Privacy Impact Assessment for the VA IT System called:

Behavioral Health Lab (BHL)

Veterans Health Administration

Office of Mental Health and Suicide Prevention

eMASS # 12

Date PIA submitted for review:

12/13/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Nancy Katz-Johnson	Nancy.katz-johnson@va.gov	203-535-7280
Information System Security Officer (ISSO)	Alvaro Camacho	Alvaro.Camacho@va.gov	410-642-1881
Information System Owner	Jeffrey Rabinowitz	Jeffrey.Rabinowitz@va.gov	732-720-5711

Abstract

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

Behavioral Health Lab (BHL) is a Commercial Off The Shelf (COTS) software program that provides patient tracking, decision support and the ability to conduct structured assessments in order to deliver evidence based mental health care for depression, PTSD, anxiety and alcohol misuse within primary care, mental health, and other care settings.

Overview

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

1 General Description

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

The name of the system is the Behavioral Health Lab (BHL) software platform, comprised of BHL Desktop and BHL Touch. The program office that owns the IT system is the Office of Mental Health and Suicide Prevention.

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

BHL enables patient assessment and tracking within primary care, mental health, and other clinical settings. The system supports the delivery of Measurement-Based Care (MBC) by allowing entry of standardized assessments for depression, PTSD, anxiety, alcohol misuse, etc., such as the PHQ-9, PCL-5, and GAD-7 measures. BHL helps with the management of mental health and other conditions by showing changes in scores (symptom severity) over time. Prior to the availability of the BHL, many providers would perform structured assessments on paper. The paper process required clinical staff to manually record, score and transfer these values into the patient record. This manual process - as most paper processes are –is error-prone and inherently inefficient. The BHL software provides clinical staff a means by which the patient assessments can be collected digitally, reliably scored, and efficiently uploaded to the patient EHRM patient record.

C. Who is the owner or control of the IT system or project?
VA Owned and VA Operated

2. Information Collection and Sharing

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

The expected number of individuals whose information is stored in the BHL system is 30,000 records per month. The typical client would be a Veteran being treated for a mental health condition (depression, PTSD, etc.)

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

Patient demographic information is stored in BHL so that clinicians can easily administer mental health assessments (for example a phone number in order to call the patient to ask questions for a given mental health assessment). The patient responses are collected in BHL so that the results can be calculated electronically, as well as graphed in order to show the clinicians changes in mental health symptoms/severity over time. This collection of assessment responses supports clinical care by helping determine the efficacy of mental health treatments, by demonstrating whether and to what extent symptom severity (depression, anxiety, alcohol use, etc.) changes over time.

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

Patient demographic and assessment information are transferred from the EHR (VistA/Cerner) to BHL, for assistance with the delivery of clinical care as previously described. Results of assessments collected in BHL (e.g. responses and results of assessments for depression, anxiety, etc.) are then transferred to the EHR in order to populate the system of record.

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

Yes, the system operates Enterprise-wide. Since user access controls across all sites are inherited (i.e. users can only access BHL if they have EHR access at a VA location), BHL ensures that users have completed the HIPAA/privacy trainings regarding appropriate use of PII that are required for EHR access. This also limits users' access to PII in BHL to the VA location/EHR to which the user has access.

3. Legal Authority and SORN

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

The Privacy Act of 1974, as amended, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. The authority of maintenance of the system listed in question 1.1 falls under Title 28, United States Code, title 38, U.S.C., sections 501(a), 1705, 1710, 1722, and 5317.

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?

No, the system is not in the process of being modified. Yes, VAEC is covered by the SORN.

4. System Changes

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

No

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

No

Section 1. Characterization of the Information

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

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

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

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

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

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

- ☒ Name
- ☒ 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[1]
☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☒ Medications
☒ Medical Records
☒ Race/Ethnicity

☐ Tax Identification Number
☒ Medical Record Number
☒ Gender
☐ Integrated Control Number (ICN)
☐ Military History/Service Connection

☐ Next of Kin
☒ Other Data Elements (list below)

Other PII/PHI data elements: Cerner: Medical Record Number (MRN)-Electronic Data Interchange Personal Identifier (EDIPI)

PII Mapping of Components (Servers/Database)

Behavioral Health Lab consists of 2 key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by BHL and the functions that collect it are mapped below.

