Privacy Impact Assessment for the VA IT System called:

Enterprise Testing Services Test Center (ETSTC)

Executive Program Management Office

Date PIA submitted for review:

<< January 8, 2021 >>

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Rita Grewal	Rita.Grewal@va.gov	202/ 632-7861
Information System Security Officer (ISSO)	Amine Messaoudi	Amine.Messaoudi@va.gov	202/ 815-9345
Information System Owner	Anthony Jones	Anthony.Jones16@va.gov	727/ 320-1977

Abstract

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

<<The Enterprise Testing Services Test Center (ETSTC) delivers a highly scalable, secure and innovative service that allows organizations to seamlessly migrate and extend their on-premises VMware vSphere-based environments to the Amazon Web Services (AWS) Cloud. This will provide customer access to all geographic locations and enhance on premises services. This allows our customers access respective databases for integral testing of applications provide a standard repository for the databases and access in the event of a Test Center outage or unavailability.
Lastly, we provide test systems to various projects in order to validate the accuracy and completeness of the respective products/applications.>>

Overview

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

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *If your system is a regional GSS, VistA, or LAN, include a list of the hospitals/medical centers, or other regional offices that fall under your system. Additionally, what region is the system under?*
- *A general description of the information in the IT system.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.*
- *A citation of the legal authority to operate the IT system.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*
- *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval?*
- *Does the system use cloud technology? If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517.*

- *Does a contract with Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII?*
- *NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?*
- *What is the magnitude of harm if privacy related data is disclosed, intentionally or unintentionally? Would the reputation of the CSP or its customers (VA) be affected?*

<<The Bay Pines Enterprise Testing Services Test Center (ETSTC) initially collects information of over 400k veterans and over 1000 contractors and VA employee information through the transfer of patient databases from several Health Care Systems throughout the Department of Veterans Affairs.

The Region 3 VistA boundary was newly created in 2013 when the Office of Information and Technology made major changes to VA systems and their security boundaries. Although the Regional 3 VistA information system boundary does provide security oversight and a variety of support functions to the facilities and their local VistA Systems, data ownership remains at the facility level and many of the decisions related to the collection, use, storage, and dissemination of the data are made at the facility level.

The Bay Pines Enterprise Testing Services Test Center (ETSTC) is administered by Testing Systems Engineering & Implementation (TSEI) personnel only utilizing an approved Electronic Permission Access system (ePAS). All user access will be vetted by TSEI utilizing and tracking via the 9957 Security form. ETSTC supports the development and testing of applications for VA teams before applications are released to production. Currently, the ETSTC instance is comprised of Windows and Linux virtual machines; which have databases such as Structured Query Language (SQL) databases, Cache databases, Oracle; applications such as Joint Legacy Viewer (JLV), Master Veteran Index (MVI), Person Service - Identity Management (PSIM), IMDQ TK, Mobile Device Management (MDM), Enrollment System Redesign (ESR), Primary Care Management Module (PCMM), Veterans Data Integration and Federation (VDIF) HealthShare Enterprise HealthConnect (HSE HC) and the supporting databases, Alternative Dispute Resolution (ADR), Safety Data Sheets (SDS); and supporting test and monitoring tools.

The Bay Pines Enterprise Testing Services Test Center (ETSTC)'s VistA hardware is located within the C.W. Bill Young Department of Veterans Affairs Medical Center, Bay Pines VA Healthcare System Campus, building 37 room 300 and has been fully operational since 1999.

The Bay Pines Enterprise Testing Services Test Center (ETSTC) staff independently decides whether or not to share data with other sources as stated throughout this document. The Bay Pines Enterprise Test Center conducts a variety of information sharing internal and external to the Department of Veterans Affairs. Internal sharing is discussing in greater detail in Section 4 of this Privacy Impact Assessment (PIA). This type of sharing is done to ensure that mission essential testing can be conducted utilizing shared patient data. External sharing, which is discussed in greater detail in Section 5 of this PIA is done with other agencies and organizations.

The legal authorities to operate the VistA system are Title 5, United States Code, section 301, Title 38, United States Codes, sections 109, 111, 501, 1703, 1705, 1710, 1712, 1717, 1720, 1721, 1724, 1725, 1727, 1728, and 7105 and Title 38, United States Code, Section 7301 (a).>>

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.

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

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

Other Unique Identifying Numbers: This system also collects: next of kin, any clinical notes, and appointments.

