Privacy Impact Assessment for the VA IT System called:

# Special Purpose – Legacy Information Technology Environment (SP-LITE)

# VA Office of Information Security (OIS) Specialized Device Cybersecurity Department (SDCD)

# VACO (VA Central Office)

# eMASS ID # 2561

Date PIA submitted for review:

03/11/2025

System Contacts:

*System Contacts*

| | Name | E-mail | Phone Number |
|---|---|---|---|
| Privacy Officer | Gina Siefert | Gina.Siefert@va.gov | 224-558-1584 |
| Information System Security Officer (ISSO) | Oscar Fibleuil | Oscar.Fibleuil@va.gov | 703-595-9295 |
| Information System Owner | Ryan McGettigan | Ryan.McGettigan@va.gov | 484-653-9539 |

| | Name | E-mail | Phone Number |
|---|---|---|---|
| Data/Business/Information Owner | Veterans Health Administration (VHA)/Veterans Benefit Administration (VBA)/National Cemetery Association (NCA) | TBD | TBD |

## Abstract

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

Special Purpose Legacy Information Technology Environment consists of specialized devices, and applicable components, hosted within the facilities associated to the Area Boundaries. VHA (Veterans Health Administration), VBA (Veterans Benefit Administration), and NCA (National Cemetery Administration as appropriate are the data and business owners of SP-LITE.
These devices support 4 Operation Categories: Healthcare Services Support (HSS) are devices/systems that are dedicated to, or essential in real time to VA healthcare and/or clinical services mission. Security Services Support (SSS) are devices/systems that are dedicated to, or essential in, real time to VA physical, personnel, and operational security services mission. Business Services Support (BSS) are devices/systems that directly support VA business owners, staff, Veterans, and visitors to a VA facility. Fixed Facility Support Services (FFSS) are Building Automation Systems (BAS) with centralized control of a facility or building HVAC lighting, access control, security systems and other interrelated systems through a Building Management System (BMS). SP-LITE relies on the Veterans Affairs Enterprise Network (VAEN) Platform to provide the networking backbone for connectivity as well as all support systems that require network transport to function. SP-LITE is managed by SDCD on behalf of the data owners.

## Overview

*The overview is the most important section of the Privacy Impact Assessment (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 business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?*

The Enterprise Special Purpose Legacy Information Technology Environment (SP-LITE) establishes a baseline of the VA special purpose devices/systems that assist, support and maintain mission capabilities and operations for building safety, healthcare services, security services, and other general services functional support areas.

*B. Who is the owner or has control of the IT system or project? If the system has an eMASS entry, ensure this information matches with the eMASS entry.*

The VA program office system owner is the Office of Information Security (OIS) Specialized Device Cybersecurity Division.

*2. Information Collection and Sharing*

*C. Indicate the expected number of individuals whose information is stored in the system and include a brief description of the typical client or affected individual?*

520054 (Estimate includes Veterans or Dependents, VA Contractors, and VA Personnel).

For Clinical Trainees, Members of the Public/Individuals, and Volunteers it is difficult to determine a specific number as it is variable and would be dependent on specific use cases.

| Check if Applicable | Demographic of individuals |
|---|---|
| ☒ | Veterans or Dependents |
| ☒ | VA Employees |
| ☒ | Clinical Trainees |
| ☒ | VA Contractors |
| ☒ | Members of the Public/Individuals |
| ☒ | Volunteers |

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

SP-LITE may collect information to include Name, Date of Birth, Medical record Number, Facial Recognition data and other entries listed in Section 1.1 of this PIA.

The information collected in the system is dependent on the Operation Category it falls under. Healthcare Services Support (HSS) devices could collect; Name, Date of Birth, Medical Record Number, Medical Records, Full SSN, Partial SSN, Financial Information, Personal Mailing Address, Personal Phone Number, Race/Ethnicity, Sex, Medications, Biometrics, Procedure Code, Driver's License Number, Patient ID Number.

Security Services Support (SSS) could collect; Name, Date of Birth, Address, Full SSN, Biometrics.

Business Services Support (BSS) could collect; Full SSN, Name, Date of Birth, Personal Mailing Address, Driver's License Number, Patient ID Number, Personal Phone Number, Biometrics

SP-LITE provides the networking backbone for connectivity as well as all support systems that require network transport to function.

*E. What information sharing is conducted by the IT system? A general description of the modules and components, where relevant, and their functions.*

Information will be shared externally with, CareCentra, Inc, Cook County Sheriff's Office, VA Office of Inspector General, Vocera Communications Inc, and Symptelligence Medical Informatics LLC as listed in Section 5.1 of this PIA.

F. Are the modules/subsystems only applicable if information is shared?
*Yes*

*G. Is the system operated in more than one site to include primary and secondary 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?*

All special purpose devices are held to Special Purpose System Protection Program (SPSPP) policies and procedures to ensure the Confidentiality, Integrity, and Availability (CIA Triad) of special purpose system data is preserved. The SPSPP is an internal VA program owned by SDCD in establishing a resource community regarding special purpose device security and procedures needed to help safely and securely maintain special purpose assets throughout the asset lifecycle. SP-LITE operates in 136 Area sites in accordance with approved configuration, administration and maintenance defined in each documented Enterprise Risk Analysis (ERA), which is a residual risk determination for all network-connected special purpose devices prior to implementation on the VA network. Legacy devices (those without an existing ERA) are being evaluated as their lifecycles permit. Legacy devices still adhere to the same policies, procedures, and security controls as those devices with an ERA. Facility Personnel in conjunction with HTM personnel provide onsite support to perform the day-to-day activities, maintenance, and management of the SP-LITE special purpose devices in accordance with the Special Purpose System Protection Program.