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

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	**Does this system collect PII? (Yes/No)**	**Does this system store PII? (Yes/No)**	**Type of PII (SSN, DOB, etc.)**	**Reason for Collection/ Storage of PII**	**Safeguards**
BHL Desktop Application	Yes	Yes	SSN (masked to last 4) First Name Last Name DOB Address Phone Physician Name Assessment Data	Patient tracking and decision support to deliver measurement-based care	No data sharing outside VA LAN. Thick Client system deployed On-Prem and managed by OI&T
BHL Touch Application	Yes	Yes	SSN (masked to last 4) First Name	Patient tracking to	Encrypted 2FA front end

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

			Last Name DOB Address Phone Physician Name Assessment Data	deliver measurement-based care	interface & 2FA encrypted SQL db on server side

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?

The information is collected directly from the EHR medical record (CPRS/Cerner) and from the individual (i.e. patient-provided responses to mental health assessments). PII and PHI are pulled from the EHR into the BHL application for the delivery of clinical care (i.e. to attain information about the patient from whom assessments are to be collected). Information collected from the patient is used to support clinical decision making, which includes the process of ensuring that patients are receiving the right level of care.

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.

Information must be pulled from the EHR since this is the VA's official system of record and enables both an efficient and accurate mechanism for pulling patient demographics. Note that BHL does **not** use data from other sources such as a commercial aggregator.

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

Yes, for assessment responses that are entered into BHL, the results are automatically scored, analyzed if appropriate (e.g. symptoms categorized as severe/moderate/minimal), and generated into a clinical report. The clinical report reflecting the scores and analysis is transferred into the patient's record in the EHR.

1.3 How is the information collected?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

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

The information is collected via an interface (lookup and transfer) from the EHR medical record and transferred into the BHL database.

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

The information collected by BHL is not subject to the Paperwork Reduction Act; therefore, no OMB control numbers exist.

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.

Regarding assessment results stored in BHL, information collected face-to-face, telephonically and via veteran direct entry is verified in the context of clinical care, in which providers review the assessment results to discuss reported symptoms and severity. A VA clinical staff member electronically transmits the information from BHL to the EHR electronic patient record, which is the official patient system of record.

The BHL system implements internal and organizational validation rules to validate **user input** to ensure data accuracy and security.

The BHL system implements internal and organizational validation controls (strong typing, checksums) to control and validate **system inputs** to ensure data accuracy and security.

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

BHL does not access a commercial aggregator of information to check for accuracy.

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

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

The legal authority for collecting information is as follow: Title 5 USC 552a and Executive Order 9397. Additionally: VA System of Record Notice (VA SORN) Patient Medical Records–VA (24VA10A7) Title 38, United States Code, Sections 501(b) and 304. **1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information**

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk:
The system collects, processes, and retains PII and PHI on Veterans. If this information was breached or accidentally disclosed to inappropriate parties or the public, it could result in personal harm to the individuals impacted and adverse negative effect to the VA.

Mitigation:
Data collected, processed, and retained will be protected in accordance with VA Handbook 6500 and FIPS 140-2 encryption and data in-transit protection standards. All systems and individuals with access to the system will be approved, authorized, and authenticated before access is granted. VA annual privacy and security training compliance will be enforced for all VA employees, contractors, and vendors.

Section 2. Uses of the Information

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

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

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

PII/PHI Data Element	Internal Use	External Use
Name	Identification purposes	N/A
SSN/MRN	Identification purposes	N/A
DOB	Identification purposes	N/A
Mailing Address	Identification purposes	N/A
Personal Phone Number	Identification/Contact purposes	N/A
Personal Email	Identification/Contact purposes	N/A
Medications	Contextual Treatment	N/A
Race/Ethnicity	Contextual Treatment	N/A
Gender	Contextual Treatment	N/A
EDIPI	Identification purposes	N/A

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?

