Privacy Impact Assessment for the VA IT System called:

Veterans Integrated Implant Application Tracking Solution (VIIATS) Assessing

Veterans Health Administration

Healthcare Environment and Logistics Management

eMASS ID 1025

Date PIA submitted for review:

April 11, 2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Phillip Cauthers	Phillip.Cauthers@va.gov	(503) 721-1037
Information System Security Officer (ISSO)	Robert Gaylor	Robert.Gaylor@va.gov	(303) 478-6558
Information System Owner	Steven Zoglman	Steven.Zoglman@va.gov	(720) 857-5301

Abstract

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

Veterans Integrated Implant Application Tracking Solution (VIIATS) is a VA Managed Service web-based Commercial off the Shelf (COTS) SaaS application also known as Unique Device Identifier Tracker (UDITracker), provided by InVita Healthcare Technologies (IHT) that is used to track the life span and chain of custody for implanted tissue as well as implantable medical devices.

Overview

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

1 General Description

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

Veterans Integrated Implant Application Tracking Solution (VIIATS), VHA Healthcare Environment and Logistics Management (HELM)

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

Healthcare Environment and Logistics Management

C. Who is the owner or control of the IT system or project?

VA Controlled/non-VA Owned and Operated

2. Information Collection and Sharing

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

The number of individuals with information to be stored in the system is variable by VA location. It can be scaled to accommodate extremely high volumes of data as required. This system resides on InVita-hosted private servers that are not publicly searchable or accessible. Data entered or transmitted into the application remains owned by the VA, including PHI and PII where it exists. VIIATS is constructed in such a way as to allow minimal storage and transmission of PHI/PHI, specifically requiring only the patient's medical record number (MRN) and Date of Birth. Still, VA facilities can expand this and store additional PII elements if desired.

All data is protected with authentication, encryption, and firewall mechanisms regardless of the data type stored or sent to the system, and all information is considered sensitive and/or confidential when handled by InVita representatives or technicians. The release of privacy-related data by accident or malicious intent would have zero, minor, or moderate effects, depending on the VA's choice to enter additional patient data. The legal authority to operate this system is H.R.28—Biological Implant Tracking and Veteran Safety Act of 2017.

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

Veterans Integrated Implant Application Tracking Solution (VIIATS) is a VA Managed Service web-based COTS SaaS application, UDITracker, provided by InVita Healthcare Technologies (IHT). It tracks the life span and chain of custody for implanted tissue and implantable medical devices utilizing Unique Device Identifiers required by the FDA and Joint Commission. Access to the secure site is provided through VPN, data is stored in, and data is stored on an offsite secured database server. All customer information is contained within its own isolated database, never intermingled with other customers. In addition, each VA customer site has its own customized web address to access their own customized web address to access its version of the application. The VIIATS/UDITracker application resides on IHT private servers hosted in the Rackspace private cloud. Data entered or transmitted into the application is owned by the VA, including PHI and PII where it exists. VIIATS is constructed in such a way as to allow minimal storage and transmission of PHI/PHI, specifically requiring only the patient medical record number (MRN) and Date of Birth. Still, VA facilities can expand this and store additional PII elements if desired.

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

VIIATS receives information from the facilities' Radio Frequency Identification (RFID) and Bar Code Scanning to assist with tracking implantable devices. This information is also shared with VistA.

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

Veterans Integrated Implant Application Tracking Solution (VIIATS) is a VA Managed Service web-based COTS SaaS application, UDITracker, provided by InVita Healthcare Technologies (IHT). Access to the secure site is provided through a VPN, and data is stored on an offsite secured database server. All customer information is contained within its own isolated database, never intermingled with other customers. In addition, each VA customer site has its own customized web address to access their own customized web address to access its version of the application. The VIIATS/UDITracker application resides on IHT private servers hosted in the Rackspace private cloud. The VA owns data entered or transmitted into the application, including PHI and PII, where it exists. VIIATS is constructed in such a way as to allow minimal storage and transmission of PHI/PHI, specifically requiring only the patient's medical record number (MRN) and Date of Birth. Still, VA facilities can expand this and store additional PII elements if desired. All data is protected with authentication, encryption, and firewall mechanisms regardless of the data type stored or sent to the system, and all information is considered sensitive and/or confidential when handled by InVita representatives or technicians.

3. Legal Authority and SORN

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

24VA10A7/85 FR 62406 – "Patient Medical Records–VA", [*https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf*](https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf). Authority for maintenance of the system: Title 38, United States Code, Sections 501(b) and 304.