*3. Legal Authority and System of Record Notices (SORN)*

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

The legal authority to operate the system is Title 38, United States Code, Sections 501(b) and 304. As well as Title 38, United States Code, Section 7301(a).

System of Record Notices (SORN) 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 record: Title 38, United States Code, Sections 501(b) and 304.

103VA07B Police and Security Records-VA 2024-07137.pdf (govinfo.gov)

146VA005Q3/73 FR 16093 Department of Veterans Affairs Identity Management System (VAIDMS)-VA https://www.govinfo.gov/content/pkg/FR-2008-03-26/pdf/E8-6120.pdf

SORN 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.*

The SORNs do not require any amendment to accommodate SP-LITE.

*4. System Changes*

*J. Will the business processes change due to the information collection and sharing?*

☐ *Yes*
☒ *No*
*if yes, <<ADD ANSWER HERE>>*

*K. Will the technology changes impact information collection and sharing?*

☐ *Yes*
☒ *No*
*if yes, <<ADD ANSWER HERE>>*

## 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 Information 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
- ☒ **Full** Social Security Number
- ☒ **Partial** 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
- ☒ Sex
- ☐ Integrated Control Number (ICN)
- ☐ Military History/Service Connection
- ☐ Next of Kin
- ☐ Date of Death
- ☐ Business Email Address
- ☐ Electronic Data Interchange Personal Identifier (EDIPI) ☐ Other Data Elements (list below)

Other PII/PHI data elements: Biometrics, PIV ID, Username, Password, Driver's License Number, Patient ID Number, Procedure Code.

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

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

*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?*

SP-LITE collects the information directly from the individuals or entities providing the data identified in Section 1.1 to include Engineering, Facilities, Police Service, and Biomedical staff.

*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.*

Data is collected from staff within the Engineering, Facilities, Police Service and Biomedical departments that manage the Special Purpose System.

.

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

Yes, certain Special Purpose Assets such as Vocera can create data analysis, trends, dashboards, and reports of all traffic that goes through the Vocera system to improve patient care.

**1.3 Methods of information collection**

*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 electronically collected from individuals where possible and/or manually collected in conversations with the individual.

*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?*

SP-LITE does not collect information on forms and is not subject to the Paperwork Reduction Act.

**1.4 Information checks for accuracy, and 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.*

SP-LITE, for special purpose devices that support medical staff, allow the staff to manage/monitor the information included in the patient's profile. The Veterans' identifying information is checked for accuracy by the Clinicians and is cross-referenced with information on Veterans each time the clinicians see their patients. Information obtained directly from the individual will be assumed to be accurate.

*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?*

There is no known commercial aggregator used for SP-LITE

**1.5 Identify the specific legal authorities, arrangements, and agreements that 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*

SP-LITE operates under the following system authority:

- SORN 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 record: Title 38, United States Code, Sections 501(b) and 304.
- SORN 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. Title 38, United States Code, Section 7301(a).
- Title 38, United States Code (U.S.C.), Chapter 3, Department of Veterans Affairs.
- Title 38, U.S.C., Chapter 5, Authority and Duties of the Secretary.
- Title 38, U.S.C., Chapter 73, Veterans Health Administration (VHA) – Organization and Functions.
- Privacy Act of 1974 Freedom of Information Act (FOIA) 5 U.S.C. 552.
- Health Insurance Portability and Accountability Act of 1996 (HIPAA).

**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: The collection ties with the purpose of the underlying mission of the organization and its enabling authority.*

*Principle of Minimization: The information is directly relevant and necessary to accomplish the specific purposes of the program.*

*Principle of Individual Participation: The program, to the extent possible and practical, collects information directly from the individual.*

*Principle of Data Quality and Integrity: VA policies and procedures must ensure that personally identifiable information is accurate, complete, and current.*
*This 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:** Special Purpose devices and systems collect the minimal amount necessary of both Personally Identifiable Information (PII) and Protected Health Information (PHI). There is risk that information contained within the systems could be inaccurate.

**Mitigation:** The VA is careful to only collect the information necessary to assist in the care of patients and provide an updated status to clinical health care providers. By only collecting the minimum necessary information, the VA can better protect the Veterans' information. Once information is collected, process, or retained, there are security safeguards in place, i.e., transmitted using encryption and stored in secure, encrypted servers behind VA firewalls.
The information is directly relevant and necessary to accomplish the purposes of patient care and treatment. The special purpose devices, to the extent possible and practical, collect information directly from the individual. PII taken directly from manual entry by manual entry into the special purpose device is verified by local facility staff.