BHL is a tool used in clinical care to implement Measurement-based care (MBC) which is a healthcare approach that involves the systematic use of patient-reported data and clinical assessments to inform treatment decisions and monitor the progress of individuals receiving mental health or medical care. The primary goal of measurement-based care is to enhance the effectiveness of treatment by regularly assessing and adjusting interventions based on objective data. BHL's role is to collect and score the patient reported outcomes. The patient reported outcome data collected by BHL is uploaded to the VAMC's EHR (VistA/Cerner) as both a TIU Note and a discrete 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.

The clinical reports and assessment results collected in BHL are added to an individual's existing electronic health record as a new note, or a note attached to an existing scheduled EHR appointment. The clinical reports created from BHL are accessible only to clinicians with access to the EHR based on their role and trainings; as such, like other medical records, they should

only be accessed if required for their role in patient care. No action should be taken against or for an individual as a result of information in their health record. Clinicians may use the assessment results to make decisions for optimal clinical care (e.g. increase antidepressant dose for depression scores not improving).

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?

BHL SQL databases hold data at rest. SQL databased are managed by OI&T and inherit database encryption.

The BHL on-prem COTS system inherits VA security controls such as VA at-rest encryption, HTTPS web traffic, VA security gateways (Email, HTTP), and associated VA infrastructure controls.

The BHL system also implements controls to encrypt, secure and maintain the confidentiality and integrity data via the implementation of HTTPS, VA SSOi authentication, encrypted (SSL) database traffic and Microsoft SQL Server at rest encryption.

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

Yes, masked SSNs are the default display of all SSNs. The user must click the field to see the complete number. When masked, the number will appear as XXX-XX-1234 and the entire number will be visible in the document when the fields are unmasked.

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

BHL utilizes a combination of encryption and hashing algorithms prior to and during data transmissions to ensure the confidentiality and integrity of data. This includes SSL Certificates for encryption and mTLS for secure communication.

2.4 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u>

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:

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

Principle of Use Limitation: *Is the use of information contained in the system relevant to the mission of the project?*
This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

2.4a How is access to the PII determined?

Access to PII is controlled via inherited permissions from EHR and PIV user access level permissions that BHL inherits.

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

Access to PII is based on EHR and user access level; criteria, procedures, controls and responsibilities regarding access are inherited by BHL (only those users meeting the criteria and training requirements to access the EHR can access BHL)..

2.4c Does access require manager approval?

No

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

Yes, the system maintains a log of user activity whenever there is an instance of accessing patient records. The system documents each interaction, ensuring transparency, traceability, and accountability in handling sensitive patient information. The logs reside directly in the BHL database and are only accessible by BHL administrators.

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

The system's Information System Security Officer (ISSO) assures safeguards for the PII.

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

The following data is retained within the BHL database: The information listed in Section 1.1 is retained in the BHL database and not deleted. • Name • Social Security Number • Date of Birth • Mailing Address • Zip Code • Current Medications • Previous Medical Records

3.2 How long is information retained?

In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. ***The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.*** *If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

The "data" in this case refers to the BHL data. The Veteran's self-entered record is to be maintained indefinitely. National Archives and Records Administration (NARA) guidelines as stated in Records Control Schedule (RCS) 10-1 record retention schedule requires retention for 75 years. Whenever technically feasible, all records are retained indefinitely in the event of additional follow-up actions on behalf of the individual.

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 data retention period has been approved by NARA and is processed according to the following: • Records Control Schedule 10-1 link for VHA: www.va.gov/vhapublications/rcs10/rcs10-1.pdf • Records Control Schedule VB-1, Part II Revised for VBA: www.benefits.va.gov/WARMS/docs/admin20/rcs/part2/part2.pdf • National Archives and Records Administration: www.nara.gov.

