



Privacy Impact Assessment for the VA IT System called:

# Real Time Location System (RTLIS)

Date PIA submitted for review:

April 9, 2021

System Contacts:

## System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Andrea Wilson	Andrea.wilson3@va.gov	321-205-4305
Information System Security Officer (ISSO)	Thomas Orlor	Thomas.orer@va.gov	708-938-1247
Information System Owner	Kimberly Brayley	Kimberly.brayley@va.gov	716-289-8904

## Abstract

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

The Real Time Location System (RTLS) is a biomedical system owned by the Veterans Health Administration (VHA). It's a combination of multiple applications and technologies integrated together to provide a comprehensive solution for tracking VA assets. Use cases include: Asset Tracking (AT), Cardiac Catheterization Lab (CL), Sterile Processing (SP), and Temperature Monitoring (TM).

## 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 Real Time Location System (RTLS) is a biomedical system owned by the Veterans Health Administration (VHA). RTLS is comprised of commercial off the shelf (COTS) components that will be used by Veterans Affairs (VA) Medical Center employees to locate medical equipment throughout their facility. RTLS capabilities may include other functionalities such as the tracking of supplies, instruments, files, staff, patients and deceased remains. Multiple technologies will be needed for deployment (using existing wireless infrastructure, non-wireless infrastructure, or contractor specific infrastructure) and the ability to use multiple tags and technologies to meet specifications and specialized needs. RTLS, for each facility, must also be capable of exchanging data with VA information systems (e.g. VistA).. To ensure consistent use and maintenance of the system and data across the sites, RTLS follows change management and configuration controls policies and procedures and integrates with VA Single Sign On/Identity and Access Management (SSOi/IAM) environment. The capability will also allow system users to run reports and conduct analyses regarding assets, inventory levels and location details. RTLS utilizes Radiofrequency identification (RFID) technology. The purpose is to improve the efficiency of business processes in its hospitals and clinics. RTLS modules in this deployment include: Asset Tracking (Intelligent InSites, CenTrak) and Catheter Lab Supply Management (Wavemark), Sterile Processing (CensiTrac), and Temperature Monitoring (Centrak)

The goals for RTLS are to:

- Improve operational efficiency.
- Decrease operational costs.
- Maximize equipment utilization.
- Increase clinical efficiencies and staff productivity.
- Reduce delays and improve patient care.
- Minimize lost and misplaced items.
- Improve the quality and safety of service from patient, physician, and institution perspectives
- Provide medical centers with the real-time capability to actively track all assets, significant medical supplies, staff, patients, and environmental conditions (e.g., temperature and humidity) through a common interface and reporting tool.
- Provide VISN and national-level reporting and information sharing through an enterprise database.
- Improve patient and staff satisfaction

The legal authority citation for the operation of RTLS is the 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). SORN 24VA10P2 states: Title 38, United States Code, Sections 501(b) and 304 is the authority to maintain the system. SORN 79VA10P2 states: Title 38, United States Code, section 7301(a) is the authority to maintain the system.

VistA Interfaces: There are 4 interfaces associated with RTLS which act as the data conduit for the transport of encrypted data from RTLS. The interfaces do not read, write, or manipulate the data packages in any way. These interfaces are named GIP, PATIENT File, Employee and CART-CL.

There are approximately 10,000 cardiac procedures performed per year with all clinical staff accessing information that is used by RTLS such as, name, DOB and Internal Entry Number (IEN). A typical use case would be a patient in the Cardiac Catheterization Lab who gets his wristband scanned to allow the nurse or technician to process the encounter and record it in the RTLS database.

The completion of this PIA will not cause changes to business processes or changes in technology.

## 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://vawww.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:

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

Additional information related to WaveMark displayed from Patient File but not listed above:

- Sex
- Integration Control Number (ICN)
- Ward,
- Room-Bed
- Internal Entry Number (IEN)

### PII Mapping of Components

RTLS consists of four key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by RTLS 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	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards

		PII? (Yes/No)			
Wavemark	Yes	No	Name, email	Metadata for encounter, user info from InSites SSO, email from address book.	Role Based Access Control (RBAC)
Intelligent InSites	Yes	No	Name, email	Metadata about a case for instrument set, user auditing.	Role Based Access Control (RBAC)
Centrak GMS	No	No	N/A	N/A	Role Based Access Control (RBAC)
Censis CensiTrac	No	No	N/A	N/A	Role Based Access Control (RBAC)

## 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.*

WaveMark has an interface to the VistA PATIENT file, which is used as a lookup to verify patient information. WaveMark also has an interface to the VistA NEW PERSON file, which is used as a lookup for staff identification and scheduling.