## Section 2. Uses of the Information

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

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

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

| PII/PHI Data Element | Internal Use | External Use |
|---|---|---|
| Name | Identification Purposes | Identification Purposes |

| | | |
|---|---|---|
| Full Social Security Number | Identification Purposes | Identification Purposes |
| Partial Social Security Number | Identification Purposes | Identification Purposes |
| Date of Birth | Identification Purposes | Identification Purposes |
| Personal Mailing Address | Communication/Equipment Delivery Purposes | Communication/Equipment Delivery Purposes |
| Personal Phone Number(s) | Communication Purposes | Communication Purposes |
| Financial Information | Treatment Purposes | Treatment Purposes |
| Medications | Treatment Purposes | Treatment Purposes |
| Medical Records | Treatment Purposes | Treatment Purposes |
| Race/Ethnicity | Identification Purposes | Identification Purposes |
| Medical Record Number | File Identification Purposes | File Identification Purposes |
| Sex | Identification Purposes | Identification Purposes |
| Biometrics | Identification Purposes | Identification Purposes |
| Procedure Code | Treatment Purposes | Treatment Purposes |
| Driver's License Number | Identification Purposes | Identification Purposes |
| Patient ID Number | Identification Purposes | Identification Purposes |
| Username | Identification Purposes (Access Control for special purpose devices) | Identification Purposes (Access Control for special purpose devices) |
| Password | Identification Purposes (Access Control for logging into special purpose devices) | Identification Purposes (Access Control for logging into special purpose devices) |
| PIV ID | Identification Purposes (Access Control for logging into special purpose devices) | Identification Purposes (Access Control for logging into special purpose devices) |

The SP-LITE system boundary is comprised of facility level instances associated with the Area boundaries. VHA (Veterans Health Administration), VBA (Veterans Benefit Administration), and NCA (National Cemetery Administration as appropriate are the data and business owners. Due to the extensive amount and nature of the information contained at each facility which can determine what information to collect, process, retain, or disseminate, a full understanding of the purpose for each individual data point can be obtained by reviewing the facility-level Privacy Impact Assessment. https://www.oprm.va.gov/privacy/pia.aspx

The records and information may be used for statistical analysis to produce various management, workload tracking and follow-up reports; to track and evaluate the ordering and delivery of equipment, services, and patient care; the planning, distribution, and utilization of resources; the possession and use of equipment or supplies; the performance of vendors, equipment, and employees; and to provide clinical and administrative support to patient medical care.

The data may be used for such purposes as facility maintenance (HVAC), access control, facility monitoring (Camera Systems) and maintenance of all related equipment. Additionally data may be used for reviews, investigations and audits conducted by staff of the health care facility, the Network Directors Office, VA Central Office, and the VA Office of Inspector General (OIG);

Data element types collected include Personal Information, Healthcare Information, VA Staff Information, and System Information. List of these data elements are below:

**Personal Information Identifiers**

Name, Full Social Security Number, Partial Social Security Number, Date of Birth, Personal Mailing Address, Personal Phone Number(s), Financial Information, Medications, Medical Records, Race/Ethnicity, Medical Record Number, Sex, Biometrics, Driver's License Number

**Healthcare Information**

Medication, Medical Records, Procedure Code, Patient ID Number

**VA Staff Information**

Username, Password

**2.2 Describe the types of tools 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?*

SP-LITE devices are network connected special purpose device/systems which are essential to supporting and maintaining the individual VA facilities located within the United States as they support facility maintenance, security of the facility, and healthcare support functions. SP-LITE devices have the ability to analyze data and provide recommendations, however the VA facility staff can accept or reject any data analysis provided by SP-LITE special purpose devices based on their judgment.

*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.*

SP-LITE devices do not create or make available new or previously unutilized information.

**2.3 How the information in the system is 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?*

SP-LITE is comprised of special purpose systems that utilize approved encryption technologies for data in transit in bi-directional traffic flows between special purpose desktop/laptops, servers, special purpose system components, and related telecommunication devices both locally (LAN) and remotely (VA WAN), when possible. Communication requirements (i.e., ports, protocols, services) are learned during the ERA process. Special Purpose Devices/Systems are deployed within VLANs, and ACLs configured to explicitly allow the required Ports, protocols, and Services (PPS) for device/system communication. ERA process ensures data at rest encryption technologies are documented for each approved special purpose system, where applicable. However, some special purpose devices within SP-LITE do not have the technology in place for encryption of data. Therefore, a Plan of Actions and Milestones (POAM) will document the planned recommendations.

*2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs? (refer to PTA question 3.8).*

SP-LITE requires each Area to document deviations from approved processes and uses of special purpose systems. Please refer to the facility-level Privacy Impact Assessment for the handling of SSNs during the collecting, processing, or retaining of SSNs locally. https://www.oprm.va.gov/privacy/pia.aspx

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

SP-LITE requires each Area to comply with all OMB Memorandum M-06.15 mandates in accordance with the Privacy controls deemed applicable to special purpose systems by SP-LITE Information System Owner and approved by VA Senior Authorizing Official. Please refer to the facility-level Privacy Impact Assessment for the PII/PHI safeguards in place at the local facility. https://www.oprm.va.gov/privacy/pia.aspx.

