Privacy Impact Assessment for the VA IT System called:

Blind Rehabilitation Services (BRS)

Clinical Ancillary
Office of the Assistant Deputy Under Secretary for Health for Patient Care Services

Date PIA submitted for review:

March 30, 2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Christian Loftus	Christian.Loftus@va.gov	859-281-2470
Information System Security Officer (ISSO)	Amine Messaoudi	Amine.Messaoudi@va.gov	202-815-9345
Information System Owner	Christopher Brown	Christopher.Brown1@va.gov	202-270-1432

Abstract

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

BRS serves as a registry that collects demographic and clinical data by providing enhanced tracking and reporting from Visual Impairment Services Team (VIST) Coordinators, Blind Rehabilitation Outpatient Specialists (BROS), Intermediate and Advanced Low Vision Clinics, Visual Impairment Services Outpatient Rehabilitation (VISOR) programs, and inpatient/residential Blind Rehabilitation Centers (BRCs). BRS creates, modifies, and tracks referrals in an electronic referral process to track patient applications for service, notifications feature to alert users of pending referrals, encounters/progress notes will be automatically created for assessments and field visits, nationwide centralization of BRS services data to allow nationwide reporting, ad-hoc reporting capabilities, allows the ability to track BRS patient care access across institutions, and patients can be referred or transferred to other institutions if they move without having to recreate patient data.

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:

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *Indicate the ownership or control of the IT system or project.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *A general description of the information in the IT system and the purpose for collecting this information.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *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.*
- *A citation of the legal authority to operate the IT system.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*
- *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?*

The Blind Rehabilitation Services (BRS) is a system owned and operated by the Department of Veterans Affairs (VA) under Patient Care Services and the product line is Clinical Ancillary. Clinical Ancillary provides a full lifecycle support for IT products enabling diagnostic and therapeutic services at VA. BRS coordinates a healthcare service delivery system that provides a continuum of care for blind and visually impaired veterans served by the VA, extending from their home environment to the local VA facility and to the appropriate rehabilitation setting. These services include adjustment to blindness counseling, patient and family education, benefits analysis, comprehensive residential inpatient training, outpatient rehabilitation services, the provision of assistive technology, and research that assists the veteran in acquiring the skills and capabilities necessary for development of personal

independence and emotional stability. BRS serves as a registry that collects demographic and clinical data by providing enhanced tracking and reporting from Visual Impairment Services Team (VIST) Coordinators, Blind Rehabilitation Outpatient Specialists (BROS), Intermediate and Advanced Low Vision Clinics, Visual Impairment Services Outpatient Rehabilitation (VISOR) programs, and inpatient/residential Blind Rehabilitation Centers (BRCs). This reduces the time to treat patients on-time and avoid the associated consequences and disabilities.

The Department of Veterans Affairs (VA) provides Blind and Visual Impairment Rehabilitation Services to eligible Veterans and active-duty Service members who have vision loss that cannot be corrected with regular eyeglasses and who are having difficulty with one or more tasks. These services assist the Veterans in developing the skills needed for personal independence and successful reintegration into the community and family environment. BRS is currently assisting approximately 235,000 Veterans.

The BRS environment resides within the VA Enterprise Cloud Amazon Web Services Government Cloud (VAEC AWS GovCloud). BRS collects information from internal VA sources and has no external connectivity outside of the VA.

The legal authority for this operating system is Title 38, United States Code (USC), Section 7301. The SORNs that relate to BRS:

- 79VA10 / 85 FR 84114 Veterans Health Information Systems and Technology Architecture (VistA) Records
  https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf

The completion of this PIA will not require changes to any business processes. BRS is currently migrating to the cloud from an on-prem environment that is unable to be upgraded in place.

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 Account Information
- ☐ Health Insurance Beneficiary Numbers
- Account numbers
- ☐ Certificate/License numbers
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☐ Current Medications
- ☐ Previous Medical Records
- ☒ Race/Ethnicity
- ☐ Tax Identification Number
- ☐ Medical Record Number
- ☒ Gender
- ☒ Integration Control Number (ICN)
- ☒ Military History/Service Connection
- ☐ Next of Kin
- ☒ Other Unique Identifying Information (list below):

- *Original VistA Institution/VistA Patient ID*
- *Spouse Name*
- *Dependent(s)Name*

PII Mapping of Components

Blind Rehabilitation Services (BRS) consists of **one (1)** key component (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **BRS** and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

Note: Due to the PIA being a public facing document, please do not include the server names in the table.

