Privacy Impact Assessment for the VA IT System called:

Clinical Health Data Repository

Veterans Health Administration (VHA)

Deputy Under Secretary for Health

Health Informatics

Date PIA submitted for review:

March 23, 2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Peggy Pugh	Margaret.Pugh@va.gov	(202) 731-6843
Information System Security Officer (ISSO)	Roland Parten	Roland.Parten@va.gov	(205) 5346179
Information System Owner	Christopher Brown	Christopher.Brown1@va.gov	(202) 802-1432

Abstract

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

The Clinical Health Data Repository (CHDR) generates standards-based, computable Electronic Health Records (EHRs) that can be exchanged between DoD Clinical Data Repository (CDR) and VA Health Data Repository (HDR) healthcare systems for patients marked as Active Dual Consumers (ADC).

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 Clinical Health Data Repository (CHDR) system is a VA owned and operated system under the Office of Assistant Deputy Under Secretary for Health - Health Informatics.

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

The Department of Defense (DoD) and the Department of Veterans Affairs (VA) in partnership, designed and implemented the CHDR system that supports the President's Executive Order to facilitate the sharing of a Veterans Health Information Exchange (VHIE) between DoD and VA.

C. Indicate the ownership or control of the IT system or project.

Department of Veterans Affairs (VA) owns the CHDR system.

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.

CHDR transmits messages using Java Messaging Service (JMS) and does not store PII/PHI in its databases. Information transmitted is on Active Dual Clients (ADC) between VA and DoD. The number of ADC patients for which CHDR transfers data is approx.. 7,111,126.

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

CHDR transfers information between the two agencies repositories and only stores messages. CHDR uses Veterans Data Integration and Federation (VDIF) to transfer information to DoD CDR. CHDR generates standards-based, computable Electronic Health Records (EHRs) that can be exchanged between the two agencies healthcare systems for patients marked as Active Dual Consumers (ADC).

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

At DoD, medical records and patient health care histories are stored in the Clinical Data Repository (CDR), a component of the Armed Forces Health Longitudinal Technology Application (AHLTA). Similarly, medical records at the VA are stored in the Health Data Repository (HDR) which stores data from CHDR and the transactional clinical data from VistA applications for select clinical domains.

CHDR is a combination of these two acronyms (CDR and HDR), and the link between these two agencies repositories. Once the patient is marked as active, data exchange can begin. Data exchange does not occur until ADC activation. CHDR facilitates the sharing of a Veterans Health Information Exchange (VHIE) between DoD and VA for our nations Veterans. This enables the VA/VHA to provide a comprehensive integrated medical record that is compliant with the Health Insurance Portability and Accountability Act (HIPAA) and other privacy regulations, and to facilitate a seamless transition from military to Veteran status. CHDR works in the background to deliver improved information sharing between the DoD and VA of medical records for ADC patients. The interoperability provides clinical users at DoD and VA medical facilities with bidirectional, real-time exchange of medical records that will include, at a minimum, the exchange of outpatient pharmacy and drug allergies (limited only to drug allergies) to enable drug/drug and drug/allergy order checks. The integrated clinical data between the DoD and VA (outpatient pharmacy and drug allergy data) can be viewed in VistA Web.

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.*

The CHDR environment resides within the Austin Information Technology Center (AITC), a data center under Infrastructure Operations (IO). The servers fall under the authorization boundary of the Infrastructure Operations (IO) UNIX Service Lines. CHDR servers and application are hosted on the Solaris M8 Supercluster Sparc/Unix. CHDR collects information from internal VA sources and has no external connectivity outside of the VA.

3. Legal Authority and SORN

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

The legal authority for this operating system is Title 38, United States Code (USC), Section 501, 501(b), 304 and 7301(a). The SORNs that relate to CHDR are 79VA10/85 FR 84114 Veterans Health Information Systems and Technology Architecture (VistA) Records-VA – 12/23/20, 24VA10A7/85 FR 62406 Patient Medical Records – VA, and 168VA005/86 FR 6975 Health Information Exchange – VA.

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?*

N/A

D. System Changes

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

The completion of this PIA will not require changes to any business processes. CHDR went through a refresh which brought the application into compliance with VA TRM.

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

The completion of this PIA will not require changes to any technology processes. CHDR went through a refresh which brought the application into compliance with VA TRM.

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*
☐ 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)
Patient ID: Electronic Data Interchange Personal Identifier (EDIPI)

PII Mapping of Components (Servers/Database)

Clinical Health Data Repository (CHDR) consists of **0** 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 **CHDR** and the reasons for the collection of the PII are in the table below.