**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?*

SP-LITE requires each Area to document how access to PII is determined. Access to special purpose devices is on a need-to-know basis, and limited to facility staff supporting a particular device (Engineering, Police Service, Biomedical Staff) and others with a legitimate need-to-know. SP-LITE is restricted to personnel with VA Privacy and Information Security Awareness and Rules of Behavior (VA 10176), and Privacy and HIPAA training (VA 10203), certified annually via the Training Management System (TMS). The access control procedures are with the supervisor or designee requesting access, thus providing the approval for the supporting staff to the special purpose devices, where the device data is transmitted and stored. The local Information System Security Officer (ISSO), and supervisor or designee review the access semi-annually. Where technically feasible for the special purpose devices, audit logs are maintained on the access to the special purpose devices. Audit logs are reviewed periodically by the system administrators and business owners. The assurance of the safeguards for PII are the responsibility of the system administrators, business owners, and users of the special purpose devices. Please refer to the facility-level Privacy Impact Assessment for local guidance on PII access. https://www.oprm.va.gov/privacy/pia.aspx.

*2.4b Are criteria, procedures, controls, and responsibilities regarding access documented? How are the documented, i.e. Policy, SOP, other. And where is this documentation located?*

SP-LITE requires each Area to document all criteria, procedures, controls, and responsibilities relevant to access to PII. Please refer to the facility-level Privacy Impact Assessment for local guidance on PII criteria, procedures, controls, and responsibilities. https://www.oprm.va.gov/privacy/pia.aspx.

*2.4c Does access require manager approval?*

SP-LITE requires each Area to document where access requires manager approval. Please refer to the facility-level Privacy Impact Assessment for local guidance on whether access requires manager approval. https://www.oprm.va.gov/privacy/pia.aspx.

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

SP-LITE requires each Area to document how access to PII is monitored, tracked, and recorded. Please refer to the facility-level Privacy Impact Assessment for local guidance for

information regarding whether the access to PII is being monitored, tracked, and recorded. https://www.oprm.va.gov/privacy/pia.aspx.

*2.4e Who is responsible for assuring safeguards for the PII as identified in eMASS?*

SP-LITE requires that all VA Staff, or those otherwise with access to any PII or PHI stored, collected, or accessed by SP-LITE systems, are trained and aware that all VA personnel are responsible for assuring PII is safeguarded. Please refer to the facility-level Privacy Impact Assessment for local guidance for information regarding the responsibility assuring safeguards for PII. https://www.oprm.va.gov/privacy/pia.aspx.

## 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*

**Personal Information Identifiers**

Name, Full Social Security Number, Partial Social Security Number, Date of Birth, Personal Mailing Address, Personal Phone Number(s), Financial Information, Medications, Medical Records, Race/Ethnicity, Medical Record Number, Sex, Biometrics, Driver's License Number

**Healthcare Information**

Medication, Medical Records, Procedure Code, Patient ID Number

**VA Staff Information**

Username, Password

### 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 https://www.archives.gov/records-mgmt/grs? This question is related to privacy control DM-2, Data Retention and Disposal.*

All information is temporarily retained for reporting purposes, depending on the special purpose device/system.

National Cemetery Administration: NCA Records Schedule, ADMINISTRATIVE/GENERAL OFFICER RECORDS (ADM), ADM-7 – Office Support, temporary records can be destroyed when 5 years old.

Veterans Benefit Administration (VBA): VBA Records Control Schedule VB-1, Part II Central Office, 2-15- OFFICE SYSTEMS AND METHODS, 2-15.1 - temporary records regarding documentation of development, analysis, installation, and evaluation of office systems can be destroyed 1 year after system termination.

Veterans Health Agency (VHA) as stated in the Records Control Schedule, RCS 10-1, Chapter Six – Healthcare Records, 6000.2 Electronic Health Record (EHR), https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf

**3.3 The retention schedule 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. Please work with the system 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?*

SP-LITE Special purpose systems with system of records, the records are stored within the approved disposition authority. All information is temporarily retained for reporting purposes. When managing and maintaining VA data and records, healthcare facilities follow the guidelines established in the National Archives and Records Administration (NARA) approved Records Control Schedule, RCS 10-1, Chapter Six – Healthcare Records, 6000.2 Electronic Health Record, temporary records can be destroyed after verification of accurate entry of information into EHRS Link - https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf.

National Cemetery Administration: NCA Records Schedule, ADMINISTRATIVE/GENERAL OFFICER RECORDS (ADM), ADM-7 – Office Support, temporary records can be destroyed when 5 years old.

Veterans Benefit Administration (VBA): VBA Records Control Schedule VB-1, Part II Central Office, 2-15- OFFICE SYSTEMS AND METHODS, 2-15.1 - temporary records regarding documentation of development, analysis, installation and evaluation of office systems can be destroyed 1 year after system termination.

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

Patient medical information is retained by SP-LITE under VA Records Control Schedule, item 6000.2a(2) with disposition authority N1-15-02-3 item 2.

National Cemetery Administration Records are retained by SP-LITE under NCA Records Schedule, ADMINISTRATIVE/GENERAL OFFICER RECORDS (ADM), ADM-7 – Office Support with disposition authority NC1-15-85-9 item 11

Veterans Benefit Administration (VBA) records are retained by SP-LITE under VB-, Part II Central Office, 2-15 – OFFICE SYSTEMS AND METHODS, 2-15.1, with disposition authority GRS 23,Item 3b(1)

**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 reports produced by Special purpose devices/systems are electronic, if hard copies exist, , the hard copy would then be shredded per the VA sanitization requirements within VA Directive 6500. The media sanitization requirements as outlined in VA Directive 6500 are followed, and this would mean that the hard drives would be destroyed to meet the VA Directive 6500 requirements. If the hard drives could not be destroyed, then local facility guidance complying with NIST SP 800-88 would be followed.

