Privacy Impact Assessment for the VA IT System called:

Administrative Data Repository (ADR)

Veterans Health Administration

Integrated Campus Support

Date PIA submitted for review:

3/23/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Nancy Katz- Johnson	Nancy.katz-johnson@va.gov	203-535-7280
Information System Security Officer (ISSO)	Joseph Facciolli	joseph.facciolli@va.gov	2158422000x2012
Information System Owner	Athanasia Boskailo	Louise.Rodebush@va.gov	2168490193
Data/Business/Information Owner2	James Whited	james.whited@va.gov	202-329-5367

Abstract

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

The purpose of the Administrative Data Repository (ADR) is to host demographic, and eligibility/enrollment information for all persons who interact with the VA's Enrollment and Identity Services applications. In addition to Veterans, healthcare providers--including direct care providers within and outside the VA, business office personnel, researchers and management--all require this administrative data to provide and improve healthcare delivery to Veterans. ADR hosts the records of 20 million individuals. In the VA enterprise n-tier architecture, ADR serves as the data layer and its consuming/supporting applications make up the service layer. Applications currently supported by ADR include Enrollment System (ES), Identity Management Application (IdHub), and related Common Services applications. Administrative data updates from the Health Eligibility Center (HEC) are synchronized with the ADR database via messaging from the supported applications. ADR production databases (ADRP) are used for online transaction processing. ADRP database is replicated nightly via disk mirroring to the ADR Reporting database (ADRRP), which is used for online analytical processing. This static copy of the ADR production database is used for read-only activities such as ESR reports and batch jobs, HEC reports, and other data extraction purposes.

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.
Administrative Data Repository (ADR). Integrated Campus Support

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

The purpose of the Administrative Data Repository (ADR) is to host demographic, identity management, and eligibility/enrollment information for all persons who interact with the VA's Enrollment and Identity Services applications. In addition to Veterans, healthcare providers--including direct care providers within and outside the VA, business office personnel, researchers and management--all require this administrative data to provide and improve healthcare delivery to Veterans. In the VA enterprise n-tier architecture, ADR serves as the data layer and its consuming/supporting applications make up the service layer. Applications currently supported by ADR include Enrollment System (ES), Identity Management Application (IdHub), and related Common Services applications. Administrative data updates from the Health Eligibility Center (HEC) are synchronized with the ADR database via messaging from the supported applications. ADR production databases (ADRP) are used for online transaction processing. ADRP database is replicated nightly via disk mirroring to the ADR Reporting database (ADRRP), which is used for online analytical processing. This static copy of the ADR production database is used for read-only activities such as ESR reports and batch jobs, HEC reports, and other data extraction purposes.

C. Indicate the ownership or control of the IT system or project.
VA Owned and VA Operated IS

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.

The purpose of the Administrative Data Repository (ADR) is to host demographic, and eligibility/enrollment information for all persons who interact with the VA's Enrollment and Identity Services applications. In addition to Veterans, healthcare providers--including direct care providers within and outside the VA, business office personnel, researchers and management--all require this administrative data to provide and improve healthcare delivery to Veterans. ADR hosts the records of 20 million individuals.

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

Administrative Data Repository (ADR) is an online transactional processing database designed to host demographic; Veterans Information Eligibility Reporting System (VIERS)/Affordable Care Act, Applications currently supported by ADR include Veterans Information Eligibility Reporting System (VIERS)/Affordable Care Act (ACA). Administrative data updates from the Health Eligibility Center (HEC) are synchronized with the ADR database via messaging from the supported applications. In addition to Veterans, healthcare providers including direct care providers within and outside the VA, business office personnel, researchers and management, all require this administrative data to provide and improve healthcare delivery to Veterans. The Administrative

Data Repository Reporting (ADRRP) database is replicated nightly via Data Guard conversion of the ADR Reporting database (ADRRP) to physical standby mode for syncing, then conversion back to snapshot standby mode. ADR is managed as a centralized corporate asset at the Austin Information Technology Center (AITC). The database is implemented in a clustered server configuration to provide high availability of the data. In addition to full database snapshots taken daily, changes to the ADR database are written at regular intervals to Oracle archive logs (transaction journals) to provide for backup/restore capability. A redundant ADR system is maintained at the Hines Information Technology Center for disaster recovery purposes.

F. 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 ADR system is housed at the Austin Information Technology Center (AITC) located at 1615 Woodward St. Austin, TX 78772.The servers listed in the Component Details tab are included for informational purposes only. These servers fall under the authorization boundary of the Infrastructure Operations (IO) UNIX Service Lines. ADR is designed as the persistence layer in the HeV architecture to store and retrieve identity and demographic data and eligibility and enrollment data. The ADR DR site is located at the Hines ITC. The servers for DR are exact replicas of the production servers. The Hines Data Center is housed in Building 215, Hines ITC, Hines, IL 60141 in Room 100.

3. Legal Authority and SORN

E8-28183.pdf (govinfo.gov)

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

SORN # 150VA19 SORN Title: Administrative Data Repository -VA
https://www.govinfo.gov/content/pkg/FR-2008-11-26/pdf/E8- 28183.pdf

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 38, United States Code, Section 501.and Section 7304.