### VistA PATIENT File

Table Name Description	Table Description
Encounter Details (ENCOUNTER)	This table stores the metadata of each encounter including the start and end times, attending staff, and encounter number

System User Information (SYSUSER)	This data is populated from the Intelligent InSites Single Sign On mechanism
User Emails (USERADDRESSBOOKENTRY)	This table stores email addresses

### **VistA NEW PERSON File (Employee Interface)**

<b>Table Name Description</b>	<b>Table Description</b>
Recipient of email alert (alert_email_recipient)	The e-mail address for a specific alert recipient
Staff Search History (filter_history)	A history of searches performed by staff members
Staff Login ID (Login)	A login ID for a staff member
Message to Staff Members (Message)	Details of a message delivered to a staff member
Staff Notification Method (notification_delivery)	A delivery method of a notification to staff
System Search History (search_history)	History of all searches performed in the system

### **VistA AEMS/MERS**

<b>Table Name Description</b>	<b>Table Description</b>
Equipment location	Location of equipment
EE number	EE number

### **1.3 How is the information collected?**

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

*If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form's OMB control number and the agency form number.*

*This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.*

Information is collected via barcode scanners (patient wristband), interface with the VistA NEW PERSON FILE and PATIENT FILE, auditing and logging functionalities within the RTLS applications and actions performed by staff such as verifying patient information displayed from patient file.

For asset tracking, data is shared between RTLS and Automated Engineering Management System/Medical Equipment Reporting (AEMS/MERS) using a VistA interface. There is no sensitive data as this is asset demographic information (EE number and location).

### **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.*

The information is collected by the RTLS applications for auditing purposes. Patient and Staff information is also used for lookup purposes such as displaying patient information and scanning patient wristband to verify patient information and for staff identification and scheduling.

### **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 interface with the VistA PATIENT and NEW PERSON files ensures accuracy of the patient and staff information used by the RTLS applications by verifying against information from patient wristband. User management is facilitated by the VA Active Directory, SSOi/IAM and Personal Identification and Verification (PIV).

### **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 following is a list of authorities that define the collection of information:

Presidential Review Directive 5, A National Obligation – Planning for Health Preparedness for and Readjustment of the Military, Veterans, and Their Families after Future Deployments, August 1998. The Department of Veterans Affairs (VA) is authorized to collect this information under the authority of Executive Order 9397 as amended by Executive Order 13478; Title III, Section 301, Subchapter III of Public Law 107-347 (Federal Information Security Management Act of 2002); Section 7406(c)(1) of Title 38 of the U.S. Code; and Sections 4103, 4115, and 4118 of Title 5 of the U.S. Code.

SORN 24VA10A7 states: Title 38, United States Code, Sections 501(b) and 304 is the authority to maintain the system. SORN 79VA10A7 states: Title 38, United States Code, section 7301(a) is the authority to maintain the system.

### **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:** RTLS accesses sensitive personal information, including social security numbers and names on Veterans. 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 financial harm or even identity theft may result.

**Mitigation:** VHA already deploys extensive security measures to protect the information from inappropriate use and/or disclosure through both access controls and training of VHA employees and contractors. VHA's security measures include maintaining the information systems and access terminals in a controlled space. Access to information is restricted by role, responsibility, and access of the employee/contractor accessing the information. Additionally, RTLS has undergone a Security controls assessment as per VA Handbook 6500.

## Section 2. Uses of the Information

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

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

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

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

The information is collected by the RTLS applications for auditing purposes. Patient and Staff information is also used for lookup purposes such as displaying patient information and scanning patient wristband to verify patient information and for staff identification and scheduling.

Description of data elements:

- Name: patients name for verification prior to procedure, user name within the application, staff names attending the encounter. Used internally.
- Email: Collected to send alerts. Used internally.
- Phone number: User identification details within the RTLS applications. Used internally.
- Integration Control Number (ICN): Patient verification.

All data elements listed below, from the VistA PATIENT File, is transmitted to the Wavemark XPOS (Extended Point of Service) stations to confirm positive patient identification. All data is used internally and none of this data is stored during the process.

- Social Security Number
- Date of Birth
- Sex
- Ward
- Room-Bed
- Internal Entry Number (IEN)

## 2.2 What types of tools are used to analyze data and what type of data may be produced?

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

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

*This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information*

The data can be analyzed using the pre-built reports provided by the RTLS applications. Analysis and reporting created by RTLS would contain information about assets and the Cardiac Catheterization Lab. Details about an individual primarily relates to usage of the RTLS applications such as logon information, which is used for auditing purposes. Other uses for this information have not been yet been planned.

## **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.*

Add answer here:

Wavemark: End user request access requests go through the Wavemark Customer Support Center. The center has the local RTLS POC list and they send an email to that POC to get approval. The user must be defined in the application.

Intelligent InSites, Centrak, CensiTrac: These applications are AD integrated. An email request is submitted to the local RTLS POC. The POCs are managers of the VHAXXX RTLS STAFF Active Directory (AD) security groups. Once verified the requestors network account is added to the AD security group.

Elevated privilege accounts are requested and obtained through the e-PAS process.

The SORN for RTLS is 24VA10P2 and is located at the following website:

For the audit log portion of this system, SORN 79VA10P2 is being updated by VHA privacy to include systems with that functionality. Collection of that data and maintaining the system are authorized by Title 38, United States Code, Section 501. The SORN can be found at:

<https://www.oprm.va.gov/docs/sorn/SORN79VA10P2.docx>

As documented in the RTL SSP, proper controls are in place, as per VA Handbook 6500 and NIST Special Publication 800-53.