PII Mapping of Components

Bay Pines Enterprise Testing Services Test Center (ETSTC) consists of **two** key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Bay Pines Enterprise Testing Services Test Center (ETSTC) and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

PII Mapped to Components

Components of the information system (servers) 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
Vhaispdbsmstr01, Vhaispdbsmstr02, Vhaispopspclg11	No	Yes - (Temporarily for the purpose of de-identification)	SSN,DOB,Address,Contact Info, clinical data	One-time transfer of the database from facility. Once the database is received, it is de-identified before using the database for testing	Data is transferred using secure File Transfer Protocol (FTP) Secure FTP (SFTP) or tools that VA Approved and used with in the Facility such as CommVault etc. for transferring. Once de-identified the raw data that is received is deleted.

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 ETSTC is located in Bay Pines, Florida, and contains a large amount of data on a wide variety of individuals and with the sources of data being varied.

The information collected, maintained and/or disseminated by the **Bay Pines Enterprise Testing Services Test Center (ETSTC)** comes from a variety of resources. The largest amount of data consists of veteran patient data from various VA Healthcare systems. That data is de-identified before use in the **Bay Pines Enterprise Testing Services Test Center (ETSTC).**

The de-identified data the **Bay Pines Enterprise Testing Services Test Center (ETSTC)** houses (in the form of databases) is also provided to other organizations within the VA, including:

- VA Enterprise Cloud (VAEC)
- Community Resource and Referral Centers (CRRCs)

The de-identified data that is required for respective applications such as enrollment, patient demographics, clinical records and any other data required by the OEHRM interfaces is shared with Cerner test instances located in Cerner cloud.>>

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.

This system collects all patient data (name, SSN, billing and prescription information, address, phone number, email address, next of kin, any clinical notes, and appointments), which is then de-identified thereby creating test data in the respective systems and transmitted to the necessary interfaces depending on the test events at a given time. >>

1.4 What is the purpose of the information being collected, used, disseminated, created, or maintained?

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

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

Data that is used is either de-identified data or fresh test data is created by the test teams to meet the functionality of the respective Commercial Off the Shelf (COTS) and Government Off the Shelf (GOTS) applications that are under a test event at a given time within OIT and/or OEHRM.

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

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

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

The data is all de-identified data and test data, so the respective team teams will validate their applications manually or create additional test data as needed.

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

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

The **Bay Pines Enterprise Testing Services Test Center (ETSTC)** is a facility level entity that operates under the authority of Veterans Health Administration – Organization and Functions, Title 38, U.S.C., Chapter 73, § 7301(a)

Additionally, the collection, processing, and dissemination of health information must follow the rules and regulations established by the:

- Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191 (Aug. 21, 1996), (codified in scattered sections of title 42 U.S. Code) (full-text); 45 C.F.R. parts 160 and 164 (HIPAA Privacy and Security Rules).
- Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5, 123 Stat. 226 (Feb. 17, 2009), codified at 42 U.S.C. §§300jj et seq.; §§17901 et seq.>>

1.7 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

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

Follow the format below when entering your risk assessment:
Privacy Risk: **Bay Pines Enterprise Testing Services Test Center (ETSTC)** VistA Databases contains sensitive personal information – including social security numbers, names, dates of birth and protected health information – on veterans, members of the public, & VA employees and contractors. Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious harm or even identity theft may result.

Mitigation: Veterans Health Administration (VHA), Region 3 as well as the **Bay Pines Enterprise Testing Services Test Center (ETSTC)** center deploy extensive security measures to protect the information from inappropriate use and/or disclosure through both access controls and training of all employees and contractors within the region. Region 3's security measures include 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, planning and maintenance, accountability, audit and risk management, data quality and integrity, data minimization and retention, individual participation and redress, transparency and use limitation.

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 de-identified test data is utilized by various OIT test efforts and OEHRM test efforts.

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

VA Developed VistA routines are used for running "reset utility" and for "deidentifying" the data. The respective application test teams create their own test data (from the issued de-identified data) to test the respective applications.

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

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

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

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

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

The controls in place to assure that the information is handled in accordance with the uses described above include mandatory online information security and HIPAA training; face-to-face training for all incoming employees conducted by the Information Security Officer and Privacy Officer; regular audits of individuals accessing sensitive information; and formal audits of systems and accounts to ensure information is appropriately accessed and controlled.

Prior to the granting of access to our databases, all users are required to agree to and sign a custom Security Form VA9957 with conditions and controls unique to our environment.

