Privacy Impact Assessment for the VA IT System called:

Veterans Data Integration and Federation Enterprise Platform (VDIF-EP)

VHA

Date PIA submitted for review:
December 30, 2022

System Contacts:

<table>
<thead>
<tr>
<th>System Contacts</th>
<th>Name</th>
<th>E-mail</th>
<th>Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Officer</td>
<td>Margaret Pugh</td>
<td><a href="mailto:Margaret.pugh@va.gov">Margaret.pugh@va.gov</a></td>
<td>202-731-6843</td>
</tr>
<tr>
<td>Information System Security Officer</td>
<td>Thomas Orler</td>
<td><a href="mailto:Thomas.orler@va.gov">Thomas.orler@va.gov</a></td>
<td>708-938-1247</td>
</tr>
<tr>
<td>(ISSO)</td>
<td>(ISSO)</td>
<td>(ISSO)</td>
<td>(ISSO)</td>
</tr>
<tr>
<td>Information System Owner</td>
<td>Christopher Brown</td>
<td><a href="mailto:Christopher.Brown1@va.gov">Christopher.Brown1@va.gov</a></td>
<td>202-270-1432</td>
</tr>
</tbody>
</table>
Abstract

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

The Veterans Data Integration and Federation Enterprise Platform (VDIF-EP) is an Intersystem COTS suite of applications that will improve access to VistA data by federating patient record data at a national level. The ability to cache the federated patient data will reduce the impact on Vista systems and will dramatically improve response times to internal as well as external partners. This platform provides the ability to transform VistA data to standard formats required by consuming systems to include; HL7 messaging, Clinical Document Architecture (CDA) documents (C32, C62, C-CDA CCD v1.1, C-CDA CCD v2.1, C-CDA SES), Fast Healthcare Interoperability Resources (FHIR), and Health Share Standard Document Architecture (SDA) to name a few. In addition, the VDIF provides the ability to support message and service oriented formats such as SOAP and Representational State Transfer (REST)-style interoperability. Another feature of the VDIF is the ability to orchestrate and execute business processes and business rules that are tightly integrated into the platform. The standardized VDIF allows for new systems/applications to quickly ramp up and take advantage of the federated data available using development tools with built in governance. For the next 2 years the Legacy Data Governance team will be migrating and integrating new and existing systems onto to the VDIF. We will be sun-setting existing systems such as the Vitria Interface Engine (VIE), the Electronic Health Exchange (eHX) Adaptor, and Electronic Messaging Infrastructure (eMI) to name a few.

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.
      Health Middleware Data Management (HMDM)

   B. The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.
      The Veterans Data Integration and Federation Enterprise Platform (VDIF-EP) is an Intersystem COTS suite of applications that will improve access to VistA data by federating patient record data at a national level.

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

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.
All eligible veterans including retirees.

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

The Veterans Data Integration and Federation (VDIF) is an Intersystems COTS suite of
applications that improves access to VistA data by federating patient record data at a national
level. The ability to cache the federated patient data reduces the impact on Vista systems and
dramatically improves response times to internal as well as external partners.

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

The platform provides the ability to transform VistA data to standard formats required
by consuming systems to include; HL7 messaging, Clinical Document Architecture (CDA)
documents (C32, C62, CCD A CCD v1.1, C-CDA CCD v2.1, C-CDA SES), Fast Healthcare
Interoperability Resources (FHIR), and HealthShare Standard Document Architecture (SDA)
to name a few. Health Share comprises Health Connect Enterprise HL7 Messaging, Regional
HL7 Router Health Connect, Regional Health Connect, Service Bus HealthConnect Proxies,
Access Gateways, Edge Gateways, Patient and Facility Registries, and an Audit Repository.

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.

Accuracy is checked by source systems (VMI, ESR, eCMS, VA VISTA, etc.) providing
data feed views to VDIF.

3. Legal Authority and SORN

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

• Presidential Review Directive 5, A National Obligation – Planning for Health
  Preparedness for and Readjustment of the Military, Veterans, and Their Families after Future
  Deployments, August 1998
• Per SORN 24VA10A7 – Patient Medical Records Title 38, United States Code, Section 501(b)
  and 304.

I. If the system is in the process of being modified and a SORN exists, will the SORN require
amendment or revision and approval? If the system is using cloud technology, does the SORN
for the system cover cloud usage or storage?
  a. No  b. No

D. System Changes
J. Whether the completion of this PIA will result in circumstances that require changes to business processes
   No changes to the business processes are required for the completion of this PIA.

K. Whether the completion of this PIA could potentially result in technology changes
   No technology changes required for the PIA completion.

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://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)
VDIF’s message traffic is transmitted by the application may contain PII/PHI such as names, SSN, addresses, emails, health information, user’s login identifier, user ID, name of user, query action, user’s unique CAC or PIV ID, start and end timestamps, and date of audit. VDIF then enables a read-only view of a patient’s medical information. Data is disseminated in the read only viewer of the client’s software.

**PII Mapping of Components (Servers/Database)**

VDIF consists of 5 key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by VDIF 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**

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

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?

Veterans Health Information Systems and Technology Architecture (VistA), Master Veteran Index (MVI), Enrollment System Redesign (ESR), Standards and Terminology Services (STS), and eHX (eHealth eXchange)

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.
VDIF only collects the login information for auditing purposes. VDIF functions as the communications backbone of the VA data sharing environment as well as the VA’s dedicated single-point transport mechanism for all connectivity services related to all interoperability integrations of medical health systems between the VA and other authorized federal agencies and private healthcare facilities.