PII Mapped to Components

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
Amazon Oracle Database	Yes	Yes	Name, SSN, DOB, Personal Mailing Address, Personal Phone Number, Race/Ethnicity, Gender, Integration Control Number (ICN), Military	Patient Care	Only administrators have access to PII; data is encrypted at rest and in transit.

			History/Service Connection, VistA Patient ID, Spouse Name, Dependent Name, and Marital Status		

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

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?

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 1.3 indicate why the system is using this source of data.

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

This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

The information in BRS system is pulled from Veterans Health Information Systems and Technology Architecture (VistA), Master Person Index (MVI) instances and/or manually entered by VA medical and administrative staff directly from the individual.

The information that is pulled from VistA and MVI allows health information to be shared across Visual Impairment Services Team (VIST) Coordinators, Blind Rehabilitation Outpatient Specialists (BROS), Intermediate and Advanced Low Vision Clinics, Visual Impairment Services Outpatient Rehabilitation (VISOR) programs, and inpatient/residential Blind Rehabilitation Centers (BRCs).

1.3 How is the information collected?

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?

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.

This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

The information collected from VistA and MVI is electronically transferred to BRS, and the information collected from individuals is collected verbally in interviews and conversations with VA medical and administrative staff.

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

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.

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.

This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

Accuracy is checked by the source systems, VistA and MVI. Patient data within the system is maintained in the VistA instances and checks for updates are synched nightly. If the data was collected directly from the individual during their visit, the accuracy will be assumed to be accurate.

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

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

This question is related to privacy control AP-1, Authority to Collect

The Legal Authority for Operating this system is:

Title 38, United States Code (U.S.C.), Sections 7301: Functions of Veterans Health Administration; (a) There is in the Department of Veterans Affairs a Veterans Health Administration. The Under Secretary for Health is the head of the Administration. The Under Secretary for Health may be.
https://www.govinfo.gov/content/pkg/USCODE-2003-title38/pdf/USCODE-2003-title38-partV.pdf

System of Records Notice (SORN):

79VA10 / 85 FR 84114 Veterans Health Information Systems and Technology Architecture (VistA) Records – VA: This system maintains a variety of information on current and former VA employees, contractors, patients, members of their immediate family, and volunteers. The records include employee productivity information, patient medical information, computer access information, budget and supply information.
https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf

Additionally, the collection, processing, and dissemination of health information must follow the rules and regulations established by the: Health Insurance Portability and Accountability Act of

1996 (HIPAA), Pub. L. No. 104-191 (Aug. 21, 1996), (codified in scattered sections of title 42 U.S. Code) (full-text); 45 C.F.R. parts 160 and 164 (HIPAA Privacy and Security Rules). https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996

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.

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

Principle of Purpose Specification: Explain how the collection ties with the purpose of the underlying mission of the organization and its enabling authority.

Principle of Minimization: Is the information directly relevant and necessary to accomplish the specific purposes of the program?

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

Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?

This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

Privacy Risk:

In order to provide ongoing healthcare to the individual PII/PHI is collected and retained in the BRS database. If the information was accessed by an unauthorized individual or otherwise breached, personal and/or emotional harm or even identity theft may result.

Mitigation:

VA medical and administrative staff are careful to only collect the information necessary to assist in the care of the individual. By only collecting the minimum necessary information, VA is able to better protect the individual's information. Once collected, the information is transmitted using encryption and stored in secured servers behind VA firewalls.

The BRS system employ a variety of security measures designed to ensure that the information is not inappropriately disclosed or released. These measures include: access control, awareness and training, audit and accountability, configuration management, contingency planning, identification and authentication, incident response, physical and environmental protection. The system employs all security controls in the respective moderate impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in National Institute of Standards and Technology (NIST) Special Publication 800 - 37 and specific VA Directives.

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.

The BRS system uses the information collected to coordinate a healthcare service delivery system that provides a continuum of care for blind and visually impaired Veterans served by the VA. These services include adjustment to blindness counseling, patient and family education, benefits analysis, comprehensive residential inpatient training, outpatient rehabilitation services, the provision of assistive technology, and research that assists the Veteran in acquiring the skills and capabilities necessary for development of personal independence and emotional stability.

