Privacy Impact Assessment for the VA IT System called:

Behavioral Health Lab (BHL)

Date PIA submitted for review:

01/15/2021

System Contacts:

<table>
<thead>
<tr>
<th>System Contacts</th>
<th>Name</th>
<th>E-mail</th>
<th>Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Officer</td>
<td>Loftus, Christian D</td>
<td><a href="mailto:Christian.Loftus@va.gov">Christian.Loftus@va.gov</a></td>
<td>859-281-2470</td>
</tr>
<tr>
<td>Information System Security Officer (ISSO)</td>
<td>Alvaro Camacho</td>
<td><a href="mailto:Alvaro.Camacho@va.gov">Alvaro.Camacho@va.gov</a></td>
<td>443-717-4096</td>
</tr>
<tr>
<td>Information System Owner</td>
<td>Michael Braithwaite</td>
<td><a href="mailto:Michael.braithwaite@va.gov">Michael.braithwaite@va.gov</a></td>
<td>801-588-5221</td>
</tr>
</tbody>
</table>
Abstract

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

Behavioral Health Lab (BHL) is a Commercial Off The Shelf (COTS) software program 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 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:

- 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.
- The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.
- If your system is a regional GSS, VistA, or LAN, include a list of the hospitals/medical centers, or other regional offices that fall under your system. Additionally, what region is the system under?
- A general description of the information in the IT system.
- 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?
- Does the system use cloud technology? 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.
- Does a contract with Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII?
• **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 is the magnitude of harm if privacy related data is disclosed, intentionally or unintentionally? Would the reputation of the CSP or its customers (VA) be affected?**

Behavioral Health Lab (BHL) is a Commercial Off The Shelf (COTS) software program that provides patient tracking by patient contacts, patient assessment scores and data associated with the tracking and delivering evidence based mental health care (depression, PTSD, anxiety and alcohol misuse within primary care settings); decision support based upon the technology domain of Decision Support Systems (DSS) and the ability to conduct structured assessments which are standard mental health questionnaire screenings, such as the PHQ9, PCL5 (see below) in order to deliver the above mental health care evidence. The oversight and use of the BHL is managed through the National Primary Care-Mental Health Integration (PC-MHI) office. The software is currently installed at 140 BHL installation sites. The current version, integrated with the VA Electronic Medical Record (EHRM) Systems (VistA & Cerner) which is the system of record for all patient information in the VA.

Prior to the availability of the BHL many facilities 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 score the resulting data, and efficiently upload this data to the patient EHRM patient record. Since the assessments are digitally recorded, the clinical staff can retrieve historic data from the software in an organized and efficient way. • The structured assessments are standard Mental Health questionnaire screenings such as the PHQ9, PCL5, and BAM. A full list of the included assessments is provided below:

**ASSIST-NIDA**: Alcohol Smoking and Substance Involvement Screening  
**AUDIT**: Alcohol Use Disorders Identification Test  
**AUDIT-C**: Screening  
**BAM-IOP**: Brief Addiction Monitor - 7 day  
**BAM-R**: Brief Addiction Monitor - 30 day  
**Blessed Memory Test**  
**BOMC**: Cognitive Impairment  
**BRS**: Brief Resilience Scale  
**CCSA-DSM5**: Cross-Cutting Symptom Assessment for DSM-5  
**CSI-16**: Couples Satisfaction Index - Partner  
**CSI-16**: Couples Satisfaction Index - Patient  
**CSI-4**: Couples Satisfaction Index - Partner  
**CSI-4**: Couples Satisfaction Index - Patient  
**C-SSRS** screener (VA Modified)  
**Depression Symptoms (PHQ-9)**  
**GAD-7**  
**Geriatric Anxiety Inventory**
Geriatric Depression Scale - Short Form
ISI: Insomnia Severity Index
Minor Depression and Distress
Patient Safety Screener 3 (PSS-3)
PCL-5 Monthly: PTSD Checklist
PCL-5 Weekly: PTSD Checklist
PC-PTSD-5: Screening: Primary Care PTSD-5
PHQ-2: Screening
PHQ-9: Depressive Symptoms
POQ-SF: Pain Outcomes
PSOCQ: Pain Stages of Change
PSS: Perceived Stress Scale
Short Warwick-Edinburgh Mental Wellbeing Scale
SNQ: Sleep Need Questionnaire
VR-12: Veterans RAND 12 Item Health Survey
WHODAS 2.0 12-item
WHQOL-BREF
Working Alliance Inventory - Short Revised (WAI-SR)
Zarit Burden Interview (ZBI-12)