As stated in the Records Control Schedule for VHA, RCS 10-1, Chapter Six – Healthcare Records, 6000.2 Electronic Health Record, temporary records can be destroyed after verification of accurate entry of information into EHR link - https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf.

National Cemetery Administration: NCA Records Schedule, ADMINISTRATIVE/GENERAL OFFICER RECORDS (ADM), ADM-7 – Office Support, temporary records can be destroyed when 5 years old.

Veterans Benefit Administration (VBA): VBA Records Control Schedule VB-1, Part II Central Office, 2-15- OFFICE SYSTEMS AND METHODS, 2-15.1 - temporary records regarding documentation of development, analysis, installation, and evaluation of office systems can be destroyed 1 year after system termination.

**3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?**

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

SD-LITE does not use PII for research, testing or training. Test data for the special purpose devices/systems would be used, if at all, and not actual sensitive data (PII).

**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 Privacy Officer (PO) 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: The project retains only the information necessary for its purpose, additionally, the PII is retained only for as long as necessary and relevant to fulfill the specified purposes.*

*Principle of Data Quality and Integrity: The PIA should describe 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 information maintained by or within an Area implementation of special purpose systems 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:** Record storage in both the retention and the number of records is reviewed and assessed during the risk analysis of special purpose devices. SPSPP (Special Purpose System Protection Program) develops guidance and promotes the adoption throughout VA of multiple layers of administrative, technical, and physical safeguards that work together to reduce the

attack surface and minimize negative outcomes of special purpose device compromise without inhibiting performance or the patient's healthcare experience. Some safeguards or compensating controls that are in place are encryption of hard drives, physical security measures to secure special purpose devices, device sanitization, and awareness and training. None of the information is retained permanently in the special purpose devices/systems.

## Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA.

**PII Mapping of Components**

4.1a SP-LITE consists of 17 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 the Special Purpose Legacy Information Technology Environment (SP-LITE ) 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 3.9a 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 |
|---|---|---|---|---|---|
| Vocera Engage (Healthcare Support Services) | **Yes** | **Yes** | Name, Date of Birth, Medical Records, Medical Record Number, Medications, Full SSN, Personal Mailing Address, Personal Phone Number, Sex, Race/Ethnicity | **Healthcare Support** | **PHI/PII Encrypted/Anonymized where possible, data access on a need-to-know basis** |
| Laerdal – A/V Equipment (Healthcare Support Services) | Yes | **Yes** | Name | **Healthcare Support** | **PHI/PII Encrypted/Anonymized where possible, data access on a need-to-know basis** |
| Physical Security Cameras (Security Services Support) | **Yes** | **Yes** | Biometrics | **Facility Support** | **PHI/PII Encrypted/Anonymized where possible, data access on a need-to-know basis** |
| Patient Facing Cameras (Security Services Support) | **Yes** | **Yes** | Biometrics | **Physical Security Support** | **PHI/PII Encrypted/Anonymized where possible, data access on a need-to-know basis** |
| Velocity Card Access Panel (Security Services Support) | **Yes** | **Yes** | Name, Date of Birth, Personal Mailing Address, Full SSN, Biometrics. | **Physical Security Support** | **PHI/PII Encrypted/Anonymized where possible, data access on a need-to-know basis** |
| Advantech,and Johnson controls-Police workstation (Security Support Services) | **Yes** | **Yes** | Name | **Physical Security Support** | **PHI/PII Encrypted/Anonymized where possible, data access on a need-to-know basis** |
| Stanley Security / Securitas Technology - Wanderguard | **Yes** | **Yes** | Name, PIV ID | **Physical Security Support** | **PHI/PII Encrypted/Anonymized where possible, data** |

| | | | | | |
|---|---|---|---|---|---|
| (Security Services Support) | | | | | **access on a need-to-know basis** |
| Carolina Recording-Police Phone recorder (Security Support Services) | **Yes** | **Yes** | Name | **Physical Security Support** | **PHI/PII Encrypted/Anonymized where possible, data access on a need-to-know basis** |
| Physical Access Control System - PACS (Security Support Services) | **Yes** | **Yes** | Name, Username, Password | **Physical Security Support** | **PHI/PII Encrypted/Anonymized where possible, data access on a need-to-know basis** |
| SPS Printers – Patient Bracelet (Business Support Services) | **Yes** | **Yes** | Full SSN, Name, Date of Birth, Personal Mailing Address, Driver's License Number, Patient ID Number, Personal Phone Number, Biometrics | **Business Support** | **PHI/PII Encrypted/Anonymized where possible, data access on a need-to-know basis** |
| QMATIC – Customer Flow Management System (Business Support Services) | **Yes** | **Yes** | Name | **Business Support** | **PHI/PII Encrypted/Anonymized where possible, data access on a need-to-know basis** |

**4.1b List internal organizations information is shared/received/transmitted, the information shared/received/transmitted, and the purpose, and how the information is transmitted.**