79VA10 /85 FR 84114 – "Veterans Health Information Systems and Technology Architecture (VistA) Records-VA", https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf. Authority for maintenance of the system: Title 38, United States Code, section 7301(a).

I. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?

The SORNs do not need to be modified at this time.

4. System Changes

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

This change will not impact the business processes.

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

No.

Section 1. Characterization of the Information

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

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

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

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

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

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

☒ Name
☒ Social Security Number
☒ Date of Birth
☐ Mother's Maiden Name
☐ Personal Mailing Address

☐ Personal Phone Number(s)
☐ Personal Fax Number
☐ Personal Email Address
☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
☐ Financial Information
☐ Health Insurance Beneficiary Numbers Account numbers
☐ Certificate/License numbers[1]
☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☐ Medications
☐ Medical Records
☐ Race/Ethnicity
☐ Tax Identification Number
☐ Medical Record Number
☐ Gender
☐ Integrated Control Number (ICN)
☐ Military History/Service Connection
☐ Next of Kin
☒ Other Data Elements (list below)

Other PII/PHI data elements: First initial last name along with last 4 of Social Security Number, Surgical Staff, Date of Surgery, UDI Device (Lot, Serial Number, Expiration Date), Patient ID.

PII Mapping of Components (Servers/Database)

VIIATS consists of 2 key components (servers/databases/instances/applications/software/application programming interfaces (API). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by VIIATS and the reasons for the collection of the PII are in the table below.

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

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
DB5	**Yes**	**Yes**	First initial of last name • DOB • Last four of the SSN	**Bi-directional tracking/recall**	**Encrypted**

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

			• Date of Surgery • Patient ID Surgical Staff • UDI Device/Product o ID/Serial Number o Lot/Expiration Date		
DB6	**Yes**	**Yes**	First initial of last name • DOB • Last four of the SSN • Date of Surgery • Patient ID Surgical Staff • UDI Device/Product o ID/Serial Number o Lot/Expiration Date	**Bi-directional tracking/recall**	Encrypted

1.2 What are the sources of the information in the system?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.2a List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

1. VA Healthcare provider/staff
2. VISTA system

1.2b Describe why information from sources other than the individual is required? For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question indicate why the system is using this source of data.

The information indicated above is added by VA healthcare provider users or inventory management specialists (receiving dock workers when receiving shipments) or linked with VistA. Patients do not need to enter this information directly since this is not a patient/direct critical care application.

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

VIIATS has its own Analytics system that uses the above data fields for users to create their own reports. Reports can be created by the individual user of the program using any combination of the data collected.

1.3 How is the information collected?

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

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

Information is sent via Health Level 7 (HL7) communication from VistA surgical package, scanned in from the patient wrist band (issued from the facility), or typed in manually by the surgical staff.

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

No associated physical forms are required for VIIATS.

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

These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

The program tracks surgically implantable devices in Veterans. Its primary purpose is to assist with managing recalls of these products. With the PII information being used, this process is now done electronically and at a greater speed than ever before. This process previously would take weeks of manual work with a 10% to 20% error rate. Using the VIIATS program, the same research is done in seconds with 100% accuracy. The PII information is used to identify the patients and the products correctly. The implant device is identified by a barcode.

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

This does not apply; no commercial aggregator can access information. IHT receives notifications from the Federal Drug Administration (FDA) and updates VIIATS as applicable.

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

- *24VA10A7/85 FR 62406 – "Patient Medical Records–VA", https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf.* Authority for maintenance of the system: Title 38, United States Code, Sections 501(b) and 304.
- *79VA10 /85 FR 84114 – "Veterans Health Information Systems and Technology Architecture (VistA) Records-VA", https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf.* Authority for maintenance of the system: Title 38, United States Code, section 7301(a).
- Food and Drug Administration Amendments Act of 2007.
- U.S. Food and Drug Administration (FDA) (§1271.290(c)).

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: The system collects, processes, and retains PII and PHI on Veterans and Employees (. If this information was breached or accidentally disclosed to inappropriate parties, the risk is considered to be moderate. There is a risk that the information maintained by VIIATS could be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released, breached, or exploited for reasons other than what is described in the privacy documentation associated with the information.