Training is conducted to ensure information is handled in accordance with the identified policies and regulations. VHA already deploys extensive security controls as per VA Handbook 6500 to protect the information from inappropriate use and/or disclosure through both access controls and training of VHA employees and contractors. VHA's security measures include maintaining the information systems and access terminals in a controlled space. Access to information is restricted by role, responsibility, and access of the employee/contractor accessing the information. Additionally, RTLS has undergone a Security controls assessment as per VA Handbook 6500. RTLS application do not allow self-registration, all access must be approved and provisioned by the administrators. The above mentioned security control families are: Access Control (AC), Awareness & Training (AT), Audit & Accountability (AU), Security Assessment & Authorization (CA), Configuration Management (CM), Contingency Planning (CP), Identification & Authentication (IA), Incident Response (IR), Maintenance (MA), Media Protection (MP), Physical & Environmental Protection (PE), Planning (PL), Personnel Security (PS), Risk Assessment (RA), System & Services Acquisition (SA), System & Communications Protection (SC), System & Information Integrity (SI).

VA has identified this control as a Facility control provided VA-wide by the Office of Information Security (OIS). The policies and procedures are reviewed and/or updated at least every 5 years. VA: a) VA Directive and Handbook 6500 (with appendices), which is a formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities; and compliance; and b) Formal, documented procedures to facilitate the implementation of the access control policies

and associated access controls in: The VA Form 9957 process detailed in this SSP (Appendix A); and VA Handbook 6500.

Typical dissemination by the VA: EO: a) EO Directives and Handbooks, 6500 series, which constitute formal, documented access control policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b) Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls in: The EO implementation details to supplement the VA 9957 process in Appendix A; and CDCO Directive and Handbook 6500.13. The EO Systems Security Office (001E) is responsible for providing subject matter experts and for submitting appropriate updates to the EO Directives and handbooks. The EO Directives Management Officer (00C) has overall responsibility for maintaining publications; ensuring they support VA and EO policies and procedures; are coordinated in the review, comment, and concurrence processes; and maintain history files (document control).

Typical dissemination by EO: AITC: AITC Handbook 6500.13 provides specific system access procedures for EO computer systems, including instructions for requesting elevated privileges. AITC is responsible for effective implementation of all applicable policies and procedures, and reviewing updates to determine if changes affect compliance and/or the security posture of organizational information systems.

HITC: Operating Memorandum (OM) I: ITS-007 - Computer Access Request System (CARS) establishes responsibilities and procedures for system access controls to Region 5 VBA systems administered at AITC, HITC and PITC. PITC: Operating Memorandum (OM) 284-18-05 Remote Access Request Procedures establishes the PITC policy and procedures for the administration of the single point of entry for subjects to access objects that exist outside of the internal VA network, as required by Federal and VA regulations.

#### Windows:

In order to receive a VA Network account the all users must apply for and get permission to use a VA PIV Card. Once approved the user then is placed in the VA active directory for the entire enterprise. The VA Enterprise Network then creates the VA network credentials for each end user on the network. Infrastructure Operations (IO) Platform Support-EWIS only uses approved active directory individual account access to its systems. There are no guest, anonymous, and temporary accounts allowed. VA information systems utilize Group Policy Objects (GPO) to manage Active Directory accounts. Infrastructure Operations (IO) Platform Support-EWIS administrator accounts are reviewed monthly. Administrative accounts do not have an account expiration or inactivity settings. Accounts are created when needed in compliance with password complexity requirements. EWIS administrator rights are managed by Infrastructure Operations (IO) using the VA 9957 process and adhere to the concepts of least privilege and separation of duties. EWIS access is via the TCP/IP network using TACACS (ACS); and absolutely no console access (direct serial connection) is authorized.

#### UNIX:

IO currently uses 3 different mechanisms for account management: (1). VA 9957 (2). Computer Access Request System (CARS) (3). Electronic Permission Access System (ePAS) Regardless of the mechanism, IO manages information system accounts as follows: UNIX Common Responses: c) 9957s are used when creating accounts and granting appropriate access. d) 9957s are used to gather appropriate approvals for access. e) System admins manage all accounts. They provision accounts

only upon a 9957 or appropriate Service Desk Manager (SDM) ticket. f) Guest/anonymous and temporary accounts are not allowed. g) Temporary accounts and need-to-know changes aren't applicable. For terminations and transfers, the 9957 process makes sure all access changes are handled. i) The 9957 process covers expected usage, necessary access, etc.

Linux: a) Guest/anonymous and temporary accounts don't exist. There are individual accounts, service accounts for monitoring and applications (WebLogic, Patrol, Nagios and Oracle) and group accounts users can run commands as. b) Group accounts are built in as part of the install routine; there are open 9957 tickets for those accounts. Individual users are later defined as a member of the group. e) System admins manage all accounts through SUDO. h) Account deletions may come by Service Desk Manager (SDM) ticket if they are inactive for 180 days or 9957 Form.