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

Bay Pines Enterprise Testing Services Test Center (ETSTC) follows national VA policies regarding information retention. The records include information concerning current and former employees, applicants for employment, trainees, contractors, sub-contractors, contract personnel, students, providers and consultants, patients and members of their immediate family, volunteers, maintenance personnel, as well as individuals working collaboratively with VA.

3.2 How long is information retained?

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

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

When managing and maintaining VA data and records, the **Bay Pines Enterprise Testing Services Test Center (ETSTC)** will follow the guidelines established in VA Record Control Schedule (RCS)-10 (http://www1.va.gov/vhapublications/RCS10/rcs10-1.pdf) as well as RCS 005-1(http://www.oprm.va.gov/docs/RCS005-1-OIT-8-21-09.pdf).

These documents specify how long records will be retained by the VA, if/when they will be transferred to a national records storage location, and the length of time the records will be stored at the national level.

For greater details related to records retention at the Veterans' Health Administration, please review RCS-10 and RCS-005-1.

Below are some key record retention schedules for your information:

Medical Records Folder File or CHR (Consolidated Health Record): These records contain all professional and administrative material necessary to document the episodes of medical care and benefits provided to individuals by the VA health care system. The medical records folder will be retained in the VA health care facility until 3 years after last episode of care, and then converted to an inactive medical record. Once designated an inactive medical record, it will be moved to a Federal records storage facility. Patient medical records are retained for a total of 75 years after the last episode of care. (Department of Veterans Affairs Record Control Schedule (RCS)-10, Part Three, Chapter Six-Healthcare Records, Item 6000.1a. and 6000.1d. (May 2016)).

Official Human Resources Personnel File: Folder will be transferred to the National Personnel Records Center (NPRC) within 30 days from the date an employee leaves the VA. NPRC will destroy 65 years after separation from Federal service. (Department of Veterans Affairs Record Control Schedule (RCS)-10, Part Two, Chapter Three-Civilian Personnel, Item No. 3000.1 (May 2016)).

Financial Records: Different forms of financial records are retained 1-7 years based on specific retention schedules. Please refer to VA Record Control Schedule (RCS)-10, Part Two, Chapter Four-Finance Management (http://www1.va.gov/vhapublications/RCS10/rcs10-1.pdf) for specific guidelines.

Office if Information & Technology (OI&T) Records: These records are created, maintained and disposed of in accordance with Department of Veterans Affairs, Office of Information & Technology RCS 005-1 (August 3, 2009). Please refer to VA Records Control Schedule (RCS)-05 (http://www.oprm.va.gov/docs/RCS005-1-OIT-8-21-09.pdf) for specific guidelines.

Additionally, under OMB and NARA guidelines, the **Bay Pines Enterprise Testing Services Test Center (ETSTC)** will reference the Records Management Resources within the General Records Schedule. These specific resources can be found at http://www.archives.gov/records-mgmt/grs/.

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 **Bay Pines Enterprise Testing Services Test Center (ETSTC)** will follow the guidelines established in the NARA-approved Department of Veterans' Affairs Record Control Schedule (RCS)-10 (http://www1.va.gov/vhapublications/RCS10/rcs10-1.pdf); Department of Veterans Affairs, Office of Information & Technology RCS 005-1(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

Paper documents are destroyed to an unreadable state in accordance with the Department of Veterans' Affairs VA Directive 6371, (April 8, 2014), http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=742&FType=2

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 the Department of Veterans' Affairs Handbook 6500.1, Electronic Media Sanitization (November 3, 2008), http://www.va.gov/vapubs/ viewPublication.asp?Pub_ID=416&FType=2. 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 per VA Handbook 6500.1. Digital media is shredded or sent out for destruction per VA Handbook 6500.1.

Additionally, the **Bay Pines Enterprise Testing Services Test Center (ETSTC)** follows Field Security Service (FSS) Bulletin for Media Sanitization Program, SOPs - FSS - All Documents as well as FSS Standard Operating Procedures (SOP) MP-6 Electronic Media Sanitization.

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

De-identified data is what will be provided to the organizations/teams; teams also create their own test data.

The PII data that will be received from the facility is done thru a secure transfer within VA network and delete the data after the database is de-identified.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks.

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

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

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

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

Follow the format below:
Privacy Risk: There is a risk that the information maintained by the **Bay Pines Enterprise Testing Services Test Center (ETSTC)** could be retained for longer than is necessary to fulfill VA authorized testing requirements. Records held longer than required are at greater risk of being unintentionally released or breached.