Mitigation: VIIATS is protected using authentication, encryption, firewalls, monitoring, and a wide array of other security tools and measures. Internal and independent testing is conducted regularly to ensure systems remain impenetrable. Risk assessment is performed on an ongoing basis. The magnitude of harm if data were to be disclosed is low to moderate, depending upon what information the VA chooses to store. All users are required to use Active Directory Federation Services (ADFS) Single Sign-on (SSO).

Section 2. Uses of the Information

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

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

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

PII/PHI Data Element	Internal Use	External Use
DOB; First initial of last name along with last four of the SSN; Date of Surgery; Surgical Staff, UDI Device: Lot, Serial Number, and Expiration Date	File Identification purposes	Not Applicable

2.2 What types of tools are used to analyze data and what type of data may be produced?
These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis?

VIIATS's data can be obtained through customizable MySQL reporting when requested by VA Admin users. The VA confirms to the greatest extent practicable upon collection or

creation of personally identifiable information (PII), the accuracy, relevance, timeliness, and completeness of that information, collects PII directly from the individual to the greatest extent practicable, checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems every 180 days, and issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information. VIIATS confirms the accuracy of collecting or creating personally identifiable information (PII) by enforcing the Notice of Privacy Practices and the Records Management policies. A VIIATS PTA, PIA, and SORN are completed.

2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

VIIATS does not create any information. The information is entered into VIIATS by a licensed healthcare provider. Any required changes will be accomplished by the licensed healthcare provider. The information put into VIIATS is then sent to the VistA nursing notes.

2.3 How is the information in the system secured?

These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

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

VIIATS is protected using authentication, encryption, firewalls, monitoring, and a wide array of other security tools and measures. Internal and independent testing is conducted regularly to ensure systems remain impenetrable. Risk assessment is conducted on an ongoing basis. The magnitude of harm if data were to be disclosed is low to moderate, depending upon what information the VA chooses to store. VIIATS incorporates SHA-256, TLS 1.2, AES-256.

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

VIIATS only collects the last 4 of the SSN and is encrypted in transit and at rest.

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

VA Administrators control access to PII and PHI, which can be restricted using the role-based access built into the VIIATS system. Any view or modification of PII/PHI is logged by username, record number, details of the event, and date/time. InVita manages general program safeguards and VA Administrators are able to additionally audit the activity related to PII/PHI within the VIIATS program. With regard to VA workers, access to PII is limited to those who have direct patient care in surgical services, along with administrative staff who oversee the program.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. Example: Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.

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

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

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

2.4a How is access to the PII determined?

Role-based access is determined by the user's role and the Facility Implant Coordinator.

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

The Privacy Officer presents to new employees during New Employee Orientation (NEO) for Privacy and HIPAA. New employees are registered in Training Management System (TMS) and subsequent annual training is completed via computer. The Privacy Officer has Information Security and HIPAA training reports that can be requested from the TMS administrator and sent via email, which display the names of the employees, contractors, and volunteers compliant/delinquent on training and service areas. The Privacy Officer has a TMS Domain Summary for the overall HIPAA/Privacy Training compliance rate. Supervisors have access to run TMS reports on staff to ensure training is not delinquent.

2.4c Does access require manager approval?

Yes, all accesses must go through and be approved by the Facility Implant Coordinator.

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

The privacy and security control review is accomplished annually, and controls are updated if changes are made. The organization defines the frequency as "Continuous" for the monitoring and auditing both privacy controls and internal privacy policy to ensure effective implementation. A PTA is accomplished annually, and a PIA is accomplished every three years or when changes are required.

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

This is a coordinated effort between all VIIATS users and IHT administrators.

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*

Information retained includes DOB, Medical Record Number that includes the First initial of last name along with the last four of the SSN, Date of Surgery, Surgical Staff, and UDI Device information: Lot Serial Number and Expiration Date.

3.2 How long is information retained?

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

All data in the system is kept for an indefinite period for recall purposes. Joint Commission requirements indicate that data should be kept for 10 years at a minimum. InVita does not purge information on an automated basis; information is kept indefinitely unless upon written request. IHT follows guidelines laid out in SORN 24VA10A7, which states that electronic storage media containing health information are maintained for seventy-five (75) years after the last episode of patient care.

Employee information collected by the system maintained under SORN 79VA10 and is destroyed 3 years after agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated or superseded, but longer retention is authorized if required for business use.

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

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule.

The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner. Please work with the system Privacy Officer and VA Records Officer to answer these questions.
This question is related to privacy control DM-2, Data Retention and Disposal.