## Section 3. Retention of Information

The following questions are intended to outline how long information will be retained after the initial collection.

### 3.1 What information is retained?

*Identify and list all information collected from question 1.1 that is retained by the system. This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal*

#### **Information retained:**

Name  
Email  
Phone Number  
Integration Control Number (ICN)

#### **Information not retained:**

Social Security Number (SSN)  
Date of Birth (DOB)  
Sex  
Ward  
Room-Bed  
Internal Entry Number (IEN)

### 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.*

RTLS requires that the data retention shall adhere to the Veterans Health Administration Records Control Schedule (VHA RCS10-1). Currently the data retention is set for 10 years. the VA is continuing to work with the sustainment teams and VHA Records Management to establish a retention plan for RTLS.

**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.*

RTLS requires that the data retention shall adhere to the Veterans Health Administration Records Control Schedule (VHA RCS10-1). The VA is continuing work with the sustainment teams and VHA Records Management to establish a retention plan for RTLS. Additional information can be found here: <https://www.archives.gov/research>.

**3.4 What are the procedures for the elimination of SPI?**

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

Electronic media sanitization: when the records are authorized for destruction (or upon system decommission), will be carried out in accordance with VA 6500.1 HB Electronic Media Sanitization.

Disposition of Printed Data: Forms and other types of printed output produced by any computer systems and related peripherals will be evaluated by the responsible staff member for data sensitivity. Printed output containing sensitive data will be stored in locked cabinets or desks, and disposed of properly (when the approved records schedule permits destruction) by shredding or similar VA approved methods in accordance with VA Directive 6371. Program listings and documentation relating to the use of or access to a computer system require special handling if the listings or documentation provide information about a system which processes sensitive data. VA personnel are responsible for retrieving/removing all printed outputs they request from printers.

Information System Security Officers (ISSO) and Office of Information & Technology (OI&T) IT personnel responsible for media sanitization and destruction access the new media sanitization portal. The responsible OI&T personnel uploads the serial numbers of the media to be destroyed, then sends the pre-sanitized media to the National Media Sanitization program for destruction. Once destruction has been completed, the OI&T personnel are contacted with a confirmation. RTLS follows the VA National Media Sanitization Program to ensure the proper sanitization, destruction and disposal of VA sensitive media that has been used to process, transmit or store VA data and information. RTLS Data Security Destruction Handbook was developed and is followed by all RTLS personnel in support of the mandates of NIST Special Publication 800-88, "Guidelines for Media Sanitization" and the VA Policy Handbook 6500.1, "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*

RTLS is hosted within the VA infrastructure with no PII data used for testing. Access to RTLS testing environments is restricted to a subset of authorized users with the appropriate need-to-know Role Based Access Controls, VA training, and personnel security requirements.

### **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:** It is recognized that there is a risk that information could be retained for longer than necessary to fulfill this system's purposes.

**Mitigation:** RTLS has not been in production long enough to ensure that the information is only retained for the time necessary for RTLS to fulfill its purpose. All records related to this system that are retained shall be kept under penalty of law until an approved Records Retention Schedule is created. The VA is currently working with the sustainment teams to establish a retention plan for RTLS.

## 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

<i>List the Program Office or IT System information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT system</i>	<i>Describe the method of transmittal</i>
Veterans Health Administration (VHA) VistA (Interface name is PATIENT File)	WaveMark associates the patient and procedure information with the supplies used to capture usage and document supplies used for patient care.	Patient Social Security Number (SSN), Name, Date of Birth (DOB), Sex, Ward, Room-Bed, and Internal Entry Number (IEN).	RESTful Web Service Application Programming Interface (API) calls
VistA NEW PERSON File (Interface Name is Employee)	WaveMark collects this information to send alerts.	mail address, Staff Search History, Staff Login ID, Message, Staff Notification Method, System Search History	VistALink, HTTPS
AEMS/MERS (Equipment Movement) Interface	Changes to equipment location are gathered by tag readers and stored in RTLS and then populated to AEMS-MERS to improve inventory processes.	Equipment location, EE number	VistaLink, RESTful Web Service Application Programming Interface (API) calls,

**4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure**

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

Follow the format below:

**Privacy Risk:** There is a risk that RTLS information may be shared with unauthorized VA programs or systems.

**Mitigation:** Safeguards implemented to ensure data is not sent to the wrong VA organization are employee security and privacy training and awareness, and required reporting of suspicious activity. Use of secure authentication and authorization methods such as integration with SSO/IAM, PIV, and access on need-to-know basis are all measures that are utilized within the facilities.

## **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*

RTLS does not share any sensitive information with external organizations

*Data Shared with External Organizations*

<i>List External Program Office or IT System information is shared/received with</i>	<i>List the purpose of information being shared / received / transmitted with the specified program office or IT system</i>	<i>List the specific data element types such as PII/PHI that are shared/received with the Program or IT system</i>	<i>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</i>	<i>List the method of transmission and the measures in place to secure data</i>
CensiTrac	Data backup capability	Non-sensitive data of surgical instrument location, sterilization and set assembly information.	National MOU/ISA	Transit Gateway (TGW)

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

In order to protect Veteran personally identifiable information (PII) the following activities occur as part of the overall information assurance activities:

1. 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.
2. 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.
3. 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.
4. Internal protection is managed by access controls such as user IDs and passwords, authentication, 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:** As RTLS does not share sensitive data with any outside organizations, there are minimal to no privacy risks to the data collected, stored, and maintained in the system.

**Mitigation:** The key mitigation to any privacy risk related to external sharing of VA data from RTLS is that the system does not share sensitive data with any external organizations or systems.

## Section 6. Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

**6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?**

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

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

*Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection. This question is related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.*

The Notice of Privacy Practice (NOPP) is a document which explains the collection and use of protected information to individuals applying for VHA benefits. A Veteran is sent a Notice every three years or sooner if a significant change to policy occurs. Employees and contractors are required to review, sign and abide by the National Rules of Behavior on an annual basis.

The Department of Veterans Affairs provides additional notice of this system by publishing System of Record Notices (SORNs):

- 1) The VA System of Record Notice (VA SORN) Patient Medical Records-VA, SORN 24VA10P2 (Feb. 11, 2014), in the Federal Register and online. An online copy of the SORN can be found at: <http://www.gpo.gov/fdsys/pkg/FR-2014-02-11/pdf/2014-02890.pdf>
- 2) The VA System of Record Notice (VA SORN) Veterans Health Information System and Technology Architecture (VISTA) - VA, SORN 79VA10P2 (Amended Oct. 31, 2012), in the Federal Register and online. An online copy of the SORN can be found at: <http://www.gpo.gov/fdsys/pkg/FR-2012-10-31/pdf/2012-26804.pdf>

This Privacy Impact Assessment (PIA) also serves as notice of RTLS. 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.”

VHA provides effective notice regarding collection, use, sharing, safeguarding, maintenance and disposal of PII, authority for collecting PII and the ability to access or amended PII through its Privacy Act SORNs. In Version Date: October 1, 2017 addition, the VHA Notice of Privacy Practices (NOPP) provides notice on privacy practices including collection, use and disclosure of PII and PHI and privacy rights such as the ability to access and amendment.

The VHA NOPP is provided to newly enrolled Veterans at the time of enrollment and currently enrolled Veterans annually. VHA also provides notice on the authority for collecting PII and choices regarding the PII at the point of collection. VHA permits individuals to agree to the collection of their PII through the use of paper and electronic forms that include Privacy Act Statements outlining why the information is being collected, how it will be used and what system of records the information will be stored.

The Privacy Act Statements on the paper and electronic forms explain whether data collection is mandatory or voluntary, and explains the consequences of not providing the information when data collection is voluntary. In addition, information is collected verbally from individuals. These individuals are made aware of why data is collected through the VHA NOPP and conversations with VHA employees.

VA Forms are reviewed by VHACO periodically to ensure compliance with various requirements including that Privacy Act Statements are on forms collecting personal information from Veterans or individuals. Lastly, VHA provides such notice in its PIAs which are published for public consumption.

## **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*

The Veterans’ Health Administration (VHA) as well as the Real Time Location System (RTLS) only request information necessary to administer benefits to Veterans and other potential

beneficiaries. While an individual may choose not to provide information to the VHA; this will prevent them from obtaining the benefits necessary to them. Individuals have a right to deny the use of their health information and/or IIHI and for the purpose of research.

VHA Handbook 1605.1 Appendix D ‘Privacy and Release Information’, section 5 lists the rights of the Veterans to request VHA to restrict the uses and/or disclosures of the individual’s individually-identifiable health information to carry out treatment, payment, or health care operations. The Veterans have the right to refuse to disclose their SSN to VHA. The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VHA an SSN (see 38 CFR 1.575(a)).

### **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*

VHA permits individuals to agree to the collection of their personally identifiable information (PII) through the use of paper and electronic forms that include Privacy Act Statements outlining why the information is being collected, how it will be used and what Privacy Act system of records the information will be stored. In addition, information is collected verbally from individuals. These individuals are made aware of why data is collected through the VHA Notice of Privacy Practices and conversations with VHA employees. VA Forms are reviewed by VHACO periodically to ensure compliance with various requirements including that Privacy Act Statements are on forms collecting personal information from Veterans or individuals. VHA uses PII and PHI only as legally permitted including obtaining authorizations were required. Where legally required, VHA obtains signed, written authorizations from individuals prior to releasing, disclosing or sharing PII and PHI.

### **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 disseminated by RTLS.

**Mitigation:** This risk is mitigated by the common practice of providing the NOPP when Veterans apply for benefits. Additionally, NOPPs are mailed out every three years Veterans and to beneficiaries. 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 Veterans

online access to their health 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 information from the medical facility's Release of Information (ROI) office. Employees should contact their facility Privacy Officer to obtain information. Contractors should contact Contract Officer Representative to obtain information upon request.