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

Veterans Health Information Systems and Technology Architecture (VistA),
Master Veteran Index (MVI),
Enrollment System Redesign (ESR),
Standards and Terminology Services (STS), and
eHX (eHealth eXchange)

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?

VDIF functions as the communications backbone of the VA data sharing environment as well as the VA’s dedicated single-point transport mechanism for all connectivity services related to all interoperability integrations of medical health systems between the VA and other authorized federal agencies and private healthcare facilities.

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.

VDIF only collects the login information for auditing purposes (see 3.1). VDIF functions as the communications backbone of the VA data sharing environment as well as the VA’s dedicated single-point transport mechanism for all connectivity services related to all interoperability integrations of medical health systems between the VA and other authorized federal agencies and private healthcare facilities.

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.

Accuracy is checked by source systems (VMI, ESR, eCMS, VA VISTA, etc.) providing data feed views to VDIF.

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.

Accuracy is checked by source systems (VMI, ESR, eCMS, VA VISTA, etc.) providing data feed views to VDIF.

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-I, Authority to Collect:

- Per SORN 24VA10A7 – Patient Medical Records Title 38, United States Code, Section 501(b) and 304.

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

Principle of Purpose Specification: Explain how the collection ties with the purpose of the underlying mission of the organization and its enabling authority.
**Principle of Minimization:** Is the information directly relevant and necessary to accomplish the specific purposes of the program?

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

**Principle of Data Quality and Integrity:** Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current? This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

**Privacy Risk:** VDIF disseminates a visual display of Personally Identifiable Information (PII) and other highly delicate Personal Health Information (PHI). If this information was breached or accidentally released to inappropriate parties or the public, it could result in financial, 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 accomplish the VA mission. Additionally, to identify the parties involved in an incident, identify potential issues and concerns, and aid the affected parties so that they may find the help they need to get through their crisis. By only collecting the minimum necessary information, the VA can better protect the individual’s information.

**Section 2. Uses of the Information**

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

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

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

VDIF’s purpose is to provide the information to internal (at this point) consumers/care givers. Specifically, VDIF provides a software middleware infrastructure for VistA applications to pass data between each other. Name: used as identifier Social security number: used as identifier Date of birth: used as identifier Email addresses: used as identifier Mailing address, zip code, phone number: used to contact individual Health insurance beneficiary numbers account numbers: used as identifier Current medications, and previous medical records: used as identifier

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.

VDIF only displays information and has no ability to analyze data.

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.

VDIF only displays information and has no ability to analyze data.

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?

These controls are inherited from the hosting facility.

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

N/A

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

The security controls for the VDIF application cover approximately 17 security areas regarding protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. The VDIF application team has implemented the required security controls based on the tailoring guidance of NIST Special Publication 800-53 Rev 4 and VA directives or handbooks. VA Records Management Policy VA 6300.1, VA 6500 HB, National Rules of Behavior (ROB), and VA
6502.1, VA6502.3, VA 6502.4 Privacy Policies govern how veterans’ information is used, stored, and protected including all data at rest and data in transit are encrypted.

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.

The System of Record Notice (SORN) (i.e., Medical Record-VA: 24VA10A7) defines the information collected from veterans, use of the information, and how the information is accessed and stored.

The security controls for the VDIF application cover approximately 17 security areas regarding protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. The VDIF application team has implemented the required security controls based on the tailoring guidance of NIST Special Publication 800-53 Rev 4 and VA directives or handbooks. VA Records Management Policy VA 6300.1, VA 6500 HB, National Rules of Behavior (ROB), and VA 6502.1, VA6502.3, VA 6502.4 Privacy Policies govern how veterans’ information is used, stored, and protected.

At VAEC, users must fill out the 9957 or ePAS form to gain access, which gets approved by their department supervisor.

- Guest/anonymous and temporary accounts don’t exist. These are manager approved individual accounts, service accounts for monitoring and applications (such as: WebLogic, Patrol, Nagios and Oracle) and group accounts users can run commands as.
- Group accounts are built in as part of the install routine; there are open 9957 or ePAS tickets for those accounts. Individual users are later defined as a member of the group.
- 9957’s or ePAS are used when creating accounts and granting appropriate access.
• 9957’s or ePAS are used to gather appropriate approvals for access.
• System administrators manage all accounts through Super User DO (sudo; a Linux command line interface command) access. They provision accounts only upon a 9957, ePAS or appropriate SDM or incident ticket.
• Temporary accounts and “need-to-know” changes aren’t applicable. For terminations and transfers, the ePAS process makes sure all access changes are handled.
• Account deletions may come by SDM or incident ticket if they are inactive for 180 days or ePAS /9957 form.
• The 9957 / ePAS process covers expected usage, necessary access, etc.
• Accounts are reviewed by system administrators.

2.4a How is access to the PII determined?

At VAEC, users must fill out the 9957 or ePAS form to gain access, which gets approved by their department supervisor. • Guest/anonymous and temporary accounts don’t exist. These are manager approved individual accounts, service accounts for monitoring and applications (such as: WebLogic, Patrol, Nagios and Oracle) and group accounts users can run commands as. • Group accounts are built in as part of the install routine; there are open 9957 or ePAS tickets for those accounts. Individual users are later defined as a member of the group. • 9957’s or ePAS are used when creating accounts and granting appropriate access. • 9957’s or ePAS are used to gather appropriate approvals for access. • System administrators manage all accounts through Super User DO (sudo; a Linux command line interface command) access. They provision accounts only upon a 9957, ePAS or appropriate SDM or incident ticket. • Temporary accounts and “need-to-know” changes aren’t applicable. For terminations and transfers, the ePAS process makes sure all access changes are handled. • Account deletions may come by SDM or incident ticket if they are inactive for 180 days or ePAS /9957 form. • The 9957 / ePAS process covers expected usage, necessary access, etc. • Accounts are reviewed by system administrators.