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

Records Control Schedule (RCS) 10-1 https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf , January 2021. Paper records and information stored on electronic storage media are maintained and disposed of in accordance with records disposition authority approved by the Archivist of the United States and VA policies and procedures for media sanitization, (SORNs 24VA10A7).

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

All data in the system is kept for an indefinite period for recall purposes. Joint Commission requirements indicate that data should be kept for a period of 10 years at a minimum. InVita does not purge information on an automated basis, information is kept indefinitely unless upon written request. IHT follows guidelines laid out in SORN 24VA10A7,which states that electronic storage media are maintained for seventy-five (75) years after the last episode of patient care (VHA Records Control Schedule (RCS 10–1) rcs10-1.pdf (va.gov), Chapter 6, 6000.1d (N1–15–91–6, Item 1d) and 6000.2b (N1–15–02–3, Item 3). SORN 24VA10A7.

Employee information collected by the system maintained under SORN 79VA10 and is destroyed 3 but longer retention is authorized if required for business use. VHA Records Control Schedule (RCS 10–1) rcs10-1.pdf (va.gov), Item 2000.2 with disposition authority DAA–GRS–2013–0005– 0004, and item 020 and Item 2100.3 with disposition authority DAA–GRS–2013–0006– 0004, item 31. SORN 79VA10.

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

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

Any sensitive paper records are shredded on-site in accordance with NIST standards. After final disposition, the contractor provides a certificate of destruction. Electronic media containing individually identifiable information is destroyed per NIST guidelines. Defective or damaged magnetic storage media used in a sensitive environment shall not be returned to the vendor (and will be annotated in all contracts/Statements of Work). The IT Area Manager, Information Security Officer (ISO), or designees will be responsible for this process.

Other Data that is not destroyed at the production site, such as that which is transported for destruction, is secured in locked containers or locked areas until it is removed for destruction. The media en route to final disposition is rendered unreadable before transport. 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. Once the records retention period has been met or records have been otherwise deemed appropriate to destroy, paper records are cross-cut shredded on-site (for records stored or used at InVita facilities) or sent to a secure shredding provider. Physical media such as hard drives or electronic storage items are electronically wiped/degaussed and then physically destroyed by shattering, bending platters, or otherwise demolished. This again may be performed on-site for InVita facility equipment, at the data center, or decommissioned by a secure destruction vendor.

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

IHT does not use VIIATS information for research, testing or training.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that PII or PHI may be held longer than it is required to be maintained. This extension of the retention period increases the risk that information may be breached or otherwise put at risk of access by unauthorized persons.

Mitigation: Data is only retained as necessary for its intended purpose. PII is only retained for as long as necessary and relevant for the purpose for which it was created. Program officials are responsible for disposing of records in their program area in accordance with VA policy SORN 24VA10A7. Staff is required to take the Records Management course via TMS, which outlines the process for the retention and purging of data. The VA also follows the Records Control Schedule (RCS) 10-1, schedules for each category or data it maintains. When data retention is reached, data will be disposed of in accordance with the approved method at the time.

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***
InVita bilateral communication with VistA Surgical Package/GIP/PIP	Data needs to be sent between the systems in order to fill out the required information on the Veterans' implants for tracking purposes.	1. First initial, last name, and last 4 of Social Security Number. 2. Date of Surgery 3. Surgical Staff 4. UDI Device: a. Lot b. Serial Number c. Expiration Date	VPN Tunnel / HTTPS Connection

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: The privacy risk associated with maintaining PII and PHI is that sharing data within the Department of Veterans Affairs could happen and that the data may be disclosed to individuals who do not require access heightens the threat of misused information.

Mitigation: The InVita Healthcare Technologies personnel strictly adhere to the principle of need-to-know. Only personnel with a clear business purpose are allowed access to the system and the information contained within. Safeguards are implemented to ensure data is not sent to unauthorized VA employees, including employee security and privacy training and required reporting of suspicious activity. Access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information integrity, security assessment, and authorization, incident response, risk assessment, program management, planning, and maintenance. Privacy measures will include authority and purpose, accountability, audit and risk management, data quality and integrity, data minimization and retention, individual participation and redress, transparency, and use limitation.

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***
Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable

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.

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

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

Follow the format below:

Privacy Risk: There is no external sharing.

Mitigation: There is no 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 6.1 on the last page of the document. Also provide notice given to individuals by the source system (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

6.1a This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

Notice is provided in multiple ways:

The VHA Notice of Privacy Practice (NOPP) https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946 explains the collection and use of protected health information to individuals receiving health care from VA. The NOPP

is mailed every three years or when there is a major change to all enrolled Veterans. Non-Veterans receiving care are provided the notice at the time of their encounter.