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

Internal Database Connections

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

1.2 What are the sources of the information in the system?

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

1.2a List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

VistA systems send data to Health Data Repository (HDR), as well as a copy of that data to CHDR for transmission to DoD Clinical Data Repository (CDR). In the reverse direction, DoD CDR sends data to CHDR which subsequently writes DoD data in HDR.

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.

CHDR transmits data in the form of Java Messaging Service (JMS) from VistA systems which sends to Health Data Repository (HDR), as well as a copy of that data to CHDR for transmission to DoD Clinical Data Repository (CDR). In the reverse direction, DoD CDR sends data to CHDR which subsequently writes DoD data in HDR. Therefore, all information collected from an individual is at the Vista, HDR, and DoD CDR level.

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

N/A

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?

CHDR does not collect data, however the transferred message data from VistA and DoD are stored in a database audit table. Transmission of the data is encrypted using Java Messaging Service (JMS) and CHDR access is role based and only available to administrators as there are no end users.

CHDR receives data from Department of Defense (DoD) Clinical Data Repository (CDR) and VistA systems as follows:

- Retrieves clinical data from the HDR repository, specifically limited to Allergies and Outpatient Pharmacy medications.
- Receives Veteran medical record data real-time from VistA systems.
- Mediate VA and DoD terminology using Standards Terminology System (STS) mapping.
- Identifies/Verifies patient identity using VA Master Patient Index (MPI).
- Receives data from VistA and DoD via VDIF HealthConnect interface models.

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

N/A

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

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

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

CHDR only audits the data that it receives from DoD and VistA. Data checked for accuracy/frequency is done at the application level by VistA, HDR, and DoD CDR applications, and not at the CHDR database level. CHDR database is only used to read data from and write data sent to mentioned applications.

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

N/A

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

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

The legal authority for this operating system is Title 38, United States Code (USC), Section 7301.Additionally CHDR supports the President's Executive Order to facilitate the sharing of a Veterans Health Information Exchange (VHIE) between DoD and VA. AUTHORITY: Executive Order 13335 Sec 2, 3, 4, Executive Order 13410 Sec 2 (b)(c) Sec 3(a) (1)(2), and PL 111-5, Title XIII, Title XXX, Executive Order 13335, Privacy Act of 1974 and Health Insurance Portability and Accountability Act (HIPAA). The SORNs that relate to CHDR is 79VA10/85 FR 84114 Veterans Health Information Systems and Technology Architecture (VistA) Records-VA – 12/23/20, 24VA10A7/85 FR 62406 Patient Medical Records – VA, and 168VA005/86 FR 6975 Health Information Exchange – VA.

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:
In order to identify the patient, CHDR transmits Personally Identifiable Information (PII) from DoD CDR and HDR to link the electronic record. If this information were breached or accidentally released to inappropriate parties of the public, it could result in personal and/or emotional harm to the individuals whose information is transmitted in the system.

Mitigation:
CHDR does not directly collect data from the individual as CHDR receives the information from the two sources, DoD CDR and VistA. CHDR exchanges medical records for Active Dual Consumers (ADC) seamlessly between the two agency repositories.

Master Patient Index (MPI) has scrambled PII for all test accounts used by CHDR. Any communication of patient records is handled with encryption. Electronic Permission Access System (ePAS) is used to allow access for users of CHDR. In addition, all CHDR employees (VA and contractors) are required to complete HIPPA and a Privacy and Information Security and sign a Rules of Behavior (ROB).

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.

Synchronizes allergy and pharmacy data for active dual consumer (ADC) between VA HDR and DoD CDR to support upper-level business systems at each respective agency.

- Current Medications and Allergies: Used to record current health and medical conditions of the Veterans. Both VA and DoD medications for Active Dual Consumer (ADC) patients are collected. CHDR exchanges real-time drug-drug, drug-allergy, etc. alerts to the provider treating the Veteran.

All data mentioned in Section 1.1 is not accessed/used directly from the perspective of the CHDR database. This data is only included within the message transfer audits; all source systems reference the DoD CDR and HDR repositories for that data as follows:

- Name: Used to identify the Veteran medical record for real-time access and treatment.
- Social Security Number: Used to verify the identity of the Veteran.• Date of Birth: Used to verify the identity of the Veteran.
- Mailing Address: Used to verify the identity and correspond with the Veteran.• Phone Number(s): Used to contact the Veteran.
- Email Address: Used for correspondence with the Veteran.
- Unique Patient ID (EUID): Used to verify the identity of the veteran to link electronic record.
- Current Medications and Allergies: Used to record current health and medical conditions of the Veterans. Both VA and DoD medications for Active Dual Consumer (ADC) patients are transmitted. CHDR exchanges real- time drug-drug, drug-allergy, etc. alerts to the provider treating the Veteran.