Redress procedures are listed in the VA System of Record Notices (SORNs):

1) The VA System of Record Notice (VA SORN) Patient Medical Records-VA, SORN 24VA10P2 (Feb. 11, 2014), in the Federal Register and online. An online copy of the SORN can be found at: <http://www.gpo.gov/fdsys/pkg/FR-2014-02-11/pdf/2014-02890.pdf>

2) The VA System of Record Notice (VA SORN) Veterans Health Information System and Technology Architecture (VISTA) - VA, SORN 79VA10P2 (Amended Oct. 31, 2012), in the Federal Register and online. An online copy of the SORN can be found at:

<http://www.gpo.gov/fdsys/pkg/FR-2012-10-31/pdf/2012-26804.pdf>

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

*Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed. If the correction procedures are the same as those given in question 7.1, state as much.*

*This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.*

The procedure for correcting inaccurate or erroneous information begins with a Veteran requesting the records in question from Release of Information (ROI). The Veteran then makes an amendment request in writing to reflect the information that they believe to be inaccurate, untimely, irrelevant or incomplete. The request for amendment is sent to the facility Privacy Office for processing. The documents are then forwarded to the practitioner who wrote the information by the facility Privacy Officer. The practitioner either grants or denies the amendment. Once the practitioner has reviewed the requested amendment, the privacy officer either makes the change or sends the Veteran a letter with their appeal right to the Office of General Counsel. The Veteran is notified of the decision via letter by the facility Privacy Officer. The requirement is to complete the request within 10 working days but not to exceed 90 working days. Employees and Veterans should contact their facility Privacy Officer for additional information.

Redress procedures are listed in the VA System of Record Notices (SORNs):

1) The VA System of Record Notice (VA SORN) Patient Medical Records-VA, SORN 24VA10P2 (Feb. 11, 2014), in the Federal Register and online. An online copy of the SORN can be found at: <http://www.gpo.gov/fdsys/pkg/FR-2014-02-11/pdf/2014-02890.pdf>

2) The VA System of Record Notice (VA SORN) Veterans Health Information System and Technology Architecture (VISTA) - VA, SORN 79VA10P2 (Amended Oct. 31, 2012), in the Federal Register and online. An online copy of the SORN can be found at:

### **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 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 facility ROI office.

Redress procedures are listed in the VA System of Record Notices (SORNs):

1) The VA System of Record Notice (VA SORN) Patient Medical Records-VA, SORN 24VA10P2 (Feb. 11, 2014), in the Federal Register and online. An online copy of the SORN can be found at: <http://www.gpo.gov/fdsys/pkg/FR-2014-02-11/pdf/2014-02890.pdf>

2) The VA System of Record Notice (VA SORN) Veterans Health Information System and Technology Architecture (VISTA) - VA, SORN 79VA10P2 (Amended Oct. 31, 2012), in the Federal Register and online. An online copy of the SORN can be found at: <http://www.gpo.gov/fdsys/pkg/FR-2012-10-31/pdf/2012-26804.pdf>

### **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 ensure data accuracy.*

Formal redress procedure is listed in the VA System of Record Notices (SORNs):

1) The VA System of Record Notice (VA SORN) Patient Medical Records-VA, SORN 24VA10P2 (Feb. 11, 2014), in the Federal Register and online. An online copy of the SORN can be found at: <http://www.gpo.gov/fdsys/pkg/FR-2014-02-11/pdf/2014-02890.pdf>

2) The VA System of Record Notice (VA SORN) Veterans Health Information System and Technology Architecture (VISTA) - VA, SORN 79VA10P2 (Amended Oct. 31, 2012), in the Federal Register and online. An online copy of the SORN can be found at: <http://www.gpo.gov/fdsys/pkg/FR-2012-10-31/pdf/2012-26804.pdf>

Veterans and other individuals are encouraged to use the formal redress procedures discussed above 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 be familiar with 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 Veteran and Beneficiary receive, discusses the process for requesting an amendment to ones records. The VHA staffs Release of Information (ROI) office at facilities assist Veterans with obtaining access to their health records. The Veterans' Health Administration (VHA) established MyHealthVet 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 and Release of Information Handbook 1605.1 establishes procedures for Veterans to have their records amended.

Additionally, redress procedures are listed in the VA System of Record Notices (SORNs):

1) The VA System of Record Notice (VA SORN) Patient Medical Records-VA, SORN 24VA10P2 (Feb. 11, 2014), in the Federal Register and online. An online copy of the SORN can be found at:

<http://www.gpo.gov/fdsys/pkg/FR-2014-02-11/pdf/2014-02890.pdf>

2) The VA System of Record Notice (VA SORN) Veterans Health Information System and Technology Architecture (VISTA) - VA, SORN 79VA10P2 (Amended Oct. 31, 2012), in the Federal Register and online. An online copy of the SORN can be found at:

<http://www.gpo.gov/fdsys/pkg/FR-2012-10-31/pdf/2012-26804.pdf>

## 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 control will be Role Based. The Users/Staff will have the concept of least privileges enabled. In general, the roles within the RTL System fall in two categories:

- Administrator – Base role, read and edit access for RTLS admins.
- Staff – Base role, read only access.