- Name: Used to identify the individual's medical records for real-time access and treatment.
- Social Security Number: Used to identify the individual.
- Date of Birth: Used to identify the individual.
- Personal Mailing Address: Used to identify and correspond with the individual.
- Personal Phone Number: Used to contact the individual.
- Race/Ethnicity: Used to identify the individual and demographic purposes.
- Gender: Used to identify the individual and demographic purposes.
- Integration Control Number: VA identifier linking records within the VA to internal/external sharing partners.
- Military History/Service Connection: Used to evaluate medical conditions that could be related to the location of military time served. It is also used to determine VA benefit and healthcare eligibility.
- VistA Patient ID: Used to identify the individual.
- Spouse Name: Used to determine benefit support and as an emergency contact person.
- Dependent(s)Name: Used to determine benefit support and as an emergency contact person.

2.2 What types of tools are used to analyze data and what type of data may be produced?

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.

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.

This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

- BRS receives information from MPI/MVI. The MPI/MVI system initiates the connection to BRS and sends the patient update information which BRS uses to update the subscribed patient's data.

- BRS utilizes multiple reports on both patient care and location as follows:
    - Roster list by facility
    - Additions to patient roster
    - Deceased Patient list
    - Inactive Patient list
    - Referral lists
    - Referral schedule
    - Patient Mailing Labels, by location
    - Print Individual Patient Records
    - Patient Eye Exam History
    - Referral History

2.3 How is the information in the system secured?

2.3a What measures are in place to protect data in transit and at rest?

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

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

This question is related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

The data in transit to and from BRS is secured through SSL encryption and host name verification. Data at rest, including SSNs, are controlled by database security policies at the host facility VAEC AWS. User access to the data is granted upon successful authentication against the Department of Veterans Affairs (VA) 2-Factor Authentication (2FA) using Singe Sign On Internal (SSOi) Web Agent with Secure Token Service (STS), only accessible on the VA Network to those users with a need-to-know basis will have access to the data.

2.4 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u> How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

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.

Access to the BRS system is obtained by submitting a request through the BRS office and appropriate roles are applied to the user based on job function. BRS enables least functionality and log access records are tracked in Amazon Oracle Database auditing utilities. Access to these utilities are controlled through Electronic Permission Access System (ePAS) and are approved by the respective manager.

The BRS application team has implemented the required security controls based on the tailoring guidance of National Institute of Standards and Technology (NIST) Special Publication 800-53 and VA directives or handbooks. VA Records Management Policy VA 6300.1, VA 6500 HB and the VA Rules of Behavior recorded in the Talent Management System (TMS), a VA annual training system, governs how Veterans' information is used, stored, and protected.

Following the NIST and VA policy guidance listed above, the separation of duties policy applied, allows BRS staff members to receive focused and recorded training that provides access only to the areas of the application that applies to their job task and responsibilities.

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.

All data elements from section 1.1 will be retained, these include:

- Name
- Social Security Number
- Date of Birth

- Personal Mailing Address
- Personal Phone Number
- Race/Ethnicity
- Gender
- Integration Control Number (ICN)
- Military History/Service Connection
- Original VistA Institution/Vista Patient ID
- Spouse Name
- Dependent(s) Name

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. If the system is using cloud technology, will it be following the NARA approved retention length and schedule?

The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.
This question is related to privacy control DM-2, Data Retention and Disposal.

Per Record Control Schedule 10-1 2000.2 - Information Technology Operations and Maintenance Records relate to the activities associated with the operations and maintenance of the basic systems and services used to supply the agency and its staff with access to computers and data telecommunications. Includes the activities associated with IT equipment, IT systems, and storage media, IT system performance testing, asset and configuration management, change management, and maintenance on network infrastructure. The information will be retained until 3 years after agreement, control measures, procedures, project activity, or transaction is obsolete, completed, terminated or superseded but longer retention is authorized if required for business use.

Per Record Control Schedule 10-1 2100.3 - System Access Records are created as part of the user identification and authorization process to gain access to systems. Records are used to monitor inappropriate systems access by users. The information is retained until 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so please indicate the name of the records retention schedule.

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner.

This question is related to privacy control DM-2, Data Retention and Disposal.

Yes, when managing and maintaining VA data and records BRS will follow the guidelines established in the NARA approved Department of Veterans Affairs Records Control Schedule (RCS)10-1.

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

3.4 What are the procedures for the elimination of SPI?

Explain how records are destroyed or eliminated at the end of the 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

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 VA Directive 6500 VA Cybersecurity Program **(**February 24, 2021) and VA Handbook 6500.1 Electronic Media Sanitization. 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. Digital media is shredded or sent out for destruction.

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. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?