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

At VAEC, users must fill out the 9957 or ePAS form to gain access, which gets approved by their department supervisor. • Guest/anonymous and temporary accounts don’t exist. These are manager approved individual accounts, service accounts for monitoring and applications (such as: WebLogic, Patrol, Nagios and Oracle) and group accounts users can run commands as. • Group accounts are built in as part of the install routine; there are open 9957 or ePAS tickets for those accounts. Individual users are later defined as a member of the group. • 9957’s or ePAS are used when creating accounts and granting appropriate access. • 9957’s or ePAS are used to gather appropriate approvals for access. • System administrators manage all accounts through Super User DO (sudo; a Linux command line interface command) access. They provision accounts only upon a 9957, ePAS or appropriate SDM or incident ticket. • Temporary accounts and “need-to-know” changes aren’t applicable. For terminations and transfers, the ePAS process makes sure all access changes are handled. • Account deletions may come by SDM or incident ticket if they are inactive for 180 days or ePAS /9957 form. • The 9957 / ePAS process covers expected usage, necessary access, etc. • Accounts are reviewed by system administrators.
2.4c Does access require manager approval?

Yes

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

Yes, all VDIF-EP PII data is automatically monitored, tracked, and recorded at the VA Enterprise level as it traverses the network, and all users must have completed an approved EPAS document signed by their supervisor for access to PII data.

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

VDIF-EP users who have access to view the PHI/PII assuring safeguards responsibility rests with the systems which accessed on holds the information.

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

VDIF retains logging information for auditing purposes only. The information retained is user's login identifier, user ID, name of user, query action, user's unique CAC or PIV ID, start and end timestamps, date of audit, and IP address of machine where user is logged in.

Name
Email address
IP address

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.
VDIF is not an archival system. The VDIF system/application does not store PII long-term. All PII maintained in a Privacy Act system of records has a retention period identified in the SORN (i.e., Medical Record-VA: 24VA10A7) which is published in the Federal Register. VHA retains the accounting of disclosures for seventy-five (75) years after the last episode of patient care and then destroyed/or deleted.

Record disposition refers to the transfer of records to a records storage facility, transfer of permanent records to the National Archives, the destruction of records, and other appropriate actions to dispose of records. The Record Control Schedule (RCS) 10-1 contains retention and disposition requirements for VHA records which have been authorized by NARA or have been assigned a General Record Schedule (GRS) disposal authority.

The VHA RCS 10-1 is the main authority for the retention and disposition requirements of VHA records. It provides a brief description of the records, states the retention period and disposition requirements. The actual defined period will be different depending on the specific record type. VHA health care facilities do not set record retention periods or disposition authority for PII, nor do they set policy for data destruction. VHA health care facilities are to comply with the VHA RCS 10-1.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)?

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner. Please work with the system Privacy Officer and VA Records Officer to answer these questions. This question is related to privacy control DM-2, Data Retention and Disposal.

3.3a Are all records stored within the system of record indicated on an approved disposition authority?

The archived audit logs are kept for six years as required by the accounting for disclosure provisions of the Privacy Act, the HIPAA Privacy Rule, and Freedom of Information Act as outlined in paragraph 35c (4) of VA Handbook 1605.1. Records control schedule (RCS) 10-1 provides the parameters for retention and destruction of data. RCS 10-1 is approved by NARA.

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

The archived audit logs are kept for six years as required by the accounting for disclosure provisions of the Privacy Act, the HIPAA Privacy Rule, and Freedom of Information Act as outlined in paragraph 35c (4) of VA Handbook 1605.1. Records control schedule (RCS) 10-1 provides the parameters for retention and destruction of data. RCS 10-1 is approved by NARA.

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.

Paper documents are destroyed to an unreadable state in accordance with the Department of Veterans’ Affairs VA Directive 6371, (April 8, 2014), https://www.va.gov/vapubs/search_action.cfm?dType=1

Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with the Department of Veterans’ Affairs Directive 6500, VA Cybersecurity Program (January 23, 2019), https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=1003&FType=2. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction per VA Handbook 6500.1. Digital media is shredded or sent out for destruction per VA Handbook 6500.1.

Additionally, VDIF follows Field Security Service (FSS) Bulletin #176 dated April 9, 2014 for Media Sanitization Program, SOPs - FSS - All Documents as well as FSS Standard Operating Procedures (SOP) MP-6 Electronic Media Sanitization.

3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

VA prohibits the use of PII/PHI in testing, research and training in VA Handbook 6500, Annex E.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).
While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

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

**Principle of Minimization:** Does the project retain only the information necessary for its purpose? Is the PII retained only for as long as necessary and relevant to fulfill the specified purposes?

**Principle of Data Quality and Integrity:** Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged? This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:

**Privacy Risk:** The risk to maintaining data with VDIF is the longer time frame information is kept, the greater the risk that the information can possibly be compromised or breached along with add IT costs.