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

The data retention period has been approved by NARA and is processed according to the following: • Records Control Schedule 10-1 link for VHA: www.va.gov/vhapublications/rcs10/rcs10-1.pdf • Records Control Schedule VB-1, Part II Revised for VBA: www.benefits.va.gov/WARMS/docs/admin20/rcs/part2/part2.pdf • National Archives and Records Administration: www.nara.gov

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

Explain how records are destroyed, eliminated or transferred to NARA at the end of their mandatory retention period. Please give the details of the process. For example, are paper records shredded

on site, or by a shredding company and accompanied by a certificate of destruction, etc.? This question is related to privacy control DM-2, Data Retention and Disposal.

Data is not removed from BHL. The status of the Veteran can be changed, but policy is to never remove a record. Data is retained until the system is decommissioned or migrated to a new replacement system. BHL is not a system of record and data is stored on SQL servers operated by OI&T. If the system is decommissioned destruction or migration will be handled by OI&T with support from the BHL team as needed.

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.

All IT system and application development and deployment is handled by VA OI&T. VHA does test new or modified IT systems for VHA operations prior to deployment, and PII/PHI may be used for that Alpha or Beta testing at the facility-level per VHA policy. In addition, VHA may need to train staff on functionality in the new or modified IT system. Training, including on IT systems, is part of health care operations and per VHA policy PII and PHI may be used for that training purpose. However, VHA must minimize the use of PII and PHI in training presentations or materials per VA policy. In case human subject research was intended to be covered by this control: VA Research investigators may use PII for VA Institutional Review Board (IRB)-approved research, and there is no effort to minimize the use of PII for research. Controls for protecting PII used for testing, training and research are often security controls if the PII is electronic. When paper PII, reasonable safeguards for protecting the PII are to be employed.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

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

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

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

Follow the format below:

Privacy Risk: There is a risk that the information contained in the system will be retained for longer than is necessary to fulfill the VA mission.

Mitigation: All personnel with access to Veteran's information are required to complete the VA Privacy and Information Security Awareness & Rules of Behavior training annually. BHL adheres to all information security requirements instituted by the VA Office of Information and Technology (OI&T).

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***
VHA VistA	To enable authorized personnel to view Veteran's Patient information in a timely manner.	PII-PHI SSN • First Name • Last Name • DOB • Address • Phone • Assessment Data	HTTPS, TCP/IP Protocol
VHA Cerner EHRM	To enable authorized personnel to view Veteran's Patient information in a timely manner.	PII-PHI SSN • First Name • Last Name • DOB • Address • Phone • Assessment Data	HTTPS, TCP/IP Protocol
BHL Touch Module (VAEC)	Allows for collection of survey data from veterans	PII-PHI SSN (masked to last 4) First Name Last Name DOB Address Phone Physician Name Assessment Data	HTTPS, TCP/IP Protocol

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

Follow the format below:

Privacy Risk: There is very little risk in transmitting, viewing and uploading the data from BHL to EHR. Information may be compromised through shoulder surfing which may result in a breach of confidentiality.

Mitigation: The VA Rules of Behavior are required to be signed by all personnel prior to accessing any VA related equipment according to VA Directive and Handbook 6500. Only authorized users have access. Role based accessed for VA activity is restricted by least privilege account management. Penalties are executed to the full extension of the law if a breach in confidentiality is determined.

Section 5. External Sharing/Receiving and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to VA, which includes Federal, State, and local governments, and the private sector.

5.1 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

Is the sharing of information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.

NOTE: Question 3.10 on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any Federal, State, or local government agency or private sector organization with which information is shared.

For each interface with a system outside VA, state what specific data elements (PII/PHI) are shared with each specific partner.

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.
This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit***	***List the method of transmission and the measures in place to secure data***

	specified program office or IT system		***external sharing (can be more than one)***	
Cerner	Electronic Medical Records	PII / PHI • First name • Middle name • Last name • Suffix • MRN-EDIPI • Date of birth • Sex • Phone number • Email • Address • Race • Ethnicity • Current Medications • Patient responses to medical assessments	MOU	HTTPS

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

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

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

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

Follow the format below:

<u>Privacy Risk:</u> There is very little existing risk (See 4.2) in the Internal Sharing (transmitting, viewing and uploading) the data from BHL to the EHR, data is transferred over secure protocols (HTTPS). There is little or no new risk related to BHL sharing data with the Cerner (VA's EHRM) System. Cerner is already an internal organization that BHL shares data with, and this process only ensures alignment across the Cerner (VA's EHRM) System.