**NOTE: Question 3.9b (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*

| ***IT system and/or Program office. Information is shared/received with*** | ***List the purpose of the information being shared /received with the specified program office or IT system*** | ***List PII/PHI data elements shared/received/transmitted.*** | ***Describe the method of transmittal*** |
|---|---|---|---|
| **Vocera Engage**: Veterans Health Information Systems and Technology Architecture (VistA) | Improvement of VA patient care. | Name, Date of Birth, Medical Records, Medical Record Number, Full SSN, Partial SSN, Personal Mailing Address, Personal Phone Number, Sex, Ethnicity/Race | CPRS via HL7 Messaging |

## 4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

*Discuss the privacy risks associated with the sharing of information within the VA network 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 in this section.).*

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

Follow the format below:

**Privacy Risk:** Data sharing is necessary for maintaining special purpose devices and providing support to healthcare staff within the VHA, VBA and NCA facilities. There is risk data could be shared with inappropriate organizations or institutions which has the potential for a catastrophic impact on privacy.

**Mitigation:** Safeguards are implemented to ensure data is not inappropriately shared or accessed including employee security and privacy training and awareness and required reporting of suspicious activity. Additionally, use of role-based access control mechanisms, need-to-know determinations, secure passwords, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption of data-at-rest and in-transit, and monitoring of access authorization are all measures that are utilized within the facilities. Access to sensitive

information and the systems where the information is stored is controlled by the VA using a "least privilege/need to know" policy. Access must be requested and only the access required by VA persons or processes acting on behalf of VA persons is to be requested or granted.

## 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 List the external organizations (outside VA) that information shared/received. and information shared/received, and the purpose, and how the information transmitted and what measures are taken to ensure it is secure.**

**The sharing of information outside the agency must be compatible with the original collection. The sharing must be covered by an appropriate routine use in a SORN. If not covered, 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 IT System or External Program Office information is shared/received with*** | ***List the purpose of information being shared / received / transmitted*** | ***List the specific PII/PHI data elements that are processed (shared/received/transmitted)*** | ***List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing*** | ***List the method of transmission and the measures in place to secure data*** |
|---|---|---|---|---|

| | | | ***(can be more than one)*** | |
|---|---|---|---|---|
| Jesse Brown VA Medical Center, Area Chicago Police Services shares data with Cook County Sheriff's Office | Process suspects taken into custody by VA police with local law enforcement agencies | Biometrics, Name, Date of Birth, Sex | Local MOU/ISA E-5375 | S2S VPN |
| CareCentra, Inc (Transmission of veteran data from CareCentra application to help predict medical issues) | Helps in predicting medical issues for veteran care improvement | Name, Sex, Personal Phone number, Personal Email address, Date of Birth, Partial SSN, Medical Records | Local MOU/ISA E-5338 | SSL/TLS |
| Vocera Engage Application Servers share data with multiple VA healthcare centers. | Temporary storage of data for troubleshooting and integration development | Name, Date of Birth, Sex Medical Records | National MOU/ISA E-741 | S2S VPN |
| VA Office of Inspector General shares data with the VA OIG Appeals Review System | Processing/Tracking of OIG Appeals | Name, Date of Birth, Full SSN, Personal Mailing Address, Medical Records, Financial Information | National MOU/ISA E-5293 | SSL/TLS |
| VA NYHHS shares data with Symptelligence Medical Informatics LLC (Exchange of Lower Urinary Tract Information between SMIL and VA NYHHS) | Track VA patient LUTS (Lower Urinary Track Symptoms) for remote detection of potential medical issues. | Name, Date of Birth, Medical Records, Medical Record Number. | Local MOU/ISA E-212 | SSL/TLS |

## 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 risk of unintended exposure of PHI/PII data to organizations that do not have a need to know or legal authority to access VA data.

**Mitigation:** Safeguards are implemented to ensure data is not inappropriately shared or accessed include employee security and privacy training and awareness and required reporting of suspicious activity. Additionally, use of role-based access control mechanisms, need-to-know determinations, secure passwords, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption of data-at-rest and in-transit, and monitoring of access authorization are all measures that are utilized within the facilities. Access to sensitive information and the systems where the information is stored is controlled by the VA using a "least privilege/need to know" policy. Access must be requested and only the access required by VA persons or processes acting on behalf of VA persons is to be requested or granted. All external connections to special purpose systems are required to comply with VA's External Connection Compliance requirements, including adjudication of MOU/ISA and S2S VPN connections between Zone implementations to SP-LITE, Enterprise Platforms or connections and contracted Vendor support.

## 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 The notice provided to the individual before collection of the information. Please provide a copy and/or screen shot of a web notice of the notice as an Appendix-A 6.1 on the last page of the document. (A notice may include a posted privacy policy, a Privacy Act notice on forms, notice given to individuals by the sources system, or a system of records notice published in the Federal Register.) If notice was not provided, explain why.**

*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 Provide the Privacy Notice provided to the public by this system or any source systems. Include a copy of the notice in Appendix A of the PIA, the Federal Register citation, or Privacy Statement from collection of information such as forms or surveys.*

The VHA Notice of Privacy Practice (NOPP) is a document which explains the collection and use of protected health information to individuals interacting with VA. The NOPP is mailed every three years or when there is a major change to all enrolled Veterans. https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946.

Additionally, the Department of Veterans Affairs also provides notice by publishing the following VA SORN in the Federal Register and online. The patient medical records are covered under the SORN 24VA10A7/85 FR 62406 - Patient Medical Records-VA https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf. Other information in this system is covered under SORN 79VA10 - Veterans Health Information Systems and Technology Architecture (VistA) Records-VA https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf.

