

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Veterans are informed of the amendment process by many resources to include the VHA Notice of Privacy Practice (NOPP) which states:

Right to Request Amendment of Health Information.
You have the right to request an amendment (correction) to your health information in our records if you believe it is incomplete, inaccurate, untimely, or unrelated to your care. You must submit your request in writing, specify the information that you want corrected, and provide a reason to support your request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains your information.

If your request for amendment is denied, you will be notified of this decision in writing and provided appeal rights. In response, you may do any of the following:

- File an appeal
- File a "Statement of Disagreement"

- Ask that your initial request for amendment accompany all future disclosures of the disputed health information

Individuals seeking information regarding access to and contesting of VA benefits records may write, call or visit the nearest VA regional office.

Additional notice is provided through the SORN listed in 6.1 of this PIA and through the Release of Information Office where care is received.

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

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

Formal redress via the amendment process is available to all individuals, as stated in questions 7.1-7.3.

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

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

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system, and are they documented?

These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.

8.1a Describe the process by which an individual receives access to the system?

The HDR II AC production system resides solely in the the Azure Cloud VAEC. HDR II AC is a backend system and does not include any user interfaces. All access to its services and interfaces is through client applications. The client application users interact directly with the client applications which in turn use the HDR II AC system to satisfy data requirements to meet the needs of the users. The user roles are determined by the client applications and are not part of or managed by HDR II AC. The HDR II AC system determines the data to be returned to client applications based on the information specified in the request.
All system administrators are granted access by following the Enterprise Operations (EO) 9957 process which is a method used by the VA to ensure that only those who require access to the system are granted access.

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?

All system administrators are granted access by following the Enterprise Operations (EO) 9957 process which is a method used by the VA to ensure that only those who require access to the system are granted access.

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.

All system administrators are granted access by following the Enterprise Operations (EO) 9957 process which is a method used by the VA to ensure that only those who require access to the system are granted access.

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, VA contractors are responsible for maintaining the HDR II AC system, and administration personnel who maintain the server hardware and software but are not primary users of the HDR II AC system itself. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of Behavior training via the VA's Talent Management System (TMS). Contracts are reviewed annually by the Contracting Officer's Representative (COR).

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.

Personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB (for technicians) prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training which all personnel 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 security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system. All VA employees must complete annual Privacy and Security training. Users agree to comply with all terms and conditions of the National Rules of Behavior, by signing a certificate of training at the end of the training session.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* <<ADD ANSWER HERE>>
2. *The System Security Plan Status Date:* <<ADD ANSWER HERE>>
3. *The Authorization Status:* <<ADD ANSWER HERE>>
4. *The Authorization Date:* <<ADD ANSWER HERE>>
5. *The Authorization Termination Date:* <<ADD ANSWER HERE>>
6. *The Risk Review Completion Date:* <<ADD ANSWER HERE>>

7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* <<ADD ANSWER HERE>>

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.***

July 31, 2024

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)*

VA Enterprise Cloud (VAEC)

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.*

No

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.

No

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.

Yes, Data and access is always the responsibility of the customer and required to comply with all VA mandated privacy rules and regulations.

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).

No

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

ID	Privacy Controls
DM-3	Minimization of PII Used in Testing, Training, and Research
IP	**Individual Participation and Redress**
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
SE	**Security**
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR	**Transparency**
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

PHILLIP CAUTHERS

Digitally signed by PHILLIP CAUTHERS
Date: 2025.01.15 09:23:02 -08'00'

Privacy Officer, Phillip Cauthers

LOUIS MCCRUTCHEN

Digitally signed by LOUIS MCCRUTCHEN
Date: 2025.01.15 08:52:44 -05'00'

Information System Security Officer, Louis McCrutchen

PAUL ARNOLD

Digitally signed by PAUL ARNOLD
Date: 2025.01.13 13:44:54 -05'00'

Information System Owner, Paul Arnold

APPENDIX A-6.1

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

VHA Notice of Privacy Practice (NOPP):https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

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

HELPFUL LINKS:

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

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

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

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

Notice of Privacy Practice (NOPP):
VHA Notice of Privacy Practices
VHA Directive 1605.04: Notice of Privacy Practices