Mitigation: Data Security is governed by the VA's EHRM security guidelines. Privacy is further secured by storing all data on encrypted VA servers behind VA firewalls.

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.

As a tool used by VHA staff, Privacy Notices for BHL collection are commensurate with VHA's own Privacy Notices. During the course of VHA operations, notice is provided in the following ways, as explained in further detail below:

1. VHA NOPP
2. This PIA
3. Applicable SORN
4. Written notice on all VA forms

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

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

Notice is also provided in the Federal Register with the publication of the SORN

The information is for BHL use only and is stated in the Privacy Notice. The following Written notice is on all VA forms: PRIVACY ACT INFORMATION: No allowance of compensation or pension may be granted unless this form is completed fully as required by law (38 U.S.C. 5101). The responses you submit are considered confidential (38 U.S.C. 5701).

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

Notice was provided as stated in 6.1 a

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

BHL notices is adequate as it is aligned with VHA's own notice practices, as described in 6.1a.

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

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

Notice is also provided in the Federal Register with the publication of the SORN

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.

The BHL application is provided PII/PHI from the EHR system of record, which implements the federal regulations that apply to Standards for Privacy of Individually Identifiable Health Information (Individual Participation IP-1 Consent control of the VA Information Security Reference Guide - Page 158). Any patient can decline to be followed by the mental health clinical staff utilizing the BHL clinical operational program. The Facility Directory Opt-Out Overview for staff members responsible for disclosure directs to the Opt-Out Fact Sheet detailing steps necessary to allow for opt-in or opt-out.

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.

The Privacy Act and VA policy require that personally identifiable information only be used for the purpose(s) for which it is collected, unless consent (opt-in) is granted. Individuals must be provided an opportunity to provide consent for any secondary use of information, such as use of collected information for surveys or marketing purposes. If the individual wants to consent to a particular use of the information, they can contact the BHL Support Desk for correction (202-670-2847).

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

Principle of Transparency: Has sufficient notice been provided to the individual?

Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?
This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.
Follow the format below:

Privacy Risk: There is a risk that individuals who provide information to the BHL application will not know how their information is being used internally to the Department of Veterans Affairs.

Mitigation: The VA mitigates this risk by providing veterans and other beneficiaries with multiple forms of notice of information collection, retention, and processing. The main forms of notice are discussed in the Privacy Act statement, a System of Record Notice, and the publishing of this Privacy Impact Assessment.

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.***

All data inquiries are to be addressed to the BHL Support Desk at (bhlsupport@va.gov).

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

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

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

It is not exempt

7.1c If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information?

It is in a privacy act system of records

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

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

The individual has the right to request amendment of erroneous information in accordance with the Privacy Act and HIPAA Privacy Rule. Any discrepancies are to be reported to BHL Support Desk for correction (bhlsupport@va.gov).

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 have access to the Notice of Privacy Practices which states the following relating to procedures for correcting their information: "Right to Request Amendment of Health Information". You have the right to request an amendment (correction) to your health information in our records if you believe it is incomplete, inaccurate, untimely, or unrelated to your care. You must submit your request in writing, specify the information that you want corrected, and provide a reason to support your request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains your information. If your request for amendment is denied, you will be notified of this decision in writing and provided appeal rights. In response, you may do any of the following:
• File an appeal.
• File a "Statement of Disagreement".
• Ask that your initial request for amendment accompany all future disclosures of the disputed health information." http://www1.va.gov/vhapublications/ViewPublication.asp?pub_ID=1089

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 as indicated above.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department's access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. ***For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals involved might change their behavior.*** *(Work with your System ISSO to complete all Privacy Risk questions inside the document this section).*

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

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

Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?
This question is related to privacy control IP-3, Redress.