H. 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

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

No

J. Whether 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.

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)

No other information is stored in ADR

PII Mapping of Components (Servers/Database)

ADR consists of 1 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 ADR 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
Database 1	Yes	Yes	VIERS shares all data types listed in section 1.1 with ADR	VIERS uses ADR to store electronic records	VA 6500 Control in place

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?

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.

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

ADR is a consolidated location used by other VA applications to store administrative records. All information stored in ADR is sent to ADR by other applications.
The applications which store information in ADR are:

• Veterans Information Eligibility Reporting System (VIERS)

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?

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.

All information stored in ADR is sent to it electronically by the applications listed in Section 1.2.

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.
ADR does not check the information provided to it for accuracy. It is the responsibility of the VA Enrollment and other applications which provide the information to ADR to check the information for accuracy

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.

ADR does not check the information provided to it for accuracy. It is the responsibility of the VA Enrollment and other applications which provide the information to ADR to check the information for accuracy

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

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

- ADR's legal authority can be found in Title 38, United States Code, Section 501 and Section 7304:
- (http://www.gpo.gov/fdsys/granule/USCODE-2011-title38/USCODE-2011-title38-partI-chap5-subchapI-sec501/content-detail.html) ;

And SORN: 150VA19 "Administrative Data Repository – VA" E8-28183.pdf (govinfo.gov)

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: Administrative Data Repository (ADR) operates using Personally Identifiable Information (PII) and Protected Health Information (PHI). 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: The Department of Veterans Affairs is careful to only collect the information necessary to provide health care to the veteran. By only collecting the minimum information necessary the VA is able to better protect the veterans' information. The information is stored using encryption and is located behind VA firewalls.

Section 2. Uses of the Information

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

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

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

-
- Name: Used to identify veteran patient records.
- Social Security Number: Used to verify the identity of the veteran.
- Date of Birth: Used to verify the identity of the veteran.
- Mother's Maiden Name: Used to identify veteran patient records.
- Phone Number: Used to identify veteran patient records.
- Email Address: Used to identify veteran patient records.
- Financial Account Information: Used to identify veteran patient records.

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.

Data stored in ADR is not analyzed and nothing is produced by ADR. ADR stores data for other applications

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.

- Data stored in ADR is not analyzed and nothing is produced by ADR. ADR stores data for other 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?
Both ACA/VIERS applications/services and DB are hosted in the same AITC secured boundary/data center

- SQLNET.FIPS_140 = TRUE
  to run Oracle Advanced Security SSL (Secure Sockets Layer) in **Federal Information Processing Standard (FIPS)** Mode

ACA/VIERS data is stored for auditing with authorization/authentication control to limited ACA/VIERS team members and ADR DBAs required VA annual VA Privacy and Information Security Awareness and ROB and HIPAA Training.

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

The collecting/processing of SSNs is conducted by ACA/VIERS applications/services.

ACA/VIERS data is stored for auditing with authorization/authentication control to limited ACA/VIERS team members and ADR DBAs required VA annual VA Privacy and Information Security Awareness and ROB and HIPAA Training.

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

- ACA/VIERS data is stored for auditing with authorization/authentication control to limited ACA/VIERS team members and ADR DBAs required VA annual VA Privacy and Information Security Awareness and ROB and HIPAA Training.

- SQLNET.FIPS_140 = TRUE
  to run Oracle Advanced Security SSL (Secure Sockets Layer) in **Federal Information Processing Standard (FIPS)** Mode

- ACA/VEIRS applications and ADR DB both are hosted in the AITC secured boundary (data center)

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?

- System administrators only access ADR database for system operational maintenance. ADR does not permit any End User access to PII.

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

All ADR access database documentation are maintained in the Epas system

2.4c Does access require manager approval?

Currently, there is no one using PII. If this changes in the future, it will go through the Epas validation process. Any access to ADR database will require user to go through ePAS validation process that ensures proper validation and management approval

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

Not Applicable – at the moment, there is no access to PII. See above response

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, Zip Code, Phone Numbers, Fax Number, Email Address, Emergency Contact Information, Financial Account Information, Health Insurance Beneficiary Numbers Account numbers, 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.*

ADR information is retained for 75 years after the last record update. This retention period is required by the Department of Veterans Affairs Record Control Schedule 10-1, Records Control Schedule 10-1 (va.gov)

RETENTION AND DISPOSAL: The records must be disposed of in accordance with the records retention standards authorized by the National Archives and Records Administration General Records Schedule 14, published in the Veterans Health Administration Records Control Schedule 10–1,. Records Control Schedule 10-1 (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. 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?

ADR records are retained in accordance with General Record Schedule 14, item 6 and published in the Veterans Health Administration Records Control Schedule 10-1, http://www.va.gov/vhapublications/RCS10/rcs10-1.pdf

The data stored in ADR falls under the Administrative Data Repository SORN: 150VA19 "Administrative Data Repository – VAE8-28183.pdf (govinfo.gov)

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

ADR records are retained in accordance with General Record Schedule 14, item 6 and published in the Veterans Health Administration Records Control Schedule 10-1, http://www.va.gov/vhapublications/RCS10/rcs10-1.pdf

The data stored in ADR falls under the Administrative Data Repository SORN: 150VA19 "Administrative Data Repository – VA" E8-28183.pdf (govinfo.gov)

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 Handbook 6500.1 – Media Sanitization, which states that data with a security categorization of high must be destroyed.