The expected number of individuals whose information is stored in the BHL system is 15,000 records per month. BHL does not analyze patient data. Rather, BHL provides patient tracking by patient contacts, patient assessment scores and data associated with the tracking and delivering evidence based mental health care; decision support based upon the technology domain of Decision Support Systems (DSS) and the ability to conduct structured assessments which are standard mental health questionnaire screenings, such as the PHQ9, PCL5 in order to deliver the above mental health care evidence.

Title 10 U.S.C. chapters 106a, 510,1606 and 1607 and Title 38, U.S.C. Section 501(a) and Chapters 11, 13, 15,18, 23, 30, 31, 32, 33, 34, 35, 36, 39, 51,53, and 55 provide the legal authority for operating the BHL. VA gathers or creates these records in order to enable it to administer statutory benefits programs to Veterans, Service members, reservists, and their spouses, surviving spouses, and dependents, who file claims for a wide variety of Federal Veteran’s benefits administered by VA.

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://www.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.

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
- Other Unique Identifying Number (list below)

### PII Mapping of Components

Behavioral Health Lab consists of 4 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.

#### PII Mapped to Components

<table>
<thead>
<tr>
<th>Components of the information system (servers) collecting/storing PII</th>
<th>Does this system collect PII? (Yes/No)</th>
<th>Does this system store PII? (Yes/No)</th>
<th>Type of PII (SSN, DOB, etc.)</th>
<th>Reason for Collection/Storage of PII</th>
<th>Safeguards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server/Database</td>
<td>Yes</td>
<td>Yes</td>
<td>PII (SSN, DOB) &amp; IIHI (Medication records)</td>
<td>Patient tracking and decision support to deliver</td>
<td>Encrypted 2FA front-end interface &amp; 2FA</td>
</tr>
</tbody>
</table>

Version Date: February 27, 2020
Page 4 of 23
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 is used directly from the EHR medical record and augmented with information from the individual. PII and PHI are pulled from EHR into BHL application where the data is used to drive workflow related, which includes the process of ensuring that patients are receiving the right level of care. In order for a BHL to obtain patient information, it must come from EHR.

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 technology 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 is collected via an interface (lookup and transfer) from the EHR medical record and transferred into the BHL database. When the clinical staff interacts with the patient they will validate and augment the data with information gathered from the patient via face-to-face, phone interactions or through patient survey entry.
1.4 What is the purpose of the information being collected, used, disseminated, created, or maintained?

Include a statement of why the particular SPI is collected, maintained, used, or disseminated in the system is necessary to the program’s or agency’s mission. Merely stating the general purpose of the system without explaining why this particular type of information should be collected and stored is not an adequate response to this question.

If the system collects, uses, disseminates, or maintains publicly available or commercial data, include a discussion of why commercial data is relevant and necessary to the system’s purpose. This question is related to privacy control AP-2, Purpose Specification.

BHL information is used in conjunction with existing data from EHR to update the patient’s electronic medical health record, allowing medical providers to provide accurate medical diagnosis. The information collected is a combination of Personal Identifiable Information (PII) and Protected Health Information (PHI).

1.5 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.