Mitigation: In addition to collecting and retaining only information necessary for fulfilling the **Bay Pines Enterprise Testing Services Test Center (ETSTC)** mission, the disposition of data housed is based on standards developed by the National Archives Records Administration (NARA). This ensures that data is held for only as long as necessary.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA. NOTE: Question 5 on Privacy Threshold Analysis should be used to answer this question.

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

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

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

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

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?
This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

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 data element types such as PII/PHI that are shared/received with the Program Office or IT system***	***Describe the method of transmittal***
Cerner	Assistance in the testing of patient data.	Pertinent PII, PHI, and III appropriate to the request. This system collects all patient data (name, SSN, billing and prescription information, address, phone number, email address, next of kin, any clinical notes, and appointments)	Secured data connections (e.g. TTLS, SSL, HTTPS, SFTP, etc.), through encrypted emails.

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 data element types such as PII/PHI that are shared/received with the Program Office or IT system*	*Describe the method of transmittal*
Chalmers P. Wylie Ambulatory Care Center (Columbus)	One-time transfer of the facility database	PII,PHI This system collects all patient data (name, SSN, billing and prescription information, address, phone number, email address, next of kin, any clinical notes, and appointments)	Secure FTP
Cheyenne Veterans Affairs Medical Center (Cheyenne)	One-time transfer of the facility database	PII,PHI This system collects all patient data (name, SSN, billing and prescription information, address, phone number, email address, next of kin, any clinical notes, and appointments)	Secure FTP
VA Central Western Massachusetts Healthcare System (Northampton)	One-time transfer of the facility database	PII,PHI This system collects all patient data (name, SSN, billing and prescription information, address, phone number, email address, next of kin, any clinical notes, and appointments)	Secure FTP
Mann-Grandstaff VA Medical Center (Spokane)	One-time transfer of the facility database	PII,PHI This system collects all patient data (name, SSN, billing and prescription information, address, phone number, email address, next of kin, any clinical notes, and appointments)	Secure FTP
VA Northeast Ohio Healthcare System (Cleveland)	One-time transfer of the facility database	PII,PHI This system collects all patient data (name, SSN, billing and	Secure FTP

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 data element types such as PII/PHI that are shared/received with the Program Office or IT system*	*Describe the method of transmittal*
		prescription information, address, phone number, email address, next of kin, any clinical notes, and appointments)	
VA Puget Sound Health Care System (PugetSound)	One-time transfer of the facility database	PII,PHI This system collects all patient data (name, SSN, billing and prescription information, address, phone number, email address, next of kin, any clinical notes, and appointments)	Secure FTP

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks.
This question is related to privacy control UL-1, Internal Use.

Follow the format below:

Privacy Risk: The sharing of de-identified data is necessary for the testing of veteran's patient data. However, there is a risk that the data could be shared with an inappropriate VA organization or institution which would have a potentially catastrophic impact on privacy.

Mitigation: The potential harm is mitigated by 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, planning and maintenance, accountability, audit and risk management, data quality and integrity, data minimization and retention, individual participation and redress, transparency and use limitation.

Electronic Permission Access System (ePAS) mitigates the risk of inadvertently sharing or disclosing information by assigning access permissions based on need to know.

The use of a Personal Identity Verification (PIV) card is implemented. This ensures the identity of the user by requiring two-factor authentication.

VistA menus and security keys are assigned by an approved ePAS request based on specific job or duty requirements with least privileges. This access is reviewed for appropriateness on a quarterly basis.

VistA applies the sensitive record flag to all employees and any veteran record where the veteran requests the record be sensitized. The ISSO reviews VistA audit messages for any potential access abnormalities or violations.

The **Bay Pines Enterprise Testing Services Test Center (ETSTC)** completes a multitude of auditing functions based on VA Handbook 6500 guidelines. The **Bay Pines Enterprise Testing Services Test Center (ETSTC)** completes an in-depth audit of VistA accounts to include separated users, elevated privileges, file access, separation of duties, sensitive records, inactive accounts as well as ad-hoc reports upon request.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible

with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?

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

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 data element types such as PII/PHI that are shared/received 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***
NA				

If specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16, note them here.

• The information with each application is categorized in accordance with FIPS 199 and NIST SP 800-60. As part of the categorization any PII is identified.

• The VA has policies which direct and guide the activities and processes performed by the VA. The policies are periodically reviewed to ensure completeness and applicability.
• The NIST SP 800-53 controls are selected based on the categorization. The controls provide protection for Veteran PII while developed or stored by an application or IT system, physically transported, between facilities, least privilege, stored offsite, or transmitted between IT centers.