RTLS Administrators will need to submit a request through the e-PAS system. They will log on with their Non Mail Enabled Account utilizing two factor authentication including PIV/Username & Password and eToken. Standard users will utilize VA credentials such as

Active Directory (AD) and PIV to access the system. RTLS does not allow for user self-registration, to gain access to the system, a user must request access, through the local biomedical organization or COTS Support Center. Access will be reviewed and approved based on need to know access.

Wavemark: End user request access requests go through the Wavemark Customer Support Center. The center has the local RTLS POC list and they send an email to that POC to get approval. The user must be defined in the application.

Intelligent InSites/Centrak/Censitrac: These applications are AD integrated. An email request is submitted to the local RTLS POC. The POCs are managers of the VHAXXX RTLS STAFF Active Directory (AD) security groups. Once verified the requestor's network account is added to the AD security group.

VA has identified this control as a Facility control provided VA-wide by OIS. The policies and procedures are reviewed and/or updated at least every 5 years. VA: a) VA Directive and Handbook 6500 (with appendices), which is a formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities; and compliance; and b) Formal, documented procedures to facilitate the implementation of the access control policies and associated access controls in: The VA Form 9957 process detailed in this SSP (Appendix A); and VA Handbook 6500.

Typical dissemination by the VA: EO: a) EO Directives and Handbooks, 6500 series, which constitute formal, documented access control policies that address purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and b) Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls in: The EO implementation details to supplement the VA 9957 process in Appendix A; and CDCO Directive and Handbook 6500.13. The EO Systems Security Office (001E) is responsible for providing subject matter experts and for submitting appropriate updates to the EO Directives and handbooks. The EO Directives Management Officer (00C) has overall responsibility for maintaining publications; ensuring they support VA and EO policies and procedures; are coordinated in the review, comment, and concurrence processes; and maintain history files (document control).

Typical dissemination by EO: AITC: AITC Handbook 6500.13 provides specific system access procedures for EO computer systems, including instructions for requesting elevated privileges. AITC is responsible for effective implementation of all applicable policies and procedures, and reviewing updates to determine if changes affect compliance and/or the security posture of organizational information systems.

HITC: Operating Memorandum (OM) I: ITS-007 - Computer Access Request System (CARS) establishes responsibilities and procedures for system access controls to Region 5 VBA systems administered at AITC, HITC and PITC. PITC: Operating Memorandum (OM) 284-18-05 Remote Access Request Procedures establishes the PITC policy and procedures for the administration of the single point of entry for subjects to access objects that exist outside of the internal VA network, as required by Federal and VA regulations.

Windows:

In order to receive a VA Network account the all users must apply for and get permission to use a VA PIV Card. Once approved the user then is placed in the VA active directory for the entire enterprise. The VA Enterprise Network then creates the VA network credentials for each end user on the network. Infrastructure Operations (IO) Platform Support-EWIS only uses approved active directory individual account access to its systems. There are no guest, anonymous, and temporary accounts allowed. VA information systems utilize Group Policy Objects (GPO) to manage Active Directory accounts. Infrastructure Operations (IO) Platform Support-EWIS administrator accounts are reviewed monthly. Administrative accounts do not have an account expiration or inactivity settings. Accounts are created when needed in compliance with password complexity requirements. EWIS administrator rights are managed by Infrastructure Operations (IO) using the VA 9957 process and adhere to the concepts of least privilege and separation of duties. EWIS access is via the TCP/IP network using TACACS (ACS); and absolutely no console access (direct serial connection) is authorized.

#### UNIX:

IO currently uses 3 different mechanisms for account management: (1). VA 9957 (2). Computer Access Request System (CARS) (3). Electronic Permission Access System (ePAS) Regardless of the mechanism, IO manages information system accounts as follows: UNIX Common Responses: c) 9957s are used when creating accounts and granting appropriate access. d) 9957s are used to gather appropriate approvals for access. e) System admins manage all accounts. They provision accounts only upon a 9957 or appropriate Service Desk Manager (SDM) ticket. f) Guest/anonymous and temporary accounts are not allowed. g) Temporary accounts and need-to-know changes aren't applicable. For terminations and transfers, the 9957 process makes sure all access changes are handled. i) The 9957 process covers expected usage, necessary access, etc.

Linux: a) Guest/anonymous and temporary accounts don't exist. There are individual accounts, service accounts for monitoring and applications (WebLogic, Patrol, Nagios and Oracle) and group accounts users can run commands as. b) Group accounts are built in as part of the install routine; there are open 9957 tickets for those accounts. Individual users are later defined as a member of the group. e) System admins manage all accounts through SUDO. h) Account deletions may come by Service Desk Manager (SDM) ticket if they are inactive for 180 days or 9957 Form.