The data being collected via face-to-face, telephonically and veteran entry; information is captured and entered into the BHL by a VA clinical staff member. The information is electronically transmitted from the EHR electronic patient record, which is the official patient system of record. The data is verified with the patient over the phone to identify any possible inaccuracy.

1.6 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) Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA, SORN 58VA21/22/28. VHA collects the data under authority of Title 38 U.S.C. Sections 501 in order for VA to determine eligibility for medical benefits.

1.7 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:** Because BHL holds Sensitive Private Information, the system may be vulnerable to Hackers, Crackers, Malicious Code and Password Privacy Negligence.

**Mitigation:** Access Control, Audit and Accountability, Awareness and Training, Security Assessment and Authorization, Configuration Management, Contingency Planning, Identification and Authentication, Incident Response, Media Protection, Personnel Security,
Section 2. Uses of the Information

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

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

Identify and list each use (both internal and external to VA) of the information collected or maintained.

This question is related to privacy control AP-2, Purpose Specification.

• Name: Used to identify the veteran who is being reviewed
• Social Security Number: Used to verify the identity of the veteran who is being reviewed
• Mailing Address: Used to verify the identity of the veteran who is being reviewed
• Zip Code: Used to verify the address
• Date of Birth: Used to verify the veteran.
• Current Medications
• Previous Medical Records

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
BHL does not analyze patient data. Rather, BHL provides patient tracking by patient contacts, patient assessment scores and data associated with the tracking and delivering evidence based mental health care; decision support based upon the technology domain of Decision Support Systems (DSS) and the ability to conduct structured assessments which are standard mental health questionnaire screenings, such as the PHQ9, PCL5 in order to deliver the above mental health care evidence.

2.3 PRIVACY IMPACT ASSESSMENT: Use of the information. 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.

The minimum-security requirements for BHL’s high impact system cover 17 security-related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. Our facility employs all security controls in the respective high 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 800-53 and specific VA directives.

Data newly created within the BHL (i.e. clinical staff members utilize the BHL software to manually enter in data) application is summarized and then uploaded into the EHR) patient medical record. This summarization and upload of data to EHR ensures that the data is tracked in the VA’s official patient system of record. The data is linked to the individual’s official record which facilitates the ability of the data to be accessible by all authorized clinical staff. Only VA
employees can access the BHL program. BHL utilizes network security controls inherited from the VA infrastructure (VA server and network (WAN/LAN)) provided by VA and Austin Information Technology Center (AITC) 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 corresponding data refers to information collected and entered by VA clinical staff into the BHL such as patient demographic and assessment information. The BHL also contains auditing features that allow administrators the ability to audit individual user actions and follow VA Standard Operating System (SOP)s with respect to disciplinary action.

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.
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)? 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.

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 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.

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.

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

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.

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. NOTE: Question 5 on Privacy Threshold Analysis should be used to answer this question.

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?

*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.*
<table>
<thead>
<tr>
<th>List the Program Office or IT System information is shared/received with</th>
<th>List the purpose of the information being shared/received with the specified program office or IT system</th>
<th>List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT system</th>
<th>Describe the method of transmittal</th>
</tr>
</thead>
<tbody>
<tr>
<td>VHA VistA</td>
<td>To enable authorized personnel to view Veteran’s Patient information in a timely manner.</td>
<td>PII-PHI</td>
<td>HTTPS, TCP/IP Protocol</td>
</tr>
<tr>
<td>VHA Cerner EHRM</td>
<td>To enable authorized personnel to view Veteran’s Patient information in a timely manner.</td>
<td>PII-PHI</td>
<td>HTTPS, TCP/IP Protocol</td>
</tr>
<tr>
<td>BHL Touch Module (VAEC)</td>
<td>Allows for collection of survey data from veterans</td>
<td>No PII-PHI</td>
<td>HTTPS, TCP/IP Protocol</td>
</tr>
</tbody>
</table>

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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: This question is #7 in the Privacy Threshold Analysis.

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

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

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

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.