**Mitigation:** To mitigate the risk posed by information retention, VDIF adheres to the VA RCS schedules for each category or data it maintains. When the retention data is reached for a record, the medical center will carefully dispose of the data by the determined method as described in question 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

<table>
<thead>
<tr>
<th>Internal Organization Name</th>
<th>IT System Name</th>
<th>Specifically list the Data Elements</th>
<th>Method of Transmission</th>
</tr>
</thead>
<tbody>
<tr>
<td>VA Master Person Index</td>
<td>MPI</td>
<td>VA eHealth Exchange queries need to be in a synchronous mode. The OMG PIDS specification defines this feature/interface as an operation that returns the IDs in the destination ID Domains that correspond to the ID passed in. In the VA IdM Service we define the VA ID Domain to include any of the SourceID that correlate to VA Enterprise Identifier (ICN).</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Veterans Health Information Systems and Technology Architecture</td>
<td>VistA</td>
<td>Users login identifier, User ID, Name of User, Patient’s Identifier (Edipi), Query Action - what widgets the user accesses within Veteran EHR, Start and End Timestamps, Date of Audit, IP Address of Machine Where User is Logged In</td>
<td>HSBus</td>
</tr>
<tr>
<td>VDIF Web Service Layer VIA</td>
<td>VWSL VIA</td>
<td>The VHIE Portal manages a Patient's Consent, also known as the Patient's</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Internal Organization Name</td>
<td>IT System Name</td>
<td>Specifically list the Data Elements</td>
<td>Method of Transmission</td>
</tr>
<tr>
<td>----------------------------</td>
<td>----------------</td>
<td>--------------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Participation Preferences (PPP) and the requests for generating Clinical Document Architecture (CDA)-type documents for selected Veterans, as well as generate and display Health Information Exchange (HIE) and Consent reports.</td>
<td></td>
</tr>
<tr>
<td>Identity Management</td>
<td>IDM</td>
<td>The Initiate Correlation of Patient Identities business process is an existing process owned by the Identity Management group. This process correlates identities between VA patients and identities known in other partners.</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Data Access Service (DAS)</td>
<td>VLER/VHIE DAS</td>
<td>C32- Summarization of Episode Note: Health summary data sharing to store for access by other VA systems.</td>
<td>Representational State Transfer (REST) Web Services over HTTPS and SFTP</td>
</tr>
<tr>
<td>Security Access Control (SAC)/ Policy Decision Point (PDP)</td>
<td>SAC PDP</td>
<td>Stores Enterprise Policies for Security and Privacy. Renders authorization decision on data sharing based on requestor information and Veteran Preferences</td>
<td>HTTPS</td>
</tr>
<tr>
<td>EO Technical Security Office/QRadar SIEM</td>
<td>EO Technical Security Office/QRadar SIEM</td>
<td>Users login identifier, User ID, Name of User, Patient’s Identifier (EDIP), Query Action - what widgets the user</td>
<td>Messages will be encrypted using two-way SSL at the HTTPS transport/session</td>
</tr>
<tr>
<td>Internal Organization Name</td>
<td>IT System Name</td>
<td>Specifically list the Data Elements</td>
<td>Method of Transmission</td>
</tr>
<tr>
<td>----------------------------</td>
<td>----------------</td>
<td>-------------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>accesses within Veteran EHR, Start and End Timestamps, Date of Audit, IP Address of Machine Where User is Logged In</td>
<td>layer and via IP/Port identification at the network layer.</td>
</tr>
<tr>
<td>Bed Management Solution</td>
<td>Bed Management Solution</td>
<td>BMS communicates with VistA and Cerner through VDIF to capture bed, patient, admission, transfer, and discharge information.</td>
<td>HL7</td>
</tr>
<tr>
<td>Community Care Document Imaging</td>
<td>Community Care Document Imaging</td>
<td>Patient Imaging, Summary Document Architecture</td>
<td>SSL/TLS</td>
</tr>
<tr>
<td>Corporate Data Warehouse</td>
<td>Corporate Data Warehouse</td>
<td>Users login identifier, User ID, Name of User, Patient’s Identifier (EDIPI), Query Action - what widgets the user accesses within Veteran EHR, Start and End Timestamps, Date of Audit, IP Address of Machine Where User is Logged In</td>
<td>SFTP / Port 22</td>
</tr>
<tr>
<td>eHealth Exchange</td>
<td>eHealth Exchange</td>
<td>Users login identifier, User ID, Name of User, Patient’s Identifier (EDIPI), Query Action - what widgets the user accesses within Veteran EHR, Start and End Timestamps, Date of Audit, IP Address of Machine Where User is Logged In</td>
<td>SSL/TLS</td>
</tr>
<tr>
<td>Enrollment System</td>
<td>Enrollment System</td>
<td>Service that provides a Veteran's preferred facility.</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Internal Organization Name</td>
<td>IT System Name</td>
<td>Specifically list the Data Elements</td>
<td>Method of Transmission</td>
</tr>
<tr>
<td>---------------------------------------------------------------</td>
<td>-------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>Veterans Enterprise Terminology Services</td>
<td>Veterans Enterprise Terminology Services</td>
<td>VETS translates clinical data terminology between different applications. For example, VETS is used by VDIF when assembling a CCD, C32 or a C62 document for trusted, external healthcare partners.</td>
<td>HTTPS</td>
</tr>
<tr>
<td>Collaborative Terminology Tooling and Data Management</td>
<td>Collaborative Terminology and Data Management</td>
<td>CTT&amp;DM translates clinical data terminology between different applications. For example, CTT&amp;DM is used by VDIF when assembling a CCD, C32 or a C62 document for trusted, external healthcare partners.</td>
<td>HTTPS</td>
</tr>
<tr>
<td>EDI</td>
<td>Electronic Data Interchange</td>
<td>PHI and PII which includes name, Social Security Number, date of birth, address, email, and any and all Veteran health information available in VistA.</td>
<td>SFTP SSH</td>
</tr>
</tbody>
</table>

### 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 SPI within the Department of Veterans’ Affairs is that the data may be disclosed to individuals who do not require access or
have a need to know. Inappropriate/unauthorized disclosure heightens the threat of the information being misused.