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

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 ADR 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, ADR 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

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 Information Eligibility Reporting System (VIERS)	VIERS uses ADR to store electronic records. VIERS also retrieves records from ADR	VIERS shares all data types listed in section 1.1 with ADR	Data is transmitted electronically.

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 is that sharing data within the Department of Veteran's Affairs could happen and that 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 Disability Clinician User Interface Version Date: December 7, 2020 Page 13 of 19 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***

No external sharing	No external sharing	No external sharing	No external sharing	No external sharing

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

Follow the format below:

Privacy Risk: There is a risk that information may be shared with an unauthorized VA program, system, or individual.

Mitigation: Safeguards implemented to ensure data is not sent to the wrong VA organization are employee security and privacy training and awareness and required reporting of suspicious activity. Use of secure passwords, access for need-to-know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized within the facilities.

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.

Data stored by ADR is received from other applications. ADR does not collect any information directly from veterans or their dependents. (VIERS).

Privacy Impact Assessments for these systems can be located:
http://www.oprm.va.gov/privacy/pia.aspx

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: E8-28183.pdf (govinfo.gov)

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.

Data stored by ADR is received from other applications. ADR does not collect any information directly from veterans or their dependents.

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.

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.

Data stored by ADR is received from other applications. ADR does not collect any information directly from veterans or their dependents.

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 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 individuals who provide information to the VA applications VIERS will not know how their information is being shared and used internal to the Department of Veterans Affairs.

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 http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.***

There are no procedures for individuals to gain access to their information on ADR. Individuals who desire to gain access to their information must contact the application which originally gathered the information (VIERS)

Individuals seeking information regarding access to and contesting of records in this system may write, call or visit the VA facility location where they are or were employed or treated or made contact.

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

This system is not exempt

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.

There are no procedures for individuals to gain access to their information on ADR. Individuals who desire to gain access to their information must contact the application which originally gathered the information (VIERS)

Information is in a Privacy Act System of Records

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 seeking information regarding access to and contesting of records in this system may write, call or visit the VA facility location where they are or were employed or treated or made contact.

There are no procedures for correcting inaccurate information. Individuals who desire to correct inaccurate information must contact the application which originally gathered the information (VIERS)

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.

There are no procedures for correcting inaccurate information. Individuals who desire to correct inaccurate information must contact the application which originally gathered the information (VIERS)

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 SORS 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.

N/A

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 the information provided to ADR is inaccurate and decisions are made with incorrect information.

Mitigation: Individuals who desire to correct inaccurate information must contact the application which originally gathered the information (VIERS).

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.

ADR functions as a back-end 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 ADR 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 ADR. The ADR system determines the data to be returned to client applications based on the information specified in the request filers. Similarly, when storing data ADR uses the information specified in the templates to identify the ADR database table in which to store the data. 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?

ADR functions as a back-end 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 ADR 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 ADR. The ADR system determines the data to be returned to client applications based on the information specified in the request filers. Similarly, when storing data

ADR uses the information specified in the templates to identify the ADR database table in which to store the data. 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.

ADR functions as a back-end 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 ADR 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 ADR. The ADR system determines the data to be returned to client applications based on the information specified in the request filers. Similarly, when storing data ADR uses the information specified in the templates to identify the ADR database table in which to store the data. 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 ADR system, and administration personnel within the Austin Information Technology Center (AITC) who maintain the server hardware and software but are not primary users of the ADR 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).

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 AITC 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:* Approved
2. *The System Security Plan Status Date:* 15-Feb-2023
3. *The Authorization Status:* Approved
4. *The Authorization Date:* 16-Dec-2022
5. *The Authorization Termination Date:* 14-Jun-2023
6. *The Risk Review Completion Date:* 05-Oct-2022
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* High

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

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

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)*

N/A

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.*

N/A

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.

N/A

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.

N/A

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).

N/A

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

ID	Privacy Controls
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.

NANCY KATZ-JOHNSON

Digitally signed by NANCY KATZ-JOHNSON
Date: 2023.04.07 15:31:12 -04'00'

Privacy Officer, Nancy Katz- Johnson

JOSEPH FACCIOLLI

Digitally signed by JOSEPH FACCIOLLI
Date: 2023.04.10 13:50:06 -04'00'

Information System Security Officer, Joseph Facciolli

ATHANASIA BOSKAILO

Digitally signed by ATHANASIA BOSKAILO
Date: 2023.04.10 13:05:35 -04'00'

Information System Owner, Athanasia Boskailo

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).

Data stored by ADR is received from other applications. ADR does not collect any information directly from veterans or their dependents. (VIERS).

Privacy Impact Assessments for these systems can be located:
http://www.oprm.va.gov/privacy/pia.aspx

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: E8-28183.pdf (govinfo.gov)

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