• Internal protection is managed by access controls such as user authentication (user IDs, passwords and Personal Identification Verification (PIV)), awareness and training, auditing, and internal network controls. Remote protection is provided by remote access control, authenticator management, audit, and encrypted transmission.

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: N/A.

Mitigation: N/A.

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.

Yes, at the facility where the source information is stored. Individual choice not to provide the information should be done at those Healthcare systems hosting the data, before transmission to the **Bay Pines Enterprise Testing Services Test Center (ETSTC)**.

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, at the facility where the source information is stored. Individual choice not to provide the information should be done at those Healthcare systems hosting the data, before transmission to the **Bay Pines Enterprise Testing Services Test Center (ETSTC)**.

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

No – The **Bay Pines Enterprise Testing Services Test Center (ETSTC)** only receives VistA database instances necessary for testing. Individual choice not to provide the information should be done at the healthcare facility hosting the data before transfer to the Bay Pines Enterprise Test Center.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks.

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

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

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

Follow the format below:
Privacy Risk: There is a risk that an individual may not receive notice that their information is being collected, maintained, processed, or being disseminated by the healthcare systems for the purpose of testing at the **Bay Pines Enterprise Testing Services Test Center (ETSTC)** prior to providing the information to the VHA.

Mitigation: This risk is mitigated by the common practice of providing a Notice of Privacy Practices (NOPP) when Veterans apply for benefits. Additionally, new NOPPs are provided to beneficiaries and periodic monitoring is performed to check that the signed acknowledgment form has been scanned into electronic records. Employees and contractors are required to review,

sign and abide by the National Rules of Behavior on a yearly basis as required by VA Handbook 6500 as well as complete annual mandatory Information Security and Privacy Awareness training.
Additional mitigation is provided by making the System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) available for review online, as discussed in question 6.1.

Section 7. Access, Redress, and Correction

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

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

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

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

If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information.
This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

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 Department of Veterans Affairs Release of Information (ROI) Office. Any individual who would like information under the Freedom of Information Act (FOIA) [5 U.S.C. 552] should contact the facility's FOIA Officer in writing.

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

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 provided the opportunity to submit a request for change in medical record via the amendment process. An amendment is the authorized alteration of health information by modification, correction, addition, or deletion. An individual can request an alteration to their health information by making a formal written request mailed or delivered to the Privacy Officer at the VA health care facility that maintains the record. 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. A decision to approve or deny is made by the practitioner who entered the data and relayed to the Veteran in writing by the system Privacy Officer. Appeal rights are provided if a request is denied. The goal is to complete any evaluation and determination within 30 days.

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 system of records, and the Bay Pines Enterprise Test Center's assigned System Privacy Officer (PO), or designee, to be date stamped; and is 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. That is, VA must maintain in its records only such information about an individual that is accurate, complete, timely, relevant, and necessary.

Individuals have the right to review and change their contact or demographic information at time of appointment or upon arrival to the VA facility and/or submit a change of address request form to the Enterprise Program Management Office for processing.

Employees should contact their immediate supervisor and Human Resources to correct inaccurate or erroneous information. Contractors should contact Contract Officer Representative to correct inaccurate or erroneous information upon request.

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 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

Information can also be obtained by contacting the Department of Veterans Affairs Release of Information (ROI) office.

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.

Veterans and other individuals are encouraged to use the formal redress procedures discussed above in Section 7.3 to request edits to their personal medical records and other personal records retained about them.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

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

Follow the format below:
Privacy Risk: There is a risk that a Veteran may not know how to obtain access to their records or how to request corrections to their records.

Mitigation: As discussed in question 7.3, the Notice of Privacy Practice (NOPP), which every patient signs prior to receiving treatment, discusses the process for requesting an amendment to ones records. Beneficiaries are reminded of this information when obtaining a copy of the NOPP. The VA ROI office is available to assist Veterans with obtaining access to their medical 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 to obtain access to all the available features.

In addition, Privacy Handbook 1605.1 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?

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 to the **Bay Pines Enterprise Testing Services Test Center (ETSTC)** working and storage areas are restricted to VA employees who must complete both the 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 to include but not limited to Information System Security Officer (ISSO), The Bay Pines Enterprise Test Center Chief Information Officer (CIO), System Administrators, Network Administrators, Database Managers, Systems Engineers or Applications Developers and Testers.

Access is requested per Region 3 policies utilizing Electronic Permission Access System (ePAS). Users submit access requests based on need to know and job duties. Supervisor, ISO and OI&T approval must be obtained prior to access granted. These requests are submitted for VA employees, contractors and all outside agency requests and are processed through the appropriate approval processes.

Access to VistA requires multi-layer authentication. The individual first must authenticate through Windows Active Directory. Additionally, they are assigned unique Access and Verify Codes. VistA access is time limited with session timeout after a designated period of inactivity and/or automatic account lock out unsuccessful attempts. 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 normal duty hours and the facilities are protected from outside access by the Federal Protective Service or other security personnel.

Access the Bay Pines Enterprise Test Center Server room 300 and its associated annex in room 343 is generally limited by appropriate locking devices and restricted to authorized **Bay Pines Enterprise Testing Services Test Center (ETSTC)** employees and vendor personnel. Automated Data Processing (ADP) peripheral devices are placed in secure areas (areas that are locked or have limited access) or are otherwise protected. Information in VistA may be accessed by authorized VA employees. Access to file information is controlled at two levels. The systems recognize authorized employees by series of individually unique passwords/codes as a part of each data message, and the employees are limited to only that information in the file which is needed in the performance of their official duties. Information that is downloaded from VistA and maintained on laptops and other approved government equipment is afforded similar storage and access protections as the data that is maintained in the original files. Access to information stored on automated storage media at other VA locations is controlled by individually unique passwords/codes. Access by Office of Inspector General (OIG) staff conducting an audit, investigation, or inspection at the C. W. Bill Young VA Medical Center, Bay Pines Health Care System or an OIG office location remote from C. W. Bill Young VA Medical Center, Bay Pines Health Care System is controlled in the same manner.

Information downloaded from VistA and maintained by the OIG headquarters and Field Offices on automated storage media is secured in storage areas for facilities to which only OIG staff have access. Paper documents are similarly secured. Access to paper documents and information on

automated storage media is limited to OIG employees who have a need for the information in the performance of their official duties. Access to information stored on automated storage media is controlled by individually unique passwords/codes.

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

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

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

Each contract is reviewed prior to approval based on the contract guidelines by the appropriate contract authority (i.e., COR, Contracting Officer, Contract Review Committee). This review is conducted each time the contract period expires.
The Privacy Officer is responsible for monitoring all local contracts that require a Business Associate Agreement (BAA). The Privacy Officer will coordinate an annual review all local contracts to monitor the contractor's compliance with the BAA.

Per specific contract guidelines, contractors can have access to the system only after completing mandatory information security and privacy training, VHA HIPAA training as well as the appropriate background investigation to include fingerprinting. Certification that this training has been completed by all contractors must be provided to the VHA employee who is responsible for the contract in question. In addition, all contracts by which contractors might access sensitive patient information must include a Business Associate Agreement which clarifies the mandatory nature of the training and the potential penalties for violating patient privacy.

Contractors with VistA access must have an approved ePAS request on file and access reviewed with the same requirements as VHA employees.

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 employees requiring access to VA systems must complete the onboarding and annual mandatory privacy and information security training. In addition, all employees who interact with patient sensitive medical information must complete the VA mandated privacy HIPAA training. Due to the fact our personnel are geographically dispersed throughout the continental United States, new employees receive face-to-face training by their closest, assigned VA Hospital Privacy Officer and Information System Security Officer during new employee orientation. The Privacy and Information Security Officer also perform subject specific trainings on an as needed basis.

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

If Yes, provide:

1. *The date the Authority to Operate (ATO) was granted,*
2. *Whether it was a full ATO or ATO with Conditions,*
3. *The amount of time the ATO was granted for, and*
4. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH).*

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

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

Yes – We were granted an Expedited 180 Day ATO on October 15, 2020 with an ATO expiration date of April 13, 2021 with a FIPS 190 Moderate System Classification.

Section 9. 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**

Signature of Responsible Officials

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

RITA K GREWAL 114938

Digitally signed by RITA K GREWAL 114938
Date: 2021.02.09 14:01:39 -05'00'

Privacy Officer, Rita Grewal

Amine Messaoudi 1136390

Digitally signed by Amine Messaoudi 1136390
Date: 2021.02.09 15:14:02 -05'00'

Information Security Systems Officer, Amine Messaoudi

Anthony D. Jones 652976

Digitally signed by Anthony D. Jones 652976
Date: 2021.02.09 15:49:21 -05'00'

System Owner, Anthony Jones

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

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).