This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research

Blind Rehab does not utilize PII for research, testing, or training in the lower environments. PII is only employed during the Pre-Prod and IOC research, testing, or training. In order to gain access to the Pre-Prod and IOC environments users are required to have requested access via a process the same as employed by production.

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.

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 BRS 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, BRS adheres to the disposition authority approved by the Archivist of the United States following National Archives Records Administration (NARA). When the retention date is reached for a record, the individual's information is carefully disposed of. The individual's information is carefully disposed of following the procedures listed in 3.4.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

NOTE: Question 3.9 (second table) on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system within VA with which information is shared.

State the purpose for the internal sharing. If you have specific authority to share the information, provide a citation to the authority.

For each interface with a system outside your program office, state what specific data elements (PII/PHI) are shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?

This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Veterans Health Information System and Technology Architecture (VistA)	Verification of patient identity and validity for patient care	Name, Social Security Number, Date of Birth, Personal Mailing Address, Personal Phone Number, Race/Ethnicity, and VistA Patient ID	Electronically pulled from VistA thru Computerized Patient Record System (CPRS) Hyper Text Transfer Protocol with Secure Sockets Layer (HTTPS) carrying Extensible Markup Language (XML)
Master Veterans Index (MVI)	Verification of patient identity and validity for patient care	Name, Social Security Number, Data of Birth, Personal Mailing Address, Personal Phone Number, and Race/Ethnicity	Record and Patient Management System (RPMS) by Health Level 7 (HL7) messages

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.

This question is related to privacy control UL-1, Internal Use.

Follow the format below:

Privacy Risk:

The privacy risk associated with sharing information 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 access request process utilizing Electronic Permission Access System (ePAS) mitigates the risk of inadvertently sharing or disclosing the information by assigning access permissions based on need-to-know. 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***	***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***	***List the method of transmission and the measures in place to secure data***

	office or IT system		***(can be more than one)***	
N/A	N/A	N/A	N/A	N/A

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum Of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.

Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.

This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

Privacy Risk:

Not Applicable

Mitigation:

Not Applicable

Section 6. Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an appendix. (A 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?

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. If notice was provided in the Federal Register, provide the citation.

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

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

This question is 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.

The Notice of Privacy Practice (NOPP) is a document which explains the collection and use of protected information to individuals applying for VHA benefits. A signed statement acknowledging that the individual read and understood the NOPP is scanned into each applicant's electronic file. When updates are made to the NOPP copies are mailed to all VHA beneficiaries. Employees and contractors are required to review, sign and abide by the National Rules of Behavior on an annual basis.

1) The SORN defines the information collected from Veterans, use of the information, and how the information is accessed and stored. 79VA10 / 85 FR 84114 Veterans Health Information Systems and Technology Architecture (VistA) Records.
2) This Privacy Impact Assessment (PIA) also serves as notice of the BRS system. As required by the Government Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means."

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

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached.

This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress

VA medical and administrative staff request only information necessary to provide ongoing healthcare for the individual. While an individual may choose not to provide information to the staff this will prevent them from obtaining the care/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

Any right to consent to particular uses of the information would be handled by the source systems, VistA and MVI.

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 ongoing healthcare.

VHA permits individuals to agree to the collection and to the consent to the use of their personally identifiable information (PII) through the use of paper and electronic forms that include Privacy Act Statements outlining why the information is being collected, how it will be used and what Privacy Act system of records the information will be stored. If the individual does not want their information collected or used then they do not sign the consent form. In addition, information is collected verbally from individuals. These individuals are made aware of why data is collected through the VHA Notice of Privacy Practices (NOPP) and conversations with VHA employees. VA Forms are reviewed by VHACO periodically to ensure compliance with various requirements including that Privacy Act Statements are on forms collecting personal information from Veterans or individuals. VHA uses PII and PHI only as legally permitted including obtaining authorizations were required.

Individuals have a right to restrict the disclosure and use of their health information and have a right to deny the use of their health information and/or Individually Identifiable Health Information (IIHI) and for the purpose of research. Individuals can request further limitations on other disclosures. A veteran, guardian or court appointed Power of Attorney can submit a request to the facility Privacy Officer to obtain information. The facility can approve or deny these requests. However, if the request to provide information is accepted the facility must conform to the restrictions

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.

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 BRS 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 on a yearly basis and periodic monitoring is performed to check that the signed acknowledgment form has been scanned into electronic records. Additional mitigation is provided by making the System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) 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?

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.

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).

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.

This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

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 health care facility where care was rendered.

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 VA medical records may write, call, or visit the last VA facility where medical care was provided.