### **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.*

VA contract employee access is verified through the Contracting Officer's Representative (COR) and other VA supervisory/administrative personnel before access is granted to any VA system. Contractor access is reviewed annually at a minimum. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of behavior training via the VA Talent Management System (TMS). All contractors are vetted using the VA background investigation process and must obtain the appropriate level background investigation for their role. Contractors with systems administrative access are required to complete additional role-based training prior to gaining system administrator access. Generally, contracts are reviewed at the start of the initiation phase of acquisitions and again during procurement of option years by the Contracting Officer, Information Security Officer, Privacy Officer, COR, Procurement Requestor/Program Manager and any other stakeholders required for approval of the acquisition. Contracts generally have an average duration of 1 -3 years and may have option years stipulated in the original contract.

Contractors will have access to the system and the contracts will be reviewed annually by the Project COR. All contractors with Logical Access are required to have a Background investigation initiated, completed Information Security and Privacy Training, signed the Contractor rules of behavior and sign a Non-Disclosure agreement.

**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.*

Personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the VA Privacy and Security Awareness training which all personnel must complete via the VA's Talent Management System (TMS). After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the privacy and security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system. 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. System administrators are required to complete additional role-based training. Users with access to PHI are required to complete HIPAA privacy training annually.

Employees are required to take Annual Information Security and Privacy Training.in TMS. Contractors with Logical Access or access to VA sensitive information are required to take Information Security and Privacy Training along with signing a Non-Disclosure Agreement.



#### **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.***

RTLS has an active Authority To Operate (ATO) issued 2/8/2021 for 180 days. The ATO expires on 8/7/2021.

## Section 9. References

### Summary of Privacy Controls by Family

*Summary of Privacy Controls by Family*

<b>ID</b>	<b>Privacy Controls</b>
<b>AP</b>	<b>Authority and Purpose</b>
AP-1	Authority to Collect
AP-2	Purpose Specification
<b>AR</b>	<b>Accountability, Audit, and Risk Management</b>
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
<b>DI</b>	<b>Data Quality and Integrity</b>
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
<b>DM</b>	<b>Data Minimization and Retention</b>
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
<b>IP</b>	<b>Individual Participation and Redress</b>
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
<b>SE</b>	<b>Security</b>
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
<b>TR</b>	<b>Transparency</b>
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
<b>UL</b>	<b>Use Limitation</b>

<b>ID</b>	<b>Privacy Controls</b>
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

**Signature of Privacy Officers**

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

---

**Privacy Officer**

**Signature of Information Security Systems Officers**

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

---

**Information Security Systems Officer**

**Signature of Area Manager**

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

---

**Area Manager**

## 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).

Link to VA Privacy Website: <https://www.va.gov/privacy/>.

Link to VHA Notice of Privacy Practices:

[https://www.va.gov/vhapublications/ViewPublication.asp?pub\\_ID=3048](https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=3048).

VA Form 10-10 EZ Privacy Act Statement:

Privacy Act Information: VA is asking you to provide the information on this form under 38 U.S.C. Sections 1705, 1710, 1712, and 1722 in order for VA to determine your eligibility for medical benefits. Information you supply may be verified from initial submission forward through a computer-matching program. VA may disclose the information that you put on the form as permitted by law. VA may make a "routine use" disclosure of the information as outlined in the Privacy Act systems of records notices and in accordance with the VHA Notice of Privacy Practices. Providing the requested information is voluntary, but if any or all of the requested information is not provided, it may delay or result in denial of your request for health care benefits. Failure to furnish the information will not have any effect on any other benefits to which you may be entitled. If you provide VA your Social Security Number, VA will use it to administer your VA benefits. VA may also use this information to identify Veterans and persons claiming or receiving VA benefits and their records, and for other purposes authorized or required by law.

VA Form 10-10EZR Privacy Act Statements:

PAPERWORK REDUCTION ACT AND PRIVACY ACT INFORMATION
<p>The Paperwork Reduction Act of 1995 requires us to notify you that this information collection is in accordance with the clearance requirements of Section 3507 of the Paperwork Reduction Act of 1995. We may not conduct or sponsor, and you are not required to respond to, a collection of information unless it displays a valid OMB number. We anticipate that the time expended by all individuals who must complete this form will average 15 minutes. This includes the time it will take to read instructions, gather the necessary facts and fill out the form.</p>
<p>Privacy Act Information: VA is asking you to provide the information on this form under 38 U.S.C. Sections 1710, 1712, and 1722 in order for VA to determine your eligibility for medical benefits. Information you supply may be verified from initial submission forward through a computer matching program. VA may disclose the information that you put on the form as permitted by law. VA may make a "routine use" disclosure of the information as outlined in the Privacy Act systems of records notices and in accordance with the Notice of Privacy Practices. Providing the requested information is voluntary, but if any or all of the requested information is not provided, it may delay or result in denial of your request for health care benefits. Failure to furnish the information will not have any effect on any other benefits to which you may be entitled. If you provide VA your Social Security Number, VA will use it to administer your VA benefits. VA may also use this information to identify veterans and persons claiming or receiving VA benefits and their records, and for other purposes authorized or required by law.</p>