Privacy Impact Assessment for the VA IT System called:

PTSD Brain Bank

VA Boston HealthCare System
Veterans Health Administration

Date PIA submitted for review:

September 27, 2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Stephania Griffin	Stephania.Griffin@va.gov	704-245-2492
Information System Security Officer (ISSO)	Karen McQuaid	Karen.McQuaid@va.gov	708-724-2761
Information System Owner	Bertrand Huber	Bertrand.Huber@va.gov	857-364-6937

Abstract

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

PTSD Brain Bank is a system in a Virtual Private Cloud (VPC) in Amazon Web Services (AWS) VA Enterprise Cloud (VAEC) for supporting research activities in the form of digitized scanned images of microscope slides to allow automated digital analysis, curation, and storage of microscopy data. The system runs VA Technical Reference Model approved software and is accessed via JumpServers and Non-Mail Enabled Account (NEMA) zero accounts by VA staff from the VA network. PTSD Brain Bank is a subnet of the VA Enterprise Cloud development VPC and is protected by AWS-Cloud Service Provider and VAEC AWS GOV Cloud High security mechanisms.

Overview

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

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

The system name is PTSD Brain Bank, and the program Office is the Department of Veterans Affairs, Boston Healthcare System Research & Development Service. The system will

support an enclave for the PTSD Brain Bank, for research projects defined by an active protocol and under oversight of a Research and Development (R&D) committee needing access to VA Enterprise Cloud (VAEC) elastic resources, model of operations, and utility payment model using the Veterans Health Administration's National Center for PTSD funding Resources. Cloud resources include compute, storage services, and platform software. These services include Relational Data Base Service (RDS) for cataloging of data, other approved cloud capabilities, VAEC services for Authentication, Authorization, and Accounting (AAA), backup, monitoring, and similar. The PTSD Brain Bank will receive de-identified information from the National Center for PTSD Brain bank, which is an Institutional Review Board (IRB) regulated VA brain bank. This protocol will also receive de-identified information from the ALS brain bank, Gulf War brain bank and CTE brain bank, which are also IRB regulated VA brain banks located a Jamaica Plain.

The enclave consists of two components: First is a Research Data Repository (RDR) component that contains the data collected by the PTSD brain bank. The data within the RDR will use the data lake architecture available from AWS through VAEC. The second component of the enclave is an analytic component used to analyze and curate the data within the Research Data Repository.

The Research Data Repository receives coded data from the PTSD Brain Bank and stores the data in a data lake database. Sources of data will include the PTSD Brain bank RedCap database, scanned whole slide images, genetic data, and 3rd party vendors and partners via the network or Cloud Service Provider.

Veterans and non-Veterans who have been diagnosed with PTSD presently or in the past are eligible to participate. In addition, tissue donations from people who are not affected by PTSD are collected as well, as scientists studying neurological disorders must compare tissues samples of unaffected people with those that have been clinically diagnosed. Given that there are roughly 9 million veterans served by health care facilities and assuming 12% of them have been diagnosed with PTSD, we can estimate potentially 1,080,000 records stored in the system for that population.

The applications and platform software component will process and curate data for analysis and reporting applications. It will conduct predictive analytics research with further data curation, algorithm development and applications of machine learning and Artificial Intelligence (AI) techniques, analysis and presentation exemplified by research protocols for traumatic brain injury and neurodegenerative conditions. These analyses will not generate PII or PHI.

Section 1. Characterization of the Information

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

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

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

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

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

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

- ☐ Name
- ☐ Social Security Number
- ☐ Date of Birth
- ☐ Mother's Maiden Name
- ☐ Personal Mailing Address
- ☐ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☐ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☐ Financial Account Information
- ☐ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☐ Current Medications
- ☐ Previous Medical Records
- ☐ Race/Ethnicity
- ☐ Tax Identification Number
- ☐ Medical Record Number
- ☐ Gender
- ☐ Integration Control Number (ICN)
- ☐ Military History/Service Connection
- ☒ Next of Kin
- ☒ Other Unique Identifying Information (list below)

Coded unique identifier and Phenomics from the PTSD Brain Bank system and similar sources; domains include: RedCap Clinical database containing information relating to trauma, PTSD, and medical history; RedCap Neuropathology database containing information derived from the neuropathological examination; Various imaging modalities: Digital pathology, images of tissue specimens; and Genomics: Text based files containing nucleic acid sequences, including FASTQ and Variant Call Format (VCF) formatted files, which is considered a biometric identifier.