**Mitigation:** The system logs are securely maintained in the QRadar event management system under EO management. The only information shared internally is audit log information recording which users accessed patient information using VDIF. Access to the audit logs is limited to only personnel with a security related job function and auditors.

**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
<table>
<thead>
<tr>
<th>System Name</th>
<th>External Organization or Agency Name</th>
<th>Specifically list the Data Elements Shared/Received</th>
<th>Type of Connection</th>
<th>Agreement Type (Can be more than one)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDC</td>
<td>CDC IZ Gateway</td>
<td>Immunization Records</td>
<td>SSL/TLS</td>
<td>MOU/ISA</td>
</tr>
<tr>
<td>Centers for Disease Control and Prevention (CDC) Center for Surveillance, Epidemiology, and Laboratory Services (CSELS), Division of Health Informatics and Surveillance (DHIS) - BioSense</td>
<td>CDC</td>
<td>Limited Data Set De-identified patient encounter data, The ability to cache the federated patient data reduces the impact on Vista systems and dramatically improve response times to internal as well as external partners.</td>
<td>PPSM</td>
<td>MOU/ISA</td>
</tr>
<tr>
<td>CDC COVID19 Response Monitoring and Assessment Team - CDC COVID-19 Vaccination Reporting Specification (CVRS)</td>
<td>CDC</td>
<td>Improves access to VistA data by federating patient record data at a national level. The ability to cache the federated patient data reduces the impact on Vista systems and dramatically improve response times to internal as well as external partners.</td>
<td>SSL/TLS</td>
<td>MOU/ISA</td>
</tr>
<tr>
<td>Associated Regional and University Pathologists (ARUP) National Laboratories - ARUP</td>
<td>ARUP Laboratory Data Sharing and Interoperability (ARUP LDSI)</td>
<td>Veteran’s eHR and associated documents.</td>
<td>Site-to-Site VPN Tunnel</td>
<td>National MOU/ISA</td>
</tr>
<tr>
<td>Defense Medical</td>
<td>DMLSS</td>
<td>Improves access to VistA data by</td>
<td>SSL/TLS</td>
<td>MOU/ISA</td>
</tr>
<tr>
<td>System Name</td>
<td>External Organization or Agency Name</td>
<td>Specifically list the Data Elements Shared/Received</td>
<td>Type of Connection</td>
<td>Agreement Type (Can be more than one)</td>
</tr>
<tr>
<td>-------------------------------------------------</td>
<td>--------------------------------------</td>
<td>----------------------------------------------------</td>
<td>--------------------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td>Logistics Standard Support (DMLSS)</td>
<td></td>
<td>federating patient record data at a national level. The ability to cache the federated patient data reduces the impact on Vista systems and dramatically improve response times to internal as well as external partners.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Joint Health Information Exchange</td>
<td>Joint Health Information Exchange</td>
<td>Veteran’s eHR and associated documents.</td>
<td>HTTPS</td>
<td>MOU/ISA</td>
</tr>
<tr>
<td>Cerner Millennium</td>
<td>Cerner Millennium (OPENLink)</td>
<td>Veteran’s eHR and associated documents.</td>
<td>SSL/TLS</td>
<td>MOU/ISA</td>
</tr>
<tr>
<td>EHRM SFTP Server</td>
<td>EHRM SFTP Server</td>
<td>Veteran’s eHR and associated documents.</td>
<td>SFTP</td>
<td>MOU/ISA</td>
</tr>
<tr>
<td>DoD Laboratory Data Sharing and Interoperability</td>
<td>DoD Laboratory Data Sharing and Interoperability (DoD LDSI)</td>
<td>Veteran’s eHR and associated documents.</td>
<td>SSL/TLS</td>
<td>MOU/ISA</td>
</tr>
<tr>
<td>DoD Life Design Station International, Inc. (LDSI)</td>
<td>LDSI</td>
<td>PHI and PII which includes name, Social Security Number, date of birth, address, email, and any and all Veteran health information available in VistA.</td>
<td>SSL/TLS</td>
<td>MOU/ISA</td>
</tr>
<tr>
<td>DoD to VA CHDR</td>
<td>DoD to VA CHDR</td>
<td>PHI and PII which includes name, Social Security Number, date of birth, address, email, and any and all Veteran health information available in VistA.</td>
<td>SSL/TLS</td>
<td>MOU/ISA</td>
</tr>
<tr>
<td>System Name</td>
<td>External Organization or Agency Name</td>
<td>Specifically list the Data Elements Shared/Received</td>
<td>Type of Connection</td>
<td>Agreement Type (Can be more than one)</td>
</tr>
<tr>
<td>-------------</td>
<td>--------------------------------------</td>
<td>-----------------------------------------------------</td>
<td>--------------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>information available in VistA.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Appriss Health to VDIF</td>
<td>Appriss Health to VDIF</td>
<td>PHI and PII which includes name, Social Security Number, date of birth, address, email, and any and all Veteran health information available in VistA.</td>
<td>HTTPS</td>
<td>MOU/ISA</td>
</tr>
<tr>
<td>LVS</td>
<td>Legacy Viewer Sustainment</td>
<td>PHI and PII which includes name, Social Security Number, date of birth, address, email, and any and all Veteran health information available in VistA.</td>
<td>SFTP SSH</td>
<td>MOU/ISA</td>
</tr>
</tbody>
</table>

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:** The possibility exists for an authorized user to capture a screen shot of the disseminated information and the information to be disseminated to unauthorized personnel which heightens the threat of the information being misused. Additionally, the possibility exists that PHI data protected under 38 U.S. Code § 7332 can be accessed through the system without the prior written consent of the patient required by statute.