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

A Privacy Act Statement is provided on all forms that collect information that will be maintained in a privacy act system of records. The statement provides the purpose, authority, and the conditions under which the information can be disclosed.

Notice is also provided in the Federal Register with the publication of the SORNs *24VA10A7/85 FR 62406 – "Patient Medical Records–VA" and 79VA10 /85 FR 84114 – "Veterans Health Information Systems and Technology Architecture (VistA) Records-VA".*

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

Notice has been provided as described above. Links to the notices are provided in Appendix A.

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

Notice is provided through the VA Notice of Privacy Practices, this Privacy Impact Assessment, which is available online, as required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs and the following VA System of Record Notices (SORNs) which are published in the Federal Register and available online: Patient Medical Records-VA, SORN 24VA10A7, Veterans Health Information Systems and Technology Architecture (VistA) Records-VA, SORN 79VA10.

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.

Information is requested when it is necessary to administer benefits to veterans and other potential beneficiaries. While an individual may choose not to provide information, this may prevent them from obtaining the benefits necessary to them. The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VHA an SSN (see 38 CFR 1.575(a)).

Employees and VA contractors are also required to provide the requested information to maintain employment or their contract with *VHA.*

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.

Individuals are provided with a copy of the Notice of Privacy Practices that indicates when information will be used without their consent and when they will be asked to provide consent. Information is used, accessed and disclosed in accordance with the Privacy Act, 5 USC 552a, Title 38 USC 5701, Confidential Nature of Claims, Title USC 7332 and the HIPAA Privacy Rule 45 CFR.

Individuals or their legal representative may consent to the use or disclosure of information via a written request submitted to their facility Privacy Officer. Individuals also have the right to request a restriction to the use of their information. The written request must state what information and/or to whom the information is restricted and must include their signature and date of the request. The request is then forwarded to facility Privacy Officer for review and processing. Individuals may also request to Opt-Out of the facility directory during an inpatient admission. If the individual chooses to opt-out, information is not disclosed from the facility directory unless otherwise required by law.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

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

Privacy Risk: There is a risk that an individual may not receive notice that their information is being collected, maintained, processed, or disseminated by the Veterans' Health Administration and the local facilities prior to providing the information to the VHA.

Mitigation: This risk is mitigated by the common practice of providing the NOPP when Veterans apply for benefits. Additionally, new NOPPs are mailed to beneficiaries at least every 3 years and periodic monitoring is performed to check that all employees are aware of the

requirement to provide guidance to Veterans and that the signed acknowledgment form, when applicable, is scanned into electronic records. The NOPP is also available at all VHA medical centers from the facility Privacy Officer.

The System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) are also available for review online, as discussed in question 6.1.

Section 7. Access, Redress, and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

7.1 What are the procedures that allow individuals to gain access to their information?

These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. ***For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at https://department.va.gov/foia/foia-requests/ to obtain information about FOIA points of contact and information about agency FOIA processes.***

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

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

Employees should contact their immediate supervisor and Human Resources to obtain information. Contractors should contact Contract Officer Representative (COR) to obtain information upon request.

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

The system is not exempt.

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

The information collected by the system falls under a Privacy Act System of Records.

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

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

Individuals are required to provide a written request to amend or correct their records to the appropriate Privacy Officer or System Manager as outlined in the Privacy Act SOR. Every Privacy Act SOR contains information on Contesting Record Procedure which informs the individual who to contact for redress. Further information regarding access and correction procedures can be found in the notices listed in Appendix A. The VHA Notice of Privacy Practices also informs individuals how to file an amendment request with VHA.

7.3 How are individuals notified of the procedures for correcting their information?

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

Veterans are informed of the amendment process by many resources to include the VHA Notice of Privacy Practice (NOPP) which states:

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

Individuals seeking information regarding access to and contesting of VA benefits records may write, call or visit the nearest VA regional office.

Additional notice is provided through the SORS listed in 6.1 of this PIA and through the Release of Information Office where care is received.

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

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

All individuals have a formal redress process via the amendment process. In addition to the formal procedures discussed in question 7.3 to request changes to one's health record.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that individual may not know how or who to seek to access or redress records about them held by the VA Office.

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

The Release of Information (ROI) office is available to assist Veterans with obtaining access to their health records and other records containing personal information.