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.*

CHDR audits processed messages which contain data elements from section 1.1, and stores/retains those messages in the CHDR processing database. The audited message contains the data elements within the Character Large Object (CLOB) of the CHDR audit table. The data elements themselves are not readily available to any database queries without parsing the CLOB object. Data checked for accuracy is done by the source systems by VistA, HDR, and DoD CDR applications, and not at the CHDR database level, therefore data production and data analysis IS performed at the business level systems.

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.

CHDR does not create or make available new information as it only transmits messages that contains previously utilized data elements in section 1.1 from the Vista, HDR, and DoD CDR applications.

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?

The data in transit to and from CHDR are secured through SSL encryption and host name verification.

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, including SSNs are controlled by database security policies at host facility, AITC. The SSN is not retained in CHDR as a separate entity nor data item. The SSN only exists as part of the xml message within one table column element in the audit table and is not exposed directly as a data field.

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

CHDR uses technical safeguards to protect PII/PHI by using SSL encryption and host name verification for data in transit and database security policies at host facility, AITC, to protect and control the data at rest, including SSNs. Physical safeguards are used at host facility, AITC, such as locked racks/cabinets, employee credentials etc.

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***

<u>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.</u>

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

<u>Principle of Transparency:</u> Is the PIA and SORN, if applicable, clear about the uses of the information?

<u>Principle of Use Limitation:</u> 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?

Although there is no "direct" access to PII, any handling of PII is determined by applicability of the job function.

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

CHDR enables Least Functionality and log access records are tracked in Oracle Database Auditing Utilities such as, SQL Developer or Oracle Enterprise Manager. Access to these utilities is controlled through Electronic Permission Access System (ePAS) and are approved by the respective manager.

2.4c Does access require manager approval?

Access to these utilities is controlled through Electronic Permission Access System (ePAS) and are approved by the respective manager.

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

Although there is no "direct" access to PII, any handling of PII is determined by applicability of the job function. CHDR enables Least Functionality and log access records are tracked in Oracle Database Auditing Utilities such as, SQL Developer or Oracle Enterprise Manager. Access to these utilities is controlled through Electronic Permission Access System (ePAS) and are approved by the respective manager.

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

The CHDR 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 VA 6300.1, VA 6500 HB and the VA Rules of Behavior recorded in the Talent Management System (TMS), a VA annual training system, governs how Veterans' information is used, stored, and protected. Following the NIST and VA policy guidance listed above, the separation of duties policy applied, allows CHDR staff members to receive focused and recorded training that provides access only to the areas of the application that applies to their job task and responsibilities. CHDR access is controlled through menu options, and security keys that is approved by the CHDR manager.

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

CHDR audits processed messages which contain data elements from section 1.1 (Name, Social Security, Date of Birth, Personal Mailing Address, Personal Phone Number, Medications, Medical Records, Integrated Control Number (ICN), Patient ID: Electronic Data Interchange Personal Identifier (EDIPI)), and stores/retains those messages in the CHDR processing database. The audited message contains the data elements within the Character Large Object (CLOB) of the CHDR audit table. The data elements themselves are not readily available to any database queries without parsing the CLOB object. There is no PII information is stored with the CHDR DB as separate elements. All data elements are stored with HDR not the CHDR DB. The data does exist in the message column of the audited event table within the format of the XML message and is not exposed directly without parsing the XML message.

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.*

CHDR retains the audited messages for three (3) years (temporary) as referenced in the Department of Veterans Affairs Record Control Schedule 10-1, revised January 2020 located at rcs10-1.pdf (va.gov)

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.
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, the record retention schedule for CHDR audited data retention has been approved by the VA records office and is listed in the Department of Veterans Affairs Record Control Schedule 10-1, revised January 2020 located at rcs10-1.pdf (va.gov) in accordance with the National Archives and Records Administration (NARA) approved General Record Schedules and/or Agency Record Control Schedules.

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

Per VA Records Control Schedule 10-1, Item No. 2000.2 Information Technology Operations and Maintenance Records and disposition authority is DAA-GRS-2013-0005-0004, item 020; 6000.1 Health Records Folder File or CHR (Consolidated Health Record) and disposition authority is N1-15-91-6, item 1a.