*6.1b If notice was not provided, explain why.*

This is not applicable as Notice is provided in the VHA Notice of Privacy Practices, in the applicable SORNS and PIA's that are available on a public facing site.

*6.1c Provide how the notice provided at the time of collection meets the purpose of use for this system.*

The VHA NOPP is a document which 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 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.

Please refer to the facility-level Privacy Impact Assessment for additional notice information. https://www.oprm.va.gov/privacy/pia.aspx

**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, individuals have the opportunity and right to decline to provide information.

**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.*

Yes, individuals must submit in writing to their facility Privacy Officer. The 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 can request further limitations on other disclosures. A veteran, legal guardian or court appointed Power of Attorney can submit a request to the facility Privacy Officer to obtain information.

**6.4 PRIVACY IMPACT ASSESSMENT: Notice**

*Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your Privacy Officer (PO) 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: This is referring to sufficient notice provided to the individual.*

*Principle of Use Limitation: The information used only for the purpose for which notice was provided either directly to the individual or through a public notice. The procedures in place must 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: B**efore providing information to the VA, an individual may not receive appropriate notice that their information is being collected, maintained, processed, or disseminated by VA. A risk that Veterans will not know that special purpose devices/systems exist or that if the special purpose devices collect, maintain and or disseminate PII/PHI.

**Mitigation:** This risk is mitigated by the common practice of providing the NOPP when Veterans are enrolled for health care. 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 SORN and PIA available for review online, as discussed in question 6.1 and the Overview section of this PIA.

## 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 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 VA Public Access Link-Home (efoia-host.com) to obtain information about FOIA points of contact and information about agency FOIA processes.***

An individual wanting notification or access, including contesting the record, should mail or deliver a request to the office identified in the SORN. If an individual does not know the "office concerned," the request may be addressed to the Post Office of any VA field station VHA facility where the person is receiving care or the Department of Veterans Affairs Central Office, 810 Vermont Avenue, NW, Washington, DC 20420. The receiving office must promptly forward the mail request received to the office of jurisdiction clearly identifying it as "Privacy Act Request" and notify the requester of the referral.

When requesting access to one's own records, patients are asked to complete VA Form 10-5345a: Individuals' Request for a Copy of their own health information, which can be obtained from the medical center where they receive treatment or online at https://www.va.gov/find-forms/about-form-10-5345a/.

Additionally, veterans and their dependents can gain access to their Electronic Health Record (EHR) by enrolling in the myHealtheVet (MHV) program, VA's online personal health record. More information about myHealtheVet is available at Home - My HealtheVet - My HealtheVet (va.gov).

Please also refer to SORN 79VA10 which states "Individuals seeking information regarding access to and contesting of records in this system may write, call or visit the VA facility location where they are or were employed or made contact."

*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 information in this system is not exempt from the Privacy Act.

*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 in the system does fall under the Privacy Act.

**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 SORN. Every Privacy Act SORN 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 NOPP also informs individuals on 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.*

The NOPP, which every patient receives when they enroll for care, discusses the process for requesting an amendment to their records. VHA staff distributes a Release of Information (ROI) procedure at facilities to assist Veterans with obtaining access to their health records and other records containing personal information. In addition, VHA Directive 1605.01 Privacy and ROI establishes procedures for Veterans to request their records to be amended. Individuals seeking information regarding access to and contesting of VA medical records may write, call, or visit the last VA facility where medical care was provided.

Also refer to the facility-level Privacy Impact Assessment for additional guidance. https://www.oprm.va.gov/privacy/pia.aspx

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

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

Formal redress is provided. Please see response to 7.3 which refers to NOPP, VHA Directive 1605.01 and the facility-level PIAs.

**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 Privacy Officer (PO) to complete all Privacy Risk questions in this section).*

*Consider the following FIPPs below to assist in providing a response:*
*Principle of Individual Participation: The individual must be provided with the ability to find out whether a project maintains a record relating to them.*

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

*Principle of Individual Participation: The mechanism by which an individual is able to prevent information about them obtained for one purpose from being used for other purposes without their 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:** The NOPP, which every patient receives when they enroll for care, discusses the process for requesting an amendment to their records. VHA staff distributes an ROI process at the VA facilities to assist Veterans with obtaining access to their health records and other records containing personal information. In addition, VHA Directive 1605.01 Privacy and ROI establishes procedures for Veterans to have their records amended when appropriate.
VHA established the MHV program to provide Veterans remote access to their health records. The Veteran must enroll in MHV to obtain access to all the available features.

## Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures. (Work with your ISSO to complete this section).

**8.1 The procedures in place to determine which users may access the system, must be documented.**

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

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

The special purpose devices/workstations have a login that the user must have credentials. This is limited to “need to know” for facility personnel and Biomedical staff. All staff with access to patient information in the performance of their duties need to know their responsibilities in maintaining the confidentiality of VA sensitive information, especially patient information, by completing the annual VA Privacy and Information Security Awareness and Rules of Behavior training, and Privacy and HIPAA training via TMS. Each facility is responsible for the creation and maintenance of system accesses. Please refer to the facility-level Privacy Impact Assessment for additional access procedures, such as account creation, modification, elevated privileges, etc. https://www.oprm.va.gov/privacy/pia.aspx.