Follow the format below:

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

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

The*]* Release of Information (ROI) office is available to assist Veterans with obtaining access to their health records and other records containing personal information.
The Veterans' Health Administration (VHA) established MyHealtheVet program to provide Veterans remote access to their medical records. In addition, VHA Directive 1605.01 Privacy and Release of Information establishes procedures for Veterans to have their records amended where appropriate.
Section 8. Technical Access and Security

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

8.1 What procedures are in place to determine which users may access the system, and are they documented?
These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.

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

The BHL inherits network security controls from the VA infrastructure. From the BHL perspective there are two distinct roles within the software:

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?

BHL utilizes network security controls inherited from the VA infrastructure to ensure that only authorized users can access the VA network and BHL application. Furthermore, the BHL application implements additional authentication security controls to ensure users have the appropriate access to the software and corresponding data. The BHL also contains auditing features that allow administrators the ability to audit individual user actions and follow VA SOPs with respect to disciplinary action. Users from other agencies cannot access the system, as they would not have the EHR access required as a prerequisite to access BHL.

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.

End user accounts (registered and in-person accounts) reside in Active Directory (AD). End user (Veteran) accounts are created when the Veterans register themselves. VA employees are able to log in against AD and do not register on the admin portal. BHL systems administrators are VA employees and therefore are not required to register through the BHL end user account. VA employees log in to the admin portal using their AD account to perform admin functions.

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.

BHL and the VA ensure that all personnel take annual security training and pass VA Privacy and Information Security Awareness training. All users of the BHL project team are required to sign a Rules of Behavior agreement prior to being given access to BHL systems. Additionally, the Rules of Behavior is required to be reviewed and signed annually by each user. Annual training for the National Rules of Behavior is performed through the Talent Management System (TMS). There are two versions of the National Rules of Behavior: one for VA employees and one for contractors. Definitions of VA employee and VA Contractor:

• VA Employees - VA employees are all individuals who are employed under title 5 or title 38, United

• States Code, as well as individuals whom the Department considers employees such as volunteers, without compensation employees, and students and other trainees.

• VA Contractors - VA contractors are all non-VA users having access to VA information resources through a contract, agreement, or other legal arrangement. Contractors must meet the security levels defined by the contract, agreement, or arrangement. Contractors must read and sign the Rules of Behavior and complete security awareness and privacy training prior to receiving access to the information systems.

Users agree to comply with all terms and conditions of the National Rules of Behavior, by signing a certificate of training at the end of the training session.

8.3 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.

VA requires Privacy and Information Security Awareness & Rules of Behavior training to be completed on an annual basis. The Talent Management System offers the following applicable privacy courses: VA 10176: Privacy and Information Security Awareness and Rules of Behavior VA 10203: Privacy and HIPPA Training VA 3812493: Annual Government Ethics

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Yes
2. *The System Security Plan Status Date:* 11/13/2023
3. *The Authorization Status: Authorization to Operate (ATO)*
4. *The Authorization Date:* 12-07-2020
5. *The Authorization Termination Date:* 12-07-2023
6. *The Risk Review Completion Date:* 10-30-2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

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

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?
BHL's cloud hosting is provided through the VAEC.
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.
BHL utilizes the VA Enterprise Cloud (VAEC)

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number

and supporting information about PII/PHI from the contract). (*Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

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.

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.

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).

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**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

NANCY KATZ-JOHNSON

Digitally signed by NANCY KATZ-JOHNSON
Date: 2024.02.23 08:45:25 -05'00'

Privacy Officer, Nancy Katz-Johnson

ALVARO CAMACHO

Digitally signed by ALVARO CAMACHO
Date: 2024.02.23 12:29:22 -05'00'

Information System Security Officer, Alvaro Camacho

JEFFREY RABINOWITZ

Digitally signed by JEFFREY RABINOWITZ
Date: 2024.02.23 09:52:31 -05'00'

Information System Owner, Jeffrey Rabinowitz

APPENDIX A-6.1

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

HELPFUL LINKS:

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

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

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

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

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