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.

CHDR as the application does not handle the destruction, erasing, or anonymizing of data as this is controlled by AITC. Per the VA 6500 Directive VA Cybersecurity Program, Establishes the Information Security Knowledge Service (KS) to provide cybersecurity policies, procedures, and guidance; the Knowledge Service has defined this parameter; additionally, VA Directive 6300 Records and Information Management - defines the frequency displayed on KS.

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.

Not applicable to CHDR as there is no access to the PII data via external systems for the purposes of research, testing, and training.

3.6 <u>PRIVACY IMPACT ASSESSMENT: Retention of information</u>

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 CHDR 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, CHDR 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***
Veterans Health Administration (VHA) Health Data Repository (HDR)	Receives XML messages from HDR and transmits to/from DoD CDR.	Name, Social Security Number, Date of Birth, Personal Mailing Address, Personal Phone Number, Personal Email Address, Current Medications and Allergies	Java Messaging Service (JMS)
Veterans Health Administration (VHA) Health Connect via Veterans Data Integration and Federation (VDIF)	Interface to transmits XML messages from CHDR to/from DoD CDR.	Name, Social Security Number, Date of Birth, Personal Mailing Address, Personal Phone Number, Personal Email Address and Current Medications and Allergies	Java Messaging Service (JMS)
Veterans Health Administration (VHA) Master Patient Index (MPI)	Transmits HL7 messages to/from MPI.	Name, Social Security Number, Date of Birth, Personal Mailing Address, Personal Phone Number, Personal Email Address, Unique Patient ID: Electronic Data Interchange Personal Identifier (EDIPI)	Java Messaging Service (JMS)
Veterans Health Administration (VHA) Veterans Health Information Systems	Receives HL7 messages from VistA.	Name, Social Security Number, Date of Birth, Personal Mailing Address, Personal Phone Number, Personal Email Address, Current Medications and Allergies	Java Messaging Service (JMS)

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***
and Technology Architecture (VistA)			

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 privacy risk associated with maintaining PII/PHI is that sharing data within the Department of Veterans' Affairs could happen and the data may be disclosed to individuals who do not require access and heightens the threat of the information being misused.

Mitigation:
The principle of need-to-know is strictly adhered to by the CHDR personnel. Only personnel with a clear business purpose are allowed access to the system and the information contained within.

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***
N/A	N/A	N/A	N/A	N/A

5.2 <u>PRIVACY IMPACT ASSESSMENT: External sharing and disclosure</u>

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:
Not Applicable

Mitigation:
Not Applicable

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.

This Privacy Impact Assessment (PIA) also serves as notice of the CHDR System. As required by the Government 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." The SORNs that relate to CHDR are 79VA10 / 85 FR 84114 Veterans Health Information Systems and Technology Architecture (VistA) Records - VA; 24VA10A7/85 FR 62406 Patient Medical Records – VA; 168VA005/86 FR 6975 Health Information Exchange – VA.

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

N/A

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.

This Privacy Impact Assessment (PIA) also serves as notice of the CHDR System. As required by the Government 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."

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.

While CHDR does not collect information directly from the Veteran but instead from the source application of DoD and VistA, depending on the information required, some data collection is mandatory while others are voluntary. Failure to provide information may result in denial of access to the health care system.

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.

Any right to consent to particular uses of the information would be handled by the source systems that collect the information from the Veteran and feeds CHDR with information. The source systems are HDR and VistA.

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 individuals are unaware that their information is being collected.

Mitigation:
Individuals are notified by this PIA. The system does not collect information directly from individuals. The source systems PIAs provide further notice.

Section 7. Access, Redress, and Correction

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

7.1 What are the procedures that allow individuals to gain access to their information?

These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions ***. For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.***

Individuals wishing to gain access to their information is managed under the source systems, HDR and VistA, Privacy Impact Assessments (PIAs).

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).

Individuals wishing to gain access to their information is managed under the source systems, HDR and VistA, Privacy Impact Assessments (PIAs).

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.

Individuals wishing to gain access to their information is managed under the source systems, HDR and VistA, Privacy Impact Assessments (PIAs).

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 wishing to obtain more information about access, redress, and record correction of their information is managed under the source systems, HDR and VistA, Privacy Impact Assessments (PIAs).

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.

Notifying individuals of the procedures for correcting their information is managed under the source systems, HDR and VistA, Privacy Impact Assessments (PIAs).

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.