The Veterans' Health Administration (VHA) established MyHealtheVet program to provide Veterans remote access to their medical records. The Veteran must enroll and have access to the premium account to obtain access to all the available features. In addition, VHA Directive 1605.01 Privacy and Release of Information establishes procedures for Veterans to have their records amended where appropriate.

Section 8. Technical Access and Security

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

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

These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.

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

Access to VASLCHCS working and storage areas is restricted to VA employees who must complete HIPAA and Information Security training. Specified access is granted based on the employee's functional category. Role-based training is required for individuals with significant information security responsibilities, including but not limited to Information Security Officer (ISO), local Chief Information Officer (CIO), System Administrators, Network Administrators, Database Managers, Users of VA Information Systems or VA Sensitive Information.

Access is requested per local policies utilizing the Network Access Request System (NARS). Users submit access requests based on need-to-know and job duties. Supervisor and OIT approval must be obtained prior to access being granted. These requests are submitted to VA employees, contractors, and all outside agency requests and are processed through the appropriate approval processes. Once access is granted, individuals can log into the system(s) through dual authentication, (i.e., a PIV card/ADFS). Once inside the system, individuals are authorized to access information on a need-to-know basis.

Strict physical security control measures are enforced to ensure that disclosure to these individuals is also based on this same principle. Generally, VA file areas are locked after regular

duty hours, and the Federal Protective Service or other security personnel protect the facilities from outside access.

Access to computer rooms at the computer facilities is limited by appropriate locking devices and restricted to authorized vendor personnel. Automated Data Processing (ADP) peripheral devices are placed in secure areas (locked or limited access) or otherwise protected areas—individually unique codes control access to information stored on automated storage media.

Only users employed/contracted by the VHA have access to the system. Access digital audit trails are documented through the Administrator's input when accounts are created, and this access is tracked through the applicable system through logging.

8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

There are no users from other agencies.

8.1c Describe the different roles in general terms that have been created to provide access to the system? For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

Standard User: Typical medical employees hired within the facility to perform duties within a specific service. These users can access only the information systems/data required to perform their duties.

OIT Administrator: These users have elevated privileges necessary to perform administrative and system management duties required in OIT operations.

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.

Contractors will have access to the system(s) only for which they have been designated/approved access per contractual agreements. Contracts are reviewed annually by the Contracting Officer Representative (COR) to determine access requirements. Contractors with access to PHI/PII must complete a Business Associate Agreement. Access to the system depends on the contractual requirements for support (i.e., remote server/workstation admin duties).

Vendors requesting access to VHA systems are required to undergo background investigations and receive clearance from an ISO prior to account creation. The ISO/CRO conducts all reviews.

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.

All VA staff (employees, volunteers and without compensation (WOCs), residents, students) that need computer access or has access to PII/PHI must complete the annual VA Privacy and Information Security Awareness training and Rules of Behavior and Privacy—HIPAA-focused training, in addition to job-specific information training that is required for different positions.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Completed
2. *The System Security Plan Status Date:* 01/29/2024
3. *The Authorization Status:* Authorization to Operate
4. *The Authorization Date:* 04/01/2024
5. *The Authorization Termination Date:* 09/28/2024
6. *The Risk Review Completion Date:* 03/19/2024
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

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

Section 9 – Technology Usage

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

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

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1*. (Refer to question 3.3.1 of the PTA)*

VIIATS does not use cloud technology.

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

VIIATS does not use cloud technology.

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.

VIIATS does not use cloud technology.

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.

VIIATS does not use cloud technology.

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).

VIIATS does not utilize RPA.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

PHILLIP CAUTHERS

Digitally signed by PHILLIP CAUTHERS
Date: 2024.05.09 15:31:03 -07'00'

Privacy Officer, Phillip Cauthers

DN: c=US, o=U.S. Government, ou=Department of Veterans Affairs, ou=People, cn=ROBERT GAYLOR, 0.9.2342.19200300.100.1.1=1009696760136001
Date: 2024.05.09 07:09:40 -06'00'

Information Systems Security Officer, Robert Gaylor

STEVEN ZOGLMAN

Digitally signed by STEVEN ZOGLMAN
Date: 2024.05.09 06:42:20 -06'00'

Information Systems Owner, Steven Zoglman

APPENDIX A-6.1

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

VHA Notice of Privacy Practices

24VA10A7/85 FR 62406 – "Patient Medical Records–VA", https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf.

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

HELPFUL LINKS:

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

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

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

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

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