*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 is no direct access to SP-LITE systems 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.*

Please refer to the facility-level Privacy Impact Assessment for role-based access procedures. https://www.oprm.va.gov/privacy/pia.aspx.

**8.2a. Will VA contractors have access to the system and the PII?**

Yes, select special purpose device vendors could have remote access to their specific devices, for which there is a national VPN agreement and/or business agreement with the vendor. Contractual, agreed upon privacy training and confidentiality is required from the vendor. A Business Associate Agreement (BAA) and/or an Interconnection System Agreement/Memorandum of Understanding (ISA/MOU) exists between the VA and the special purpose device vendor. If PII/PHI may be shared, transmitted, or received the data elements are captured in the MOU.

**8.2b. What involvement will contractors have with the design and maintenance of the system?**

Yes, contractors who are the vendor or manufacturer of the special purpose device are involved with the design, configuration, and maintenance of their special purpose device/system.

**8.2c. Does the contractor have a signed confidentiality agreement?**

If applicable, a confidentiality agreement, BAA or NDA is developed for contractors who work on the system. VA controls access to the system at the hosting infrastructure level and ensures Rules of Behavior are in place and signed before granting access to the VA network. Contractors may obtain VA network accounts if the contractors complete appropriate background investigations and have received security clearance in accordance with VA Standard Policies and Procedures needed to perform their tasks; and complete VA Privacy and Information Security Awareness and Rules of Behavior training, and Privacy and HIPAA training, and are re-certified annually via TMS.

**8.2d. Does the contractor have an implemented Business Associate Agreement for applicable PHI?**

If applicable, a confidentiality agreement, BAA or NDA is developed for contractors who work on the system. VA controls access to the system at the hosting infrastructure level and ensures Rules of Behavior are in place and signed before granting access to the VA network. Contractors may obtain VA network accounts if the contractors complete appropriate background investigations and have received security clearance in accordance with VA Standard Policies and Procedures needed to perform their tasks; and complete VA Privacy and Information Security Awareness and Rules of Behavior training, and Privacy and HIPAA training, and are re-certified annually via TMS.

**8.2e. Does the contractor have a signed non-Disclosure Agreement in place?**

*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.*

If applicable, a confidentiality agreement, BAA or NDA is developed for contractors who work on the system. VA controls access to the system at the hosting infrastructure level and ensures Rules of Behavior are in place and signed before granting access to the VA network. Contractors may obtain VA network accounts if the contractors complete appropriate background investigations and have received security clearance in accordance with VA Standard Policies and Procedures needed to perform their tasks; and complete VA Privacy and Information Security Awareness and Rules of Behavior training, and Privacy and HIPAA training, and are re-certified annually via TMS.

**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/contractors who have access to the VA network must complete the initial and annual VA Privacy and Information Security Awareness and Rules of Behavior training via the TMS site. In addition, all employees who have access to PHI must also complete the TMS Privacy and HIPAA training. Finally, new on-site employees receive face-to-face training by the facility Privacy Officer and Information Security Officer during new employee orientation. The Privacy and Information Security Officer also perform subject specific trainings on an as needed basis.

**8.4 The Authorization and Accreditation (A&A) completed for the system.**

*8.4a If Yes, provide:*

1. *The Security Plan Status:* <<ADD ANSWER HERE>>
2. *The System Security Plan Status Date:* <<ADD ANSWER HERE>>
3. *The Authorization Status:* <<ADD ANSWER HERE>>
4. *The Authorization Date:* <<ADD ANSWER HERE>>
5. *The Authorization Termination Date:* <<ADD ANSWER HERE>>
6. *The Risk Review Completion Date:* <<ADD ANSWER HERE>>
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* <<ADD ANSWER HERE>>

*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.***

SP-LITE Initial ATO submission in process, IOC Date: 03/31/2025

## 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.* ***(Refer to question 1.8 of the PTA)***

No cloud technology is utilized.

**9.2 Does the contract with the Hosting 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 3.3.1 of the PTA)*** *This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

Not applicable as no cloud technology is utilized.

**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.*

Not applicable as no cloud technology is utilized.

**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.*

Not applicable as no cloud technology is utilized.

**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).*

SP-LITE does not implement Robotic Process Automation

## Section 10. References

Summary of Privacy Controls by Family

*Summary of Privacy Controls by Family*

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

**Signature of Responsible Officials**

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

GINA SIEFERT Digitally signed by GINA SIEFERT
Date: 2025.03.31 07:06:33 -05'00'

**Privacy Officer, Gina Siefert**

OSCAR FIBLEUIL Digitally signed by OSCAR FIBLEUIL
Date: 2025.03.27 12:54:51 -05'00'

**Information System Security Officer, Oscar Fibleuil**

RYAN MCGETTIGAN Digitally signed by RYAN MCGETTIGAN
Date: 2025.03.27 10:04:05 -04'00'

**Information System Owner, Ryan McGettigan**

## 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).

**Notice of Privacy Practice (NOPP):**
VHA Directive 1605.04
IB 10-163p (va.gov)

## HELPFUL LINKS:

**Records Control Schedule 10-1 (va.gov)**

**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 Directive 1605.04
IB 10-163p (va.gov)