**Mitigation:** The Office of Information & Technology (OIT) has created the VA National Rules of Behavior which codifies the responsibilities and expected behavior of all VA personnel (employees and contractors) when accessing either VA information systems or sensitive information. All personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the Rules 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 VAs Talent Management System (TMS). After the user’s initial acceptance of the Rules, the user must reaffirm their acceptance annually as part of the security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system. For contractors, there is the VAs Contractors Rules of Behavior 7332 Protected Data.

**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.

No

6.1b If notice was not provided, explain why. If it was provided, attach a copy of the current notice.
No

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

The Department of Veterans Affairs does provide public notice that the system does exist. This notice is provided in 2 ways: 1) The System of record Notice (SORN) 24VA10A7 - Patient Medical Records dated 8/14/2014. The SORN can be found online at: https://www.oprm.va.gov/privacy/systems_of_records.aspx NOTIFICATION PROCEDURE: An individual who wishes to determine whether a record is being maintained in this system under his or her name or other personal identifier, or wants to review the contents of such record, should submit a written request or apply in person to the last VA healthcare facility where care was rendered. Addresses of VA health care facilities may be found in VA Appendix 1 of the Biennial Publication of Privacy Act Issuances. All inquiries must reasonably describe the portion of the medical record involved and the place and approximate date that medical care was provided. Inquiries should include the patient’s full name, social security number, and return address. 2) This Privacy Impact Assessment (PIA) also serves as notice of the System Oriented Architecture. 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.” VDIF does not collect information directly from the individual.

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.

VHA Directive 1605.1 Appendix D ‘Privacy and Release Information’, section 5 lists the rights of the Veterans to request VHA to restrict the uses and/or disclosures of the individual’s individually-identifiable health information to carry out treatment, payment, or health care operations. The Veterans have the right to refuse to disclose their SSN to VHA. The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VHA an SSN (see 38 CFR 1.575(a)).

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?
This question is directed at whether an individual may provide consent for specific uses or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent.

When a Veteran seeks enrollment into VA’s Healthcare System, information is collected from Veterans or their representative during registration; check in for clinic appointments, and other encounters or interactions with the Veteran. Individuals are providing consent for VA to use relevant authoritative sources of information to establish Healthcare Benefits eligibility and receive resulting ongoing healthcare. The Veteran’s information is provided during enrollment and populated in VistA. VHA has itemized consent for specific uses of data such as for human subject research (See VA Form 10-0493). Consent may be verbal at the point of PII collection or could be obtained on an informed consent document, other data collection forms, such as the 10-10EZ, or an authorization form.

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:** If there is insufficient notice, the veteran will not have enough information on why the PII is being collected and what course of action is available to take regarding his or her privacy.

**Mitigation:** VHA provides effective notice regarding collection, use, sharing, safeguarding, maintenance and disposal of PII, authority for collecting PII and the ability to access or amended PII through its Privacy Act SORNs. In addition, the VHA Notice of Privacy Practices (NOPP) provides notice on privacy practices including collection, use and disclosure of PII and PHI and privacy rights such as the ability to access and amendment. The VHA NOPP is provided to newly enrolled Veterans upon enrollment and currently enrolled Veterans annually. VHA also provides notice on the authority for collecting PII and choices regarding the PII at the point of collection. VHA permits individuals to agree to the collection of their PII by paper and electronic forms that include Privacy Act Statements outlining why the information is being collected, how it will be used and what system of records the information will be stored. The Privacy Act Statements on the paper and electronic forms explain whether data collection is mandatory or
voluntary and explains the consequences of not providing the information when data collection is voluntary. In addition, information is collected verbally from individuals. These individuals are made aware of why data is collected through the VHA NOPP and conversations with VHA employees. This Privacy Impact Assessment (PIA) also serves as notice of the System Oriented Architecture. 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.”

**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 (patients) are not given access to their information in VDIF. VDIF system data is for use by medical service providers only. Individuals wishing to obtain more information about access, redress and record correction of their patient medical records, should contact the Department of Veteran’s Affairs regional office as directed in the System of Record Notice (SORN) 24VA10A7 - Patient Medical Records which can be found online at: https://www.oprm.va.gov/privacy/systems_of_records.aspx.

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).

N/A

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 (patients) are not given access to their information in VDIF. VDIF system data is for use by medical service providers only.
Individuals wishing to obtain more information about access, redress and record correction of their patient medical records, should contact the Department of Veteran’s Affairs regional office as directed in the System of Record Notice (SORN) 24VA10A7.

The System of record Notice (SORN) 24VA10A7 - Patient Medical Records dated 8/14/2014. The SORN can be found online at: https://www.gpo.gov/fdsys/pkg/FR-2014-08-14/pdf/2014-19283.pdf

NOTIFICATION PROCEDURE: An individual who wishes to determine whether a record is being maintained in this system under his or her name or other personal identifier, or wants to review the contents of such record, should submit a written request or apply in person to the last VA healthcare facility where care was rendered. Addresses of VA health care facilities may be found in VA Appendix 1 of the Biennial Publication of Privacy Act Issuances. All inquiries must reasonably describe the portion of the medical record involved and the place and approximate date that medical care was provided. Inquiries should include the patient’s full name, social security number, and return address.

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

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

This would have occurred at the point of collection, VistA. Any corrections to their data would be done at the source system, the enrollment system through existing processes. Veterans can correct data within those systems by submitting a form 1010 EZR. Veterans already enrolled in the VA Health system can correct data by submitting VA form 10-10 EZR. Mail the original application and supporting materials to the Health Eligibility Center, 2957 Claremont Road, Suite 200 Atlanta, GA 30329.

More information on VA form 10-10 EZR can be found at: https://www.va.gov/vaforms/medical/pdf/vha-10-10ezrfill.pdf

The System of record Notice (SORN) 24VA10A7 - Patient Medical Records dated 8/14/2014. The SORN can be found online at: https://www.gpo.gov/fdsys/pkg/FR-2014-08-14/pdf/2014-19283.pdf

NOTIFICATION PROCEDURE: An individual who wishes to determine whether a record is being maintained in this system under his or her name or other personal identifier, or wants to review the contents of such record, should submit a written request or apply in person to the last VA healthcare facility where care was rendered. Addresses of VA health care facilities may be found in VA Appendix 1 of the Biennial Publication of Privacy Act Issuances. All inquiries must reasonably describe the portion of the medical record involved and the place and approximate date that medical care was provided. Inquiries should include the patient’s full name, social security number, and return address.
7.3 How are individuals notified of the procedures for correcting their information?

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

Veterans already enrolled in the VA Health system can correct data by submitting VA form 10-10 EZR. Mail the original application and supporting materials to the Health Eligibility Center, 2957 Clairmont Road, Suite 200 Atlanta, GA 30329. Veterans are notified by mail regarding correction of information. They can also call the Vets.gov Help Desk at 855-574-7286, Monday through Friday, 8am-8pm (ET) for further assistance.

More information on VA form 10-10 EZR can be found at: https://www.va.gov/vaforms/medical/pdf/vha-10-10ezrfill.pdf

Individuals wishing to obtain more information about access, redress and record correction of their patient medical records, should contact the Department of Veteran’s Affairs regional office as directed in the System of Record Notice (SORN) 24VA10A7 - Patient Medical Records which can be found online at the links noted is section 6.1 above.

This would have occurred at the point of collection, VistA.

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

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

Formal redress is provided in SORN 24VA10A7 (Formerly 24VA136). Individuals seeking information regarding access to and contesting of VA medical records may write, call, or visit the last VA facility where medical care was provided as directed in the System of Record Notice (SORN) 24VA10A7 - Patient Medical Records which can be found online at the links noted is section 6.1 above.
Veterans already enrolled in the VA Health system can correct data by submitting VA form 10-10 EZR. Mail the original application and supporting materials to the Health Eligibility Center, 2957 Clairmont Road, Suite 200 Atlanta, GA 30329.

More information on VA form 10-10 EZR can be found at: https://www.vets.gov/healthcare/apply

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 a Veteran could accidentally provide incorrect information to the VA when enrolling for health benefits and that incorrect information could be disseminated by VDIF.

Mitigation: Veterans can update their enrollment information in the source systems using VA form 1010EZR or by following the instructions in SORN 24VA10A7 (Formerly 24VA136).

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.

Individuals (patients) are not given access to their information in VDIF. VDIF system data is for use by medical service providers only. Individuals wishing to obtain more information about access, redress and record correction of their patient medical records, should contact the Department of Veteran’s Affairs regional office as directed in the System of Record Notice (SORN) 24VA10A7 - Patient Medical Records which can be found online at: https://www.oprm.va.gov/privacy/systems_of_records.aspx.

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?

VA contract employee access is verified through the Contracting Officer’s Representative (COR) and other VA supervisory/administrative personnel before access is granted to any VA system. Contractor access is reviewed annually at a minimum. 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 Talent Management System (TMS). All contractors are vetted using the VA background investigation process and must obtain the appropriate level background investigation for their role. Contractors with systems administrative access are required to complete additional role-based training prior to gaining system administrator access. Generally, contracts are reviewed at the start of the initiation phase of acquisitions and again during procurement of option years by the Contracting Officer, Information Security Officer, Privacy Officer, COR, Procurement Requestor/Program Manager and any other stakeholders required for approval of the acquisition. Contracts generally have an average duration of 1-3 years and may have option years stipulated in the original contract.

8.1c 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.

Per VA Directive and Handbook 6330, every 5 years the Office of Information Technology (OIT) develops, disseminates, and reviews/uploads a formal, documented policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; along with formal, documented procedures to facilitate the implementation of the control policy and associated controls.

OIT documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and retains individual training records. This documentation and monitoring are performed by TMS.

VDIF enforces approved authorizations for logical access to information systems. Logical access to all VA information systems are based on a demonstrated need; the concepts of least privilege and separation of duties; and granted in accordance with policy. System access is granted based on VA background investigations; special access and IT position designations and requirements;
and appropriate security clearance and nondisclosure agreements as required for access to VA sensitive information. For access control, VDIF uses two-factor authentication. All authorized users (government, military, and contractor personnel) must authenticate using an active credential, i.e., DOD CAC or VA PIV credential.

At VAEC, users must fill out the 9957 or ePAS form to gain access, which gets approved by their department supervisor.

- Guest/anonymous and temporary accounts don’t exist. There are individual accounts, service accounts for monitoring and applications (WebLogic, Patrol, Nagios and Oracle) and group accounts users can run commands as.

- Group accounts are built in as part of the install routine; there are open 9957 or ePAS tickets for those accounts. Individual users are later defined as a member of the group. • 9957’s ePAS are used when creating accounts and granting appropriate access.

- 9957’s or ePAS are used to gather appropriate approvals for access.

- System administrators manage all accounts through SUDO. They provision accounts only upon an ePAS or appropriate SDM / incident ticket.

- Temporary accounts and “need-to-know” changes aren’t applicable. For terminations and transfers, the 9957 or ePAS process makes sure all access changes are handled.

- Account deletions may come by SDM or incident ticket if they are inactive for 180 days or 9957 or ePAS form.

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.

VA contract employee access is verified through the Contracting Officer’s Representative (COR) and other VA supervisory/administrative personnel before access is granted to any VA system. Contractor access is reviewed annually at a minimum. 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 Talent Management System (TMS). All contractors are vetted using the VA background investigation process and must obtain the appropriate level background
investigation for their role. Contractors with systems administrative access are required to complete additional role-based training prior to gaining system administrator access. Generally, contracts are reviewed at the start of the initiation phase of acquisitions and again during procurement of option years by the Contracting Officer, Information Security Officer, Privacy Officer, COR, Procurement Requestor/Program Manager and any other stakeholders required for approval of the acquisition. Contracts generally have an average duration of 1-3 years and may have option years stipulated in the original contract.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PHI 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 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 ROB, 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.

System administrators are required to complete additional role-based training. Users with access to PHI are required to complete HIPAA privacy training annually.

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

8.4a If Yes, provide:

1. The Security Plan Status: Approved
2. The System Security Plan Status Date: December 21, 2022
3. The Authorization Status: ATO
4. The Authorization Date: April 15, 2022
5. The Authorization Termination Date: April 15, 2023
6. The Risk Review Completion Date: December 5, 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)

VAEC is currently in use.

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**

<table>
<thead>
<tr>
<th>ID</th>
<th>Privacy Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>AP</td>
<td><strong>Authority and Purpose</strong></td>
</tr>
<tr>
<td>AP-1</td>
<td>Authority to Collect</td>
</tr>
<tr>
<td>AP-2</td>
<td>Purpose Specification</td>
</tr>
<tr>
<td>AR</td>
<td><strong>Accountability, Audit, and Risk Management</strong></td>
</tr>
<tr>
<td>AR-1</td>
<td>Governance and Privacy Program</td>
</tr>
<tr>
<td>AR-2</td>
<td>Privacy Impact and Risk Assessment</td>
</tr>
<tr>
<td>AR-3</td>
<td>Privacy Requirements for Contractors and Service Providers</td>
</tr>
<tr>
<td>AR-4</td>
<td>Privacy Monitoring and Auditing</td>
</tr>
<tr>
<td>AR-5</td>
<td>Privacy Awareness and Training</td>
</tr>
<tr>
<td>AR-7</td>
<td>Privacy-Enhanced System Design and Development</td>
</tr>
<tr>
<td>AR-8</td>
<td>Accounting of Disclosures</td>
</tr>
<tr>
<td>DI</td>
<td><strong>Data Quality and Integrity</strong></td>
</tr>
<tr>
<td>DI-1</td>
<td>Data Quality</td>
</tr>
<tr>
<td>DI-2</td>
<td>Data Integrity and Data Integrity Board</td>
</tr>
<tr>
<td>DM</td>
<td><strong>Data Minimization and Retention</strong></td>
</tr>
<tr>
<td>DM-1</td>
<td>Minimization of Personally Identifiable Information</td>
</tr>
<tr>
<td>DM-2</td>
<td>Data Retention and Disposal</td>
</tr>
<tr>
<td>DM-3</td>
<td>Minimization of PII Used in Testing, Training, and Research</td>
</tr>
<tr>
<td>IP</td>
<td><strong>Individual Participation and Redress</strong></td>
</tr>
<tr>
<td>IP-1</td>
<td>Consent</td>
</tr>
<tr>
<td>IP-2</td>
<td>Individual Access</td>
</tr>
<tr>
<td>IP-3</td>
<td>Redress</td>
</tr>
<tr>
<td>IP-4</td>
<td>Complaint Management</td>
</tr>
<tr>
<td>SE</td>
<td><strong>Security</strong></td>
</tr>
<tr>
<td>SE-1</td>
<td>Inventory of Personally Identifiable Information</td>
</tr>
<tr>
<td>SE-2</td>
<td>Privacy Incident Response</td>
</tr>
<tr>
<td>TR</td>
<td><strong>Transparency</strong></td>
</tr>
<tr>
<td>TR-1</td>
<td>Privacy Notice</td>
</tr>
<tr>
<td>TR-2</td>
<td>System of Records Notices and Privacy Act Statements</td>
</tr>
<tr>
<td>TR-3</td>
<td>Dissemination of Privacy Program Information</td>
</tr>
<tr>
<td>UL</td>
<td><strong>Use Limitation</strong></td>
</tr>
<tr>
<td>UL-1</td>
<td>Internal Use</td>
</tr>
<tr>
<td>UL-2</td>
<td>Information Sharing with Third Parties</td>
</tr>
</tbody>
</table>
Signature of Responsible Officials
The individuals below attest that the information provided in this Privacy Impact Assessment is true and accurate.

Margaret L. Pugh 104985
Digitally signed by Margaret L. Pugh
104985
Date: 2023.01.10 15:35:30 -05'00'

Privacy Officer, Margaret Pugh

Thomas J. Orler 178546
Digitally signed by Thomas J. Orler
178546
Date: 2023.01.12 11:22:03 -06'00'

Information System Security Officer, Thomas Orler

Christopher Brown 101386
Digitally signed by Christopher Brown
101386
Date: 2023.01.19 15:50:28 -06'00'

Information System Owner, Christopher Brown

JOHN WORSHAM (Affiliate)
Digitally signed by JOHN WORSHAM (Affiliate)
Date: 2023.02.02 11:30:56 -06'00'

Reviewed for accuracy by PIA Support Analyst
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).
HELPFUL LINKS:

Record Control Schedules:

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

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