PII Mapping of Components

PTSD Brain Bank consists of four key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by PTSD Brain Bank and the reasons for the collection of the PII are in the table below."

PII Mapped to Components

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

PII Mapped to Components

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
VA Boston Healthcare System General Support System Brain Bank	No	No	N/A	This database contains coded demographic data including, gender, race, age (over 89 is listed as 89+), military service, history of trauma and clinical data including medical history, medication lists, ICD9 and ICD10 diagnoses are gathered from deceased study participants from the National Center for PTSD brain bank is stored in this database. Deidentified data from this database will be stored in the PTSD brain bank database	N/A

				after the tissue is processed	
Veteran's Informatics Computing Infrastructure (VINCI) RedCap Neuropathology database	No	No	N/A	This system collects deidentified information including deposition of neuropathological aggregates such as Tau, amyloid, TDP-43, and alpha synuclein as well as evidence of demyelination, and increases in inflammatory cells collected from the neuropathological evaluation. This evaluation provides information about the presence of neurodegenerative processes	Federal Risk and Authorization Management Program (FedRAMP) Compliant encryption at rest and in transit; Two factor user authentication; Network monitoring by various Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools. Compliance to FedRAMP Moderate specified controls is mandated and verified by Information System Security staff.
Veteran's Informatics Computing Infrastructure (VINCI) RedCap Clinical database	No	No	N/A	This system collects deidentified information pertaining to the individual's health status including gender, race, age (over 89 is listed as 89+), military service, history of trauma and clinical data including medical history, medication lists, ICD9 and ICD10 diagnoses. This data will inform	Federal Risk and Authorization Management Program (FedRAMP) Compliant encryption at rest and in transit; Two factor user authentication; Network monitoring by various Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools. Compliance to FedRAMP

				studies on factors that influence the outcome of stress and trauma on the brain	Moderate specified controls is mandated and verified by Information System Security staff.
VAEC Storage	Yes	Yes	Genetic data	The PTSD Brain Bank collects and stores genetic data to determine the role of genetics in susceptibility and resilience to developing PTSD. Techniques for evaluating genetic data are constantly improving and evolving, so it is imperative to retain the data for future studies	Federal Risk and Authorization Management Program (FedRAMP) Compliant encryption at rest and in transit; Two factor user authentication; Network monitoring by various Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools. Compliance to FedRAMP Moderate specified controls is mandated and verified by Information System Security staff.

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 Lieber Brain Institute is performing the genetic sequencing on the donor tissue pursuant to a contract and providing the data to the PTSD Brain Bank.
VA Informatic and Computing Infrastructure (VINCI)

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.

Information is received from the VA Biorepository Brain Bank: National PTSD Brain Bank, VA Biorepository Brain Bank Gulf War Veterans Illness Biorepository, VA Biorepository, and Chronic Traumatic Encephalopathy Brain Bank, and Chronic Effects of Neurotrauma VA TBI Brain Bank. Coded data from these studies is stored within the Biorepository. Digital pathology, images of tissue specimens; and Genomics: Digital pathology image formats include DICOM standard whole slide images (WSI), ScanScope Virtual Slide files (.SVS), QTIFF, JPEG2000, CZI, OME TIFF and DV2 files. These file formats use lossless compression and pyramidal storage to rapid access to any subregion without rendering the entire image. These formats contain metadata elements about the image and the coded case number, but no identifiable information is contained within the image. Text based files containing nucleic acid sequences, including FASTQ and Variant Call Format (VCF) formatted files are curated and stored for additional studies. The Biorepository will collect additional data from the coded specimens of the same types listed above. No attempt will be made to reidentify specimens.

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

Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that

receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.
This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

The data will be stored in the VAEC AWS cloud space, which is very safe from loss based on the design of the database. A data hash will be created for each data file. A data hash is a data fingerprint. If the data is modified or corrupted the hash can be used to detect which files are corrupted. The hash database will be maintained and checked every six months to ensure data fidelity. The PTSD Brain Bank will receive data as it becomes available from the National Center for PTSD Brain Bank. This will happen when the National Center for PTSD Brain Bank does a data freeze. Each time the data is received from the PTSD Brain Bank the data hash will be checked for the incoming files to ensure the fidelity of transmission.

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 authority for the system is Veterans' Benefits: Functions of Veterans Health Administration,38 U.S. Code § 7303, which states, in part:
(a)(1) In order to carry out more effectively the primary function of the Administration and inorder to contribute to the Nation's knowledge about disease and disability, the Secretary shallcarry out a program of medical research in connection with the provision of medical care andtreatment to veterans. Funds appropriated to carry out this section shall remain available untilexpended.
(2) Such program of medical research shall include biomedical research, mental illness research, prosthetic and other rehabilitative research, and health-care-services research.
The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule permits the use of protected health information for research purposes pursuant to a HIPAA authorization, whichis obtained from individual patients under the MVP research study to access, collect and store their health information and blood sample(s) for future research use.

As stated in Privacy Act Systems of Record Notice (SORN) 34VA10, "Veteran, Patient, Employee, and Volunteer Research and Development Project Records-VA", Title 38, United States Code, Section 501 is the authority for maintenance and operation of this system.

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks.

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

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

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

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

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

Follow the format below when entering your risk assessment:
Privacy Risk: The privacy risk is potential exposure of the limited data stored in this system.This system does not include the entire VA database but rather the partial data of the subset of research subjects whose information would be currently being processed in the system at the time.

The data within the PTSD Brain Bank is from deceased donors therefore there is no risk to the individual. The data collected from the donors includes information like disease status, drug use history, as well as a medical history. There is also genetic information. The main privacy risk would be to the next of kin, where the information might be sensitive or embarrassing. It could potentially be used for phishing attacks or more sophisticated confidence games that rely on personal information.

Mitigation: VA security protocols are followed throughout the system. The VAEC is a FISMA High environment and approved by VA to hold PII and PHI. This system is protected by a myriad of security features including limited, approved access, encryption, network isolation, 24-hour security monitoring, auditing, security configuration, scanning, patching, personnel security

as well as physical security required by FISMA and continually undergoes FISMA standard evaluations and reviews.

Section 2. Uses of the Information

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

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

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

The information in this system is used to support VA sanctioned research to improve veteran's health through new and innovative processes and technologies.

The purpose of the PTSD Brain Bank is to better understand the effects of trauma on the brain and in so doing understand the pathophysiology of the disease. Ultimately, this understanding will lead to the development of better therapeutics and better treatments for Veterans (and others) with PTSD.

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

The Research Data Repository (RDR) component contains the data collected by the PTSD brain bank. The data within the RDR will use the data lake architecture available from AWS through VAEC. The second component of the enclave is an analytic component used to analyze and curate the data within the Research Data Repository that will involve the use of the following software products: 1E Client (formerly Nomad) 6.x, Hashcorp Consul 1.10x, Docker Enterprise 3.1x, Python3 versions 3.6.12, 3.8x, 3.9x, 3.10x, Flask 1.1x, Neo4j 4.1.x, HALO 3.0 and SPSS 28.

2.3 How is the information in the system secured?

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

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

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

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

Controls are in place to assure that the information is handled in accordance with the uses described above to include online information security and Privacy and HIPAA training; face-to-face training for all incoming new employees conducted by the facility Information System Security Officer and Privacy Officer; and regular audits of individuals accessing sensitive information to ensure it is being appropriately used and controlled. Data is protected at rest and in transit with FIPS 140-2 validated encryption.

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

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. <u>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.</u>

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.

Only VA accredited staff have access to instances in the VAEC and data on a per protocol basis. The list of approved personnel is maintained in VAIRRS. The IRB has oversight for each protocol. All research activity is pre-approved by the local Privacy Officer and Research ISSO. This system uses FISMA standard processes for approving and monitoring access. This system is continually monitored and audited for compliance to FISMA security standards.

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

Summary coded data extracted from lab results, orders of medication, records of outpatient visits, surgery records, patient personal information, next of kin interviews, actionable genetic profile, international codes used to identify disease, etc. The crosswalk file is not stored on the PTSD Brain Bank system.

3.2 How long is information retained?

In some cases VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. If the system is using cloud technology, will it be following the NARA approved retention length and schedule?

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

The data will be retained in accordance with 34VA10 for 10 years for retrospective analysis of data. Active analysis usually takes a few years and is often gated by the growing number of participants in the research project. The data is then archived to reduce the cost of storage and possible future reference.

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.

When managing and maintaining VA data and records, the PTSD Brain Bank follows the guidelines established in the NARA-approved Department of Veterans Affairs (VA), Veterans Health Administration Record Control Schedule (RCS) 10-1 (March 2011) https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

Department of Veterans Affairs (VA), Office of Information & Technology RCS 005-1 (August 3,2009) http://www.oprm.va.gov/docs/RCS005-1-OIT-8-21-09.pdf and the General Records Schedule (http://www.archives.gov/records-mgmt/grs/).

3.4 What are the procedures for the elimination of SPI?

Explain how records are destroyed or eliminated at the end of the retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc?
This question is related to privacy control DM-2, Data Retention and Disposal

Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and VA Handbook 6500.1 Electronic Media Sanitization. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destruction. https://www.va.gov/vapubs/search_action.cfm?dType=1

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

Office of Information and Technology (OIT) documents and monitors individual information system security training activities including basic security awareness training and specific information system security training. This documentation and monitoring are performed through the use of Talent Management System (TMS). Access to the any system for research, testing or training is granted to VA clinical staffs and contractors by the local authority within each administrative area staff office. De-identified or test data is used when feasible for test or initiation of users.

3.6 <u>PRIVACY IMPACT ASSESSMENT: Retention of information</u>

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:

<u>Principle of Minimization:</u> 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?

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

Follow the format below:

Privacy Risk:
The PTSD Brain Bank contains records from deceased participants and the release of this information would have no harm on the participant. The only potential for harm would be to the next of kin. The information within the PTSD Brain Bank could be embarrassing to the family. This risk would persist as long as the data was retained.

Mitigation: There is no individual component that leaves the protected environment. When latter is the case, an elaborate de-identification process is conducted under review of the privacy officer and ISSO. The environment where information is held and processed is protected by both VA Office of Information and Technology and the VA Enterprise Cloud security mechanisms. Furthermore, the enclave is going through a comprehensive process to get an ATO and will be monitored for maintaining security standards. This system is protected by a myriad of security features including limited, approved access, encryption, network isolation, 24-hour security monitoring, auditing, security configuration, scanning, patching, personnel security as well as physical security required by FISMA and continually undergoes FISMA standard evaluations and reviews.

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***
VA Boston Healthcare System General Support System	Share deidentified data with internal VA investigators and with external investigators that have obtained permission via a Data Use Agreement (DUA).	Summary deidentified data extracted from lab results, orders of medication, records of outpatient visits, surgery records, patient personal information, next of kin interviews, actionable genetic profile, international codes used to identify disease, etc. (no PII)	Federal Risk and Authorization Management Program (FedRAMP) Compliant encryption at rest and in transit; Two factor user authentication; Network monitoring by various Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools. Compliance to FedRAMP Moderate specified controls is mandated and verified by Information System Security staff. Data is transferred using HTTPS transfer protocol.
Veteran's Informatics Computing Infrastructure (VINCI) – RedCap Neuropathology database	This data provides the status of neurodegenerative disease in the subject. This data will be combined with clinical data to determine how stress and trauma lead to long term neurodegenerative changes.	The instances of RedCap contain no PII/PHI. There are two RedCap databases associated with the PTSD brain bank. The first is a database containing neuropathology variables, which record external features like atrophy and brain size, and neuropathological variables like the presence or absence of neurodegenerative proteins. The second database contains clinical variables like history of PTSD, trauma, contact sports involvement. These databases do list age, but list	Federal Risk and Authorization Management Program (FedRAMP) Compliant encryption at rest and in transit; Two factor user authentication; Network monitoring by various Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools. Compliance to FedRAMP Moderate specified controls is mandated and verified by Information System Security staff. Data is transferred using HTTPS transfer protocol.

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*
		anyone over the age of 89 as 89+.	
Veteran's Informatics Computing Infrastructure (VINCI) – RedCap Clinical database	This data provides the clinical status of the subject. This data will be combined with neurodegenerative data to determine how stress and trauma lead to long term neurodegenerative changes.	The instances of RedCap contain no PII/PHI. There are two RedCap databases associated with the PTSD brain bank. The first is a database containing neuropathology variables, which record external features like atrophy and brain size, and neuropathological variables like the presence or absence of neurodegenerative proteins. The second database contains clinical variables like history of PTSD, trauma, contact sports involvement. These databases do list age, but list anyone over the age of 89 as 89+.	Federal Risk and Authorization Management Program (FedRAMP) Compliant encryption at rest and in transit; Two factor user authentication; Network monitoring by various Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools. Compliance to FedRAMP Moderate specified controls is mandated and verified by Information System Security staff. Data is transferred using HTTPS transfer protocol.
VA Investigators	Provide tissue and data to researchers to better understand the pathophysiology of PTSD and Trauma and to develop better therapies.	DNA whole genome sequencing data is biometric data.	Federal Risk and Authorization Management Program (FedRAMP) Compliant encryption at rest and in transit; Two factor user authentication; Network monitoring by various Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools. Compliance to FedRAMP Moderate specified controls is mandated and verified by Information System Security staff. Data is

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*
			transferred using HTTPS transfer 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.
This question is related to privacy control UL-1, Internal Use.

Follow the format below:
Privacy Risk: There is a risk that information may be shared with unauthorized VA program or system or that data could be shared. The privacy risk is potential exposure of the limited data stored in this system. This system does not include the entire VA database but rather the partial data of the subset of research subjects whose information would be currently being processed in the system at the time.

Mitigation: Safeguards implemented to ensure data is not sent to the wrong VA organization are employee security and privacy training and awareness and required reporting of suspicious activity. Use of secure passwords, access granted on a business need to know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access controlsand authorization are all measures that are utilized. This system is protected by a myriad of security features including limited, approved access, encryption, network isolation, 24-hour security monitoring, auditing, security configuration, scanning, patching, personnel security as well as physical security required by FISMA and continually undergoes FISMA standard evaluations and reviews.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
Genomics Vendors	Vendors will provide sequencing results to the PTSD brain bank in support of research projects	Genomics Vendors will sequence tissue samples which generates a biometric identifier. Vendors will be contractually obligated to not attempt to reidentify specimens.	34VA10, Data Use Agreement (DUA) or Memorandum of Understanding (MOU)	FIPS 140.2 or better encrypted hard drives. Other VAEC approved methods transporting encrypted data. Data is

				transferred using HTTPS transfer protocol.
Internal VA Researchers	The PTSD brain bank will supply tissue and data to internal VA researchers in support of research projects	Internal VA investigators will be provided with sequencing data under a fully executed data use agreement with the VA. Investigators will be contractually obligated to not attempt to reidentify specimen and will be required to maintain data security.	34VA10, Data Use Agreement (DUA) or Memorandum of Understanding (MOU)	FIPS 140.2 or better encrypted hard drives. Other VAEC approved methods transporting encrypted data. Data is transferred using HTTPS transfer protocol.
External Researchers	The PTSD brain bank will supply tissue and data to external researchers in support of research projects	External VA investigators will be provided with sequencing data under a fully executed data use agreement with the VA. Investigators will be contractually obligated to not attempt to reidentify specimen and will be required to maintain data security.	34VA10, Data Use Agreement (DUA) or Memorandum of Understanding (MOU)	FIPS 140.2 or better encrypted hard drives. Other VAEC approved methods transporting encrypted data. Data is transferred using HTTPS transfer protocol.

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: Imperfections in the de-identification process. Attempts to potential to re-identify the patient using tools that could assist in identifying patients.

Mitigation: Data transfers are over encrypted secured connections and use specific access rights agreed to by both parties defined in a DUA. Risks are mitigated due to data being deidentified prior to external sharing. VA data are de-identified and shared with a known partner and using a DUA. The partner stores information in a FISMA moderate environment and VA remains the data steward. Risks are mitigated due to data being deidentified prior to external sharing.

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.

We get data from primary sources. Data is only collected for consented patients with the approval of Privacy. Notifications include the standard VA patient notification process notice of privacy practices as well as IRB approved consent forms and HIPAA authorizations.
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=3147

Systems of Record Notice (SORN) 34VA10, "Veteran, Patient, Employee, and Volunteer Research and Development Project Records-VA
https://www.oprm.va.gov/docs/Current_SORN_List_7_1_2022.pdf

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

Yes, in addition to the normal VA standard opportunities and right to decline offered to all patients, only consents are returned and there is no penalty for research protocols. Normal VA practices of "Notice of Privacy Practices" and HIPAA waver.

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

In addition to the normal VA standard processes for right to consent additional research consentforms vary with protocol and are protocol specific. The use is for purpose of research and the defined protocol. Normal VA practices of "Notice of Privacy Practices" and HIPAA waiver. Individuals do not have the right to consent to particular uses of the information.

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:
If the data was released without sufficient notice, there is a potential that the information gathered from the deceased individuals in the database could be used to embarrass or take advantage of family members.

Mitigation: Each protocol stores data in such a way that only approved research team has permissions to access the data. Continual evaluation of consents is done with each new protocol approved. Systems of Record Notice (SORN) 34VA10, "Veteran, Patient, Employee, and Volunteer Research and Development Project Records-VA
https://www.oprm.va.gov/docs/Current_SORN_List_7_1_2022.pdf

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.

VHA Directive 1605.01 Privacy and Release Information', section 7(b) states the rights of the Veterans (or their proxy) to request access to review their records. VA Form 10-5345a, Individual's Request for a Copy of Their Own Health Information, may be used as the written request requirement. All requests to review must be received by direct mail, fax, in person, or by mail referral from another agency or VA office. All requests for access must be delivered to and reviewed by the Records Manager for the concerned VHA system of records, the facility Privacy Officer, or their designee. Each request must be date stamped and reviewed to determine whether the request for access should be granted.

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.

Under the jurisdiction of VHA, VHA Directive 1605.01 'Privacy and Release Information', section 8 states the rights of the Veterans to amend to their records via submitting VA Form 10- 5345a, Individual's Request for a Copy of Their Own Health Information, may be used as the written request requirement, which includes designated record sets, as provided in 38 CFR 1.579and 45 CFR 164.526. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA systemof records, and the facility Privacy Officer, or designee, to be date stamped; and be filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579.

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.

Notification for correcting the information must be accomplished by informing the individual towhom the record pertains by mail. The individual making the amendment must be advised in writing that the record has been amended and provided with a copy of the amended record. The System Manager for the concerned VHA system of records, the facility Privacy Officer, or theirdesignee, must notify the relevant persons or organizations who had previously received the record about the amendment. If 38 U.S.C. 7332-protected information was amended, the individual must provide written authorization to allow the sharing of the amendment with relevant persons or organizations. Request to amend a record must be acknowledged in writing within 10 workdays of receipt. If a determination has not been made within this time period, the System Manager for the concerned VHA system of records or designee, and/or the facility Privacy Officer, or designee, must advise the individual when the facility expects to notify the individual of the action taken on the request. The review must be completed as soon as possible,in most cases within 30 workdays from receipt of the request. If the anticipated completion dateindicated in the acknowledgment cannot be met, the individual must be advised, in writing, of the reasons for the delay and the date the action is expected to be completed. The delay may not exceed 90 calendar days from the receipt of the request.

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.

Request to amend a record must be acknowledged in writing within 10 workdays of receipt. If a determination has not been made within this time period, the System Manager for the concerned VHA system of records or designee, and/or the facility Privacy Officer, or designee, must advise theindividual when the facility expects to

notify the individual of the action taken on the request. The review must be completed as soon as possible, in most cases within 30 workdays from receipt of therequest. If the anticipated completion date indicated in the acknowledgment cannot be met, the individual must be advised, in writing, of the reasons for the delay and the date action is expected tobe completed. The delay may not exceed 90 calendar days from receipt of the request.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:
Privacy Risk: The data within the PTSD Brain Bank is from deceased individuals only. The only risk is to the next of kin. If the decedent was involved in illegal activities or was participating activities that could embarrass the family, the information could be used for blackmail. It could also compromise investigations of the family as the family might be aware that historical information is retained about the decedent.

Mitigation: The PTSD brain bank requires that anyone using the data originating from the brain bank sign a data use agreement that stipulates no attempt to reidentify individuals in the study will be attempted. The DUA also requires that the data is maintained in a safe environment and not shared with third parties without permission.

Section 8. Technical Access and Security

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

8.1 What procedures are in place to determine which users may access the system, and are they documented?

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

Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

Describe the different roles in general terms that have been created to provide access to the system. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

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

Access is defined in the protocol and a list of people with access is defined in the VA Innovation and Research Review System (VAIRRS). To gain access to PTSD Brain Bank, the user's supervisor requests access from a system administrator. The application is behind the VA firewall and is accessible only to VA staff. Any change is approved by an Institutional Review Board (IRB)

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

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

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

VA Contractor access is verified through VA Personnel Security before access is granted to any VA contractor. Contracts and contractor access are reviewed annually at a minimum. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of Behavior training via the Talent Management System (TMS). All contractors are cleared using VA background investigation process and must obtain the appropriate level of background investigation for their role. Contractors with systems administrative access are required to complete additional role-based training prior to gaining system administrator access.

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.

No additional privacy or information security training would be offered specific to the PTSD Brain Bank system. Existing VA privacy and information security trainings are deemed to be sufficient. DVA awareness training consists of VA TMS trainings VA Privacy and Information Security Awareness and Rules of Behavior (ROB), number 10176 and VA Privacy and HIPAA training, courses number 10203. The trainings must be completed annually. Once completed, all information system users will be able to identify the types of information that must be carefully handled to protect privacy; recognize the required information security practices, legal requirements and consequences for non-compliance; and explain how to report incidents as detailed in VA Handbook 6500: Risk Management Framework for VA Information Systems VA Information Security Program. The awareness program is consistent, continuously updated and required for all employees, including contractors and temporary staff.

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

If Yes, provide:

1. *The Security Plan Status,*
2. *The Security Plan Status Date,*
3. *The Authorization Status,*
4. *The Authorization Date,*
5. *The Authorization Termination Date,*
6. *The Risk Review Completion Date,*
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH).*

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

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

No, IOC: June 1, 2023, we are working to get an ATO. The system is classified as a moderate security system.

Section 9 – Technology Usage

The following questions are used to identify the technologies being used by the IT system or project.

9.1 Does the system use cloud technology? If so, what cloud model is being utilized?

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS).

This question is related to privacy control UL-1, Information Sharing with Third Parties.

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1.

Yes. The system is in the process of attaining an ATO. The PTSD Brain Bank system utilizes VAEC AWS.

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract)

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

Yes, handled through VAEC contract number for ECC is NNG15SD22B / VA118-17-F-2284

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.

No.

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

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

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

The principal is described in the customer contract. The project is using VAEC as a Platform as a Service (PaaS).

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).

Not Applicable

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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

Signature of Responsible Officials

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

Stephania H. Griffin 229066

Digitally signed by Stephania H. Griffin 229066
Date: 2022.11.18 09:39:42 -05'00'

Privacy Officer, Stephania Griffin

Karen A. McQuaid 321576

Digitally signed by Karen A. McQuaid 321576
Date: 2022.11.18 08:51:43 -06'00'

Information Systems Security Officer, Karen McQuaid

BERTRAND R. HUBER 424483

Digitally signed by BERTRAND R. HUBER 424483
Date: 2022.11.18 11:33:16 -05'00'

Information Systems Owner, Bertrand Huber

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).

NOPP

https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=3147

Systems of Record Notice (SORN) 34VA10, "Veteran, Patient, Employee, and Volunteer Research and Development Project Records-VA

https://www.oprm.va.gov/docs/Current_SORN_List_7_1_2022.pdf