This question is related to privacy control UL-2, Information Sharing with Third Parties

<table>
<thead>
<tr>
<th>List External Program Office or IT System information is shared/received with</th>
<th>List the purpose of information being shared / received / transmitted with the specified program office or IT system</th>
<th>List the specific data element types such as PII/PHI that are shared/received with the Program or IT system</th>
<th>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</th>
<th>List the method of transmission and the measures in place to secure data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cerner Electronic Medical Records</td>
<td>PII / PHI</td>
<td>Unknown</td>
<td>HTTPS</td>
<td></td>
</tr>
</tbody>
</table>
If specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16, note them here.

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: As BHL does not share data with any outside organizations, there are minimal to no privacy risks to the data collected, stored, and maintained in the system.

Mitigation: The key mitigation to any privacy risk related to external sharing of VA data from CSS is that the system does not connect to or share with any external organizations or systems. Privacy is further secured by storing all data on encrypted local servers behind 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 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 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). VA may disclose the information that you provide, including Social Security numbers, outside VA, if the disclosure is authorized under the Privacy Act, including the routine uses identified in the VA system of records, 58VA21/22 Compensation, Pension, Education, and Rehabilitation Records - VA. The requested information is considered relevant and necessary to determine maximum benefits under the law. Information submitted is subject to verification through computer matching. The Department of Veterans Affairs also provides notice by publishing the VA System of Record Notice (VA SORN) Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA, SORN 58VA21/22/28 (July 19, 2012), in the Federal Register and online. An online copy of the SORN can be found at: http://www.gpo.gov/fdsys/pkg/FR-2012-07-19/html/2012-17507.htm.

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

Some of the information required for BHL data collection is mandatory as others are voluntary. 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 want 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.

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?

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.

All Data inquiries are to be addressed to the BHL Support Desk at (202-670-2847) additionally, individuals seeking information regarding access to and contesting of VA records may write, call or visit the nearest VA regional office. Address locations are listed in VA Appendix 1. See VA SORN Compensation, Pension, Education and Employment Records-VA, SORN 58VA21/22/28(July 19, 2012)

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 (202-670-2847).

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.
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.

The individual has the right to request amendment of erroneous information. All Data inquiries are to be addressed to the BHL Support Desk at (202-670-2847) Additionally; the Veteran can visit a VBA Regional Office, visit the VBA Internet Site, or call 1-888-442-4551.

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
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 members of the public will not know the relevant procedures for gaining access to, correcting or contesting their information.

**Mitigation:** The privacy risk is mitigated by information provided by VA SORN Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA, SORN 58VA21/22/28(July 19, 2012). This states that individuals should contact their local VA Regional Office for additional information about accessing and contesting their records at the VA. Furthermore, this document and the SORN provide the point of contact for members of the public who have questions or concerns about the application.

### 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.

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

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.

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 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?

If Yes, provide:

1. The date the Authority to Operate (ATO) was granted,
2. Whether it was a full ATO or ATO with Conditions,
3. The amount of time the ATO was granted for, and
4. 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.

BHL received a Full ATO on December 7, 2020 and good for three years.
## Section 9. References

Summary of Privacy Controls by Family

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

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

CHRISTIAN D LOFTUS
222466
Digitally signed by CHRISTIAN D LOFTUS 222466
Date: 2021.01.25 13:44:14 -05'00'

Privacy Officer
Signature of Information Security Systems Officers

The Information Security Systems Officers below attest that the information provided in this Privacy Impact Assessment is true and accurate.

Alvaro W. Camacho
142149

Digitally signed by Alvaro W. Camacho
142149
Date: 2021.01.26 10:17:59 -05'00'

Information Security Systems Officer
Signature of Area Manager

The Area Manager below attests that the information provided in this Privacy Impact Assessment is true and accurate.

Michael J. Braithwaite
570687

System Owner
APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy, a Privacy Act notice on forms).