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.

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.

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.

This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.

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.

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.

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

Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

Principle of Individual Participation: If access and/or correction is denied, then is the individual provided notice as to why the denial was made and how to challenge such a denial?

Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?

This question is related to privacy control IP-3, Redress.

Follow the format below:

Privacy Risk:

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

Mitigation:

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. They can also refer to the Notice of Privacy Practice (NOPP) that is provided to all Veterans which discusses the proper process for requesting an amendment to ones' records.

Also, by publishing this PIA, and the applicable SORNs, the VA makes the public aware of the unique status of applications and evidence files, such as those stored on the Virtual VA platform. Furthermore, this document and the SORN provide the point of contact for members of the public who have questions or concerns about applications and evidence files.

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?

Describe the process by which an individual receives access to the system.

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?

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.

This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.

Access is requested per VA policies utilizing Electronic Permission Access System (ePAS). Users submit access requests based on need to know and job duties. Supervisor and OIT approval must be obtained prior to access granted. These requests are submitted for VA employees, contractors and all outside agency requests and are processed through the appropriate approval processes.

8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please

describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII.

This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

Yes, contractors will have access to the system. BRS falls under the Health Services Development, Security, and Operations (DevSecOps) Support sustainment portfolio and contractors are responsible for maintaining the application Technical Reference Model (TRM), Fortify compliance as well as defect repair where applicable. WebLogic, and Database administrators are responsible for supporting the hardware and infrastructure on which BRS is deployed.

All contractors sign a Non-Disclosure Agreement (NDA) and are cleared using the VA background investigation process and must obtain a Moderate Background Investigation (MBI). This process is taken care of during the onboarding process of the BRS project.

Developers and Administrators with a need for elevated roles and access permissions are required to submit an Electronic Permission Access System (ePAS) request for access to the respective system and are only granted upon approval by the Supervisor and OIT prior to access granted. The contractors who provide support to the system are required to complete annual role-based training which is mandated for all BRS personnel with elevated privileges and is administrated through IT Workforce Development (ITWD). Annual privacy and security training is required for all BRS personnel and is administered through VA Talent Management System (TMS).

VA contracting performs reviews on contracts according to their Period of Performance defined within the existing/current contract.

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

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately.

This question is related to privacy control AR-5, Privacy Awareness and Training.

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

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

If Yes, provide:

1. *The Security Plan Status,*
2. *The Security Plan Status Date,*
3. *The Authorization Status,*
4. *The Authorization Date,*
5. *The Authorization Termination Date,*

6. *The Risk Review Completion Date,*
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH).*

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

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

Yes, the Security plan is currently uploaded to eMASS dated 12/15/2021. BRS has a 180-day ATO that was authorized on 01/28/2022 and expires on 07/27/2022. The Risk Review was completed on 01/03/2022. Per FIPS 199, classification of BRS is a Moderate impact system.

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).

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.

Yes, the BRS system is hosted in the VA Enterprise Cloud (VAEC) Amazon Web Services (AWS) and employs both Infrastructure as a Service (IaaS) to manage Webservers and Software as a Service (SaaS).

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)

This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

The BRS system is hosted in the VA Enterprise Cloud (VAEC) Amazon Web Services (AWS).

9.3 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data

collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.

This question is related to privacy control DI-1, Data Quality.

The BRS system is hosted in the VA Enterprise Cloud (VAEC) Amazon Web Services (AWS) and the VA will retain ownership over all data.

9.4 NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met?

This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

The BRS system is hosted in the VA Enterprise Cloud (VAEC) Amazon Web Services (AWS).

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).

BRS system does not utilize RPA.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

ID	Privacy Controls
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

CHRISTIAN LOFTUS

Digitally signed by CHRISTIAN LOFTUS
Date: 2022.04.12 12:43:06 -04'00'

Privacy Officer, Christian Loftus

Amine Messaoudi 1136390

Digitally signed by Amine Messaoudi 1136390
Date: 2022.04.21 10:25:29 -05'00'

Information Systems Security Officer, Amine Messaoudi

Christopher Brown 101386

Digitally signed by Christopher Brown 101386
Date: 2022.04.13 13:30:59 -05'00'

Information Systems Owner, Christopher Brown

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).

Find VA Locations | Veterans Affairs

https://www.va.gov/find-locations

SORNs

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

https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf

Notice of Privacy Practices | HHS.gov

https://www.hhs.gov/hipaa/for-individuals/notice-privacy-practices/index.html