Individuals wishing to obtain more information about access, redress, and record correction of their information is managed under the source systems, HDR and VistA, Privacy Impact Assessments (PIAs).

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 information provided by an individual is incorrect and they are unaware of how to correct it.

Mitigation:
The system does not collect information directly from individuals. The source systems PIAs provide detail on access, redress, and correction.

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 CHDR database is controlled and documented through Electronic Permission Access System (ePAS) and are approved by the respective manager. There is no direct access to the information other than system and database administration 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?

N/A

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.

The roles used for CHDR access are as follows:

- AITC Production Systems Administrator provides full root access;
- AITC Production WebLogic Administrator provides full root access;
- AITC Production Database Administrator provides full root access;
- HDSO Sustainment Support Systems Administrator provides limited elevated privileges access to the OS level;
- HDSO Sustainment Support WebLogic Administrator provides limited access to production WebLogic console as read only. Administrator access to WebLogic console in SQA and Development environments;
- HDSO Sustainment Support Database Administrator provides limited access to production DB as read only. Limited access to SQA and development DB as required to support CHDR Sustainment.

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, contractors will have access to the system. Health Services Development, Security, and Operations (DevSecOps) support contractors are responsible for maintaining application Technical Reference Model (TRM) and Fortify compliance as well as defect repair where applicable. WebLogic, and Database administrators are responsible for supporting the hardware and infrastructure on which CHDR is deployed. All contractors sign a Non-Disclosure Agreement (NDA) and are cleared using the VA background investigation process and must obtain a Moderate Background Investigation (MBI). This process is taken care of during the onboarding process of the CHDR project.

Developers and Administrators with a need for elevated roles and access permissions are required to submit an ePAS request for access to respective systems and are only granted upon approval by the VA COR and Security Representatives as described in section 2.4. The contractors who provide support to the system are required to complete annual role-based training which is mandated for all CHDR personnel with elevated privileges and is administrated through IT Workforce Development (ITWD). Annual privacy training is required for all CHDR personnel and is administered through VA Talent Management System (TMS).

VA contracting performs reviews on contracts according to their Period of Performance defined within the existing/current contract. Contractors have no specific need to access PII. Access is inherent only if Contractors/Administrators have a need to access to the audited messages within the CHDR processing database.

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.

Annual role-based training is mandated for all CHDR personnel with elevated privileges and is administrated through IT Workforce Development (ITWD). Annual privacy training is required for all CHDR personnel and is administered through VA Talent Management System (TMS).

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Completed
2. *The System Security Plan Status Date:* 04/18/2022
3. *The Authorization Status:* 1-year ATO
4. *The Authorization Date:* 06/10/2022
5. *The Authorization Termination Date:* 06/10/2023
6. *The Risk Review Completion Date:* 05/11/2022
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

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

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)*

Not Applicable; CHDR 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.*

Not Applicable; CHDR 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.

Not Applicable; CHDR 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.

Not Applicable; CHDR 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).

Not Applicable; CHDR does not use Robotics Process Automation (RPA).

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

ID	Privacy Controls
AP	**Authority and Purpose**
AP-1	Authority to Collect
AP-2	Purpose Specification
AR	**Accountability, Audit, and Risk Management**
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-7	Privacy-Enhanced System Design and Development
AR-8	Accounting of Disclosures
DI	**Data Quality and Integrity**
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
DM	**Data Minimization and Retention**
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
IP	**Individual Participation and Redress**
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
SE	**Security**
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR	**Transparency**
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**

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.

Margaret L. Pugh 104985

Digitally signed by Margaret L. Pugh 104985
Date: 2023.04.17 16:40:22 -04'00'

Privacy Officer,

ROLAND PARTEN

Digitally signed by ROLAND PARTEN
Date: 2023.04.17 15:16:09 -05'00'

Information System Security Officer,

Christopher Brown 101386

Digitally signed by Christopher Brown 101386
Date: 2023.04.20 15:32:57 -05'00'

Information System Owner,

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).

Government Act of 2002, Pub.L. 107–347

Current SORN List (va.gov)

79VA10 / 85 FR 84114 Veterans Health Information Systems and Technology Architecture (VistA) Records – VA

24VA10A7/85 FR 62406 Patient Medical Records – VA

168VA005/86 FR 6975 Health Information Exchange – VA

HELPFUL LINKS:

Record Control Schedules:

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

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

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

National Archives (Federal Records Management):

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

VHA Publications:

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

VA Privacy Service Privacy Hub:

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

Notice of Privacy Practice (NOPP):

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices