Privacy Impact Assessment for the VA IT System called:

ARANZ Wound Management System

Veterans Health Administration

Office of Connected Care – VHA Telehealth Services

#1371

Date PIA submitted for review:

06/05/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Dennis Lahl	Dennis.Lahl@va.gov	202-461-7330
Information System Security Officer (ISSO)	Oliver Patague	Oliver.Patague@va.gov	509-910-2849
Information System Owner	Harpreet Sodhi	Harpreet.Sodhi@va.gov	240-421-5445

Abstract

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

The Applied Research Associates New Zealand (ARANZ Silhouette) Wound Management System consists of suite of software that helps generate wound metrics. ARANZ captures the images and metrics, this allows the provider to make clinical decisions regarding treatment. The system allows for expedited treatment recommendations and can be utilized to facilitate telehealth wound management.

Developed by ARANZ and provided to VA. The ARANZ Silhouette Wound Management System is used for managing care of wounds and creates metrics around healing of those wounds. Silhouette allows for clinical guidance for clinical staff. Per BIA, Section 3: (1) Provide Access to Healthcare using Latest Technologies, (2) Capture Diagnostic Image MirthConnect: MirthConnect is a cross-platform interface engine used in the healthcare industry that enables the management of information using bi-directional sending of many types of messages. Addition of Software Application (Use of Mirth Connect, Mirth Connect (va.gov). ICR 723 - integration with Oracle Health for VA National will require ARANZ to install middleware software called MirthConnect. This will connect to Cerner Millennium for the Electronic Health Record (EHR), Bidirectional. We will receive Admission Discharge Transfer (ADT) from Oracle Health and ARANZ will be sending Health Level 7 (HL7) Messages back. Aranz will be required to send pdfs to Oracle Health via Centralized VistA Imaging Exchange (CVIX) and Cerner CVIX Integration Adapter (CCIA). New external connection (i.e., ports, protocols, or services) to Oracle Health.

Overview

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

1 *General Description*

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

The ARANZ Wound Management System is owned by the Veterans Health Administrations (VHA), Office of Connected Care.

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

The purpose of the system is to gather information surrounding a wound healing by providing clinicians with data that can be utilized to expedite treatment and decrease healing times of wounds. The system helps meet the VA's mission to provide quality timely care to veterans. The system hosts the patient data in the VAEC Azure Cloud. Work Item - ICR 723 - Integration with Oracle Health for VA National. This will require ARANZ to install middleware software called MirthConnect. This will connect to Cerner Millennium for the Electronic Health Record (EHR), Bidirectional. We will receive Admission Discharge Transfer (ADT) from Oracle Health and ARANZ will be sending Health Level 7 (HL7) Messages back. ARANZ will be required to send pdfs to Oracle Health via Centralized VistA Imaging Exchange (CVIX) and Cerner CVIX

Integration Adapter (CCIA). New external connection (i.e., ports, protocols, or services) to Oracle Health.

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

The ARANZ Wound Management System is VA owned and Non-VA operated by the Veterans Health Administrations (VHA), Office of Connected Care – VHA Telehealth Services and ARANZ and IronBow.

2. Information Collection and Sharing

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

The number of individuals incorporated into the system is currently at 5000 patients with 28000 active wound assessments. There is continued growth expected in veteran and assessment count. The patients who will be utilizing the system will have a wound of various clinical need. The information housed within the system are the patient full names, Electronic Data Interchange Personal Identifier (EDIPI), date of birth (DOB), birth gender, self-identified gender, and wound images. External connections exist with the VHA Unified Electronic Health Record (EHR) through the Cerner Corporation [now known as Oracle Health] (National ISA/ MOU – Cerner VA ISA/MOU – ID: E-2168) and DoD Defense health Agency (Interagency Agreement DOD DHA VA National MEDCOI ISA – ID 733).

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

The ARANZ system will be used across the VA system of care. Standard data input will be implemented and maintained through the central server. End users are not directly inputting data via SilhouetteCentral. They use SilhouetteConnect. Edits to the information can be performed through SilhouetteCentral, the centralized database that is located within the VAEC environment. Protected Individual Identifiable (PII) and use is monitored through the central database. ARANZ Silhouette has TRM approval. ICR 723 - integration with Oracle Health for VA National. This will require ARANZ to install middleware software called MirthConnect. This will connect to Cerner Millennium for the Electronic Health Record (EHR), Bidirectional. we will receive Admission Discharge Transfer (ADT) from Oracle Health and ARANZ will be sending Health Level 7 (HL7) Messages back. Aranz will be required to send pdfs to Oracle Health via CVIX/CCIA. New external connection (i.e., ports, protocols, or services) to Oracle Health. VA has a contract with the vendor under contract # V17-01041-001. ARANZ Wound Management system operates under the following system authority of Title 38, United States Code, Section 501(b); SORN of Patient Medical Records – VA SORN (24VA10A7), October 2, 2020 (previously (24VA10P2). Legal Authority. Title 38, United State Code, Sections 501(b) and 304.

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

The ARANZ Wound Management System consists of the ARANZ SilhouetteConnect software, ARANZ SilhouetteCentral, and the ARANZ SilhouetteStar. SilhouetteConnect is software that is installed on a VA workstation that helps collect data and generate wound metrics. SilhouetteCentral is the central database where images are housed and allows for expedited provider review. SilhouetteCentral allows for account management for the creation of groups and users utilizing the Microsoft Entra ID usernames for various sites/facilities. SilhouetteStar is the physical scanner that captures the images using lasers to ensure that the proper focal point is attained for each image. The system captures an image of a wound and the software generates metrics around the wounds healing. Length, Width, Depth, Volume, Area, and Area reduction are captured, and these metrics allow the provider to make clinical decisions regarding treatment. The system allows for expedited treatment recommendations and can be utilized to facilitate telehealth wound management. The system is cloud-based hosted in the VA Enterprise Cloud (VAEC) Azure Cloud which allows comparing of wound healing. It can potentially augment managing wounds and identifying which sites have the best management regarding wound healing.

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

Yes, ARANZ Wound Management System has the potential to impact business practice by gathering information around wound healing on a large scale. This data can impact the business process by identifying areas for improvement and can potentially lower cost for all VHA sites. The implementation of the ARANZ system has the potential to close the gap between clinical providers and technological monitoring providing a more robust picture of how effective treatments are being utilized. A contract is in place between VA and Microsoft Azure as a GovCloud service provider. VA is the owner of the data for all VA projects/products whose applications are hosted in the VAEC Azure Cloud. Also, Azure's FedRAMP High certification states VA is owner of all VA application data, including PII. As described in the above referenced contract between the VA and Microsoft Azure, the accountability for security and privacy of data held by the Azure Cloud provider is described. Significant harm will result in intentional or unintentional disclosure of PII/PHI data. The reputation of the cloud provider and its customers would most likely be affected with such disclosure. The database is not accessible from any external internet. Veteran's safety is the highest priority and all data that is kept will be minimal to ensure veterans privacy. Access to the database will be limited and users must have elevated privilege access which follows the established Office of Information Technology procedures.

3. Legal Authority and SORN

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

The ARANZ Wound Management System operates under contract # V17-01041-001. The legal authority is HIPAA Privacy Rule, 45 CFR Parts 160 and 164. The patient medical record information is found under the SORN of Patient Medical Records – VA SORN (24VA10A7 / 85 FR 62406), October 2, 2020. Legal Authority: Title 38, United State Code, Sections 501(b) and 304. (https://www.oprm.va.gov/privacy/systems_of_records.aspx).

I. *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? No*
If the system is using cloud technology, does the SORN for the system cover cloud usage or storage? Yes

4. System Changes

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

Yes, Modifications will reduce the current number of steps needed for the end-user. MirthConnect will be added but will be installed onto the same server as ARANZ. This will increase the security support required to maintain all required connections.

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

Yes, integration with Oracle Health for VA National will require ARANZ to install middleware software called MirthConnect. This will connect to Oracle Health for the Electronic Health Record (EHR), Bidirectional. we will receive Admission Discharge Transfer (ADT) from Oracle Health and ARANZ will be sending Health Level 7 (HL7) Messages back. Aranz will be required to send pdfs to Oracle Health via Centralized VistA Imaging Exchange (CVIX) / Cerner CVIX Integration Adapter (CCIA). Operating System - ARANZ is currently utilizing Windows 2016 on pre-prod and production servers which are in Divest. ARANZ will be upgrading the Operating System to Windows Server 2022 for ARANZ pre-production and production servers. (Windows Server (va.gov)).

Section 1. Characterization of the Information

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

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

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

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

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

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

☒ Name
☐ Social Security Number
☒ Date of Birth

☐ Mother's Maiden Name
☐ Personal Mailing Address

☐ Personal Phone Number(s)

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

Other PII/PHI data elements: (Per Direction of Privacy Officer Dennis Lahl – adding below)
☒ EDIPI
☒ Wound Imaging
☒ Note for Gender: Birth Sex and Self-Identified Gender Identify
☒ Microsoft Entra ID – User Accounts (Which includes their work email accounts

PII Mapping of Components (Servers/Database)

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

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

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards

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

ARANZ Production Database:	Yes	Yes	• EDIPI • Name – Last, First, Middle • Date of Birth • Birth sex • Self-identified gender identity • Wound Images (wound size, dimensions, and location)	To allow for the transfer of data within the ARANZ Wound Management System and allow for provider review	The data is located within a VAEC cloud environment, protected by various defense in depth devices and agents, and encrypted. Access to the to the server also requires additional access approvals.
ARANZ Preproduction Database:	Yes	Yes	• Sampling subset of the following is used in preprod for testing and configuration verification • EDIPI • Name – Last, First, Middle • Date of Birth • Birth sex • Self-identified gender identity • Wound Images (wound size, dimensions, and location)	To allow for the transfer of data within the ARANZ Wound Management System and allow for provider review	The data is located within a VAEC cloud environment, protected by various defense in depth devices and agents, and encrypted. Access to the to the server also requires additional access approvals.

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

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

Information is collected and verified from the Veteran and added to the patient record by Oracle Health. Oracle Health then sends over patient details via ADT feed. A wound image or assessment report can be generated in PDF within the system that shows wound healing metrics using ARANZ and will contain PII/PHI information. This PDF report gets sent back to Oracle Health and becomes part of the patient record in the EHR.

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.*

There is nothing pulled from public websites or a commercial aggregator.

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

System uses copies of records; it is not a source of data**.** The actual data records are in Oracle Health Millennium. For sites connected to Oracle Health the information is exchanged bi-directionally and via an automated process. For sites not yet using Oracle Health the uploading of data from Silhouette to Oracle Health is a manual process**.**

1.3 How is the information collected?

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

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

The information can be collected from patient directly. For sites utilizing Oracle Health's Millennium EHR the data is received via electronic transmission.

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?

Photographs, digital images, and other non-written media images when obtained for treatment purposes must be placed in the health record, and are subject to all of the same privacy regulations for use and disclosure as the entire content of the patient's health record, accordance to VHA Handbook 1907.01, *Health Information Management and Health Records* and Authority U.S.C 305, 5723(d), 5727(9); 44 U.S.C 3102(1).

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

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

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

Information is collected and verified when patient profiles are created. Once created patient information can only be modified within the Cerner Millennium. The Veterans' identifying information is checked for accuracy by the Clinicians and is cross-referenced with information on the Veterans.

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?

The Veterans' identifying information is checked for accuracy by the Clinicians and is cross-referenced with information on the Veterans.

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

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

The ARANZ Wound Management System operates under contract # V17-01041-001. The legal authority is HIPAA Privacy Rule, 45 CFR Parts 160 and 164. The patient medical record information is found under the SORN of Patient Medical Records – VA SORN (24VA10A7), October 2, 2020. Legal Authority: Title 38, United State Code, Sections 501(b) and 304.

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: The system contains sensitive personal information such as Name – Last, First, Middle; Date of Birth, Birth Sex, Self-Identified Gender Identity and location of the patient's wound. Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious harm, or even identity theft may result.

Mitigation: VHA deploys extensive security measures to protect the patient information from inappropriate use and/or disclosure through both access and training of government personnel within VHA to include access control, configuration management, media protection, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information integrity, security assessment and authorization, incident response, risk assessment, planning and maintenance.

The system is managed by Office of Information and Technology (OI&T) via the cloud server by the system administrator utilizing two-factor authentication (2FA) NEMA with zero account tokens for accessing the servers. Azure dashboard or via direct CyberArk. User access is managed via Microsoft Entra ID/LEAF applications. The software is TRM approved. Minimal information regarding patient information is collected. VA guidelines regarding PII will be observed.

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 training, and HIPAA Privacy Training. Patient health records are, by law, confidential regardless of medium. The privacy of patient information must be preserved, and the information must not be accessible to, or discussed with, any unauthorized persons, nor is the information to be discussed in public areas.

Every employee with access to patient health records in any medium is responsible for the proper use, disclosure, and handling of the patient health records (see VHA Directive 1605.01 Privacy and Release of Information, VHA Directive 1605 VHA Privacy Program and VA Directive 6500, Information Security Program). They are also accountable for safeguarding patient confidentiality and privacy, and failure to do so results in administrative action, up to and including, termination or other legal adverse action.

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 – Last, First, Middle	File Identification purposes	Not used

EDIPI	File Identification purposes	Not used
Date of Birth	File Identification purposes	Not used
Birth Sex	File Identification purposes	Not used
Self-Identified Gender Identity	File Identification purposes	Not used
Wound Information	File Identification purposes	Not used
Microsoft Entra ID – User Accounts (Which includes their work email accounts	File Identification purposes	Not used

The data allows for decision support and early intervention of our most critically ill patients. System information is required to identify individual patients and allow for patient charting and continuity of care between shifts and transfer to other health care providers. Use is in-line with VA practices for caring. Information collected will be used to validate treatments for wound care. Utilization of the ARANZ system provides valuable metrics that can be used to expedite care, identify effective treatments for wounds, track hospital acquired pressure injuries, and showcase outstanding wound healing clinics that can provide best practices to other sites. The use of the ARANZ system will meet the mandates of providing expedited care for Veterans.

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

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

ARANZ Silhouette software conducts 3D Wound imaging. The system captures an image of a wound and the software generates metrics around the wounds healing. Metrics include wound location on the body, area, width, length, perimeter, volume, and depth. Area reduction is a key measure of healing and is tracked for each wound. An image of the wound is used to allow remote providers to view the wound and with the metrics make clinical decisions and treatment recommendations. The information is stored in the patients record in Silhouette and will be stored in Oracle Health as well. The information will be generated into a PDF report once the wound image is captured by ARANZ Silhouette. This information will be accessible to VA employees who will make determinations regarding patient care. This information will be available to providers for clinicians to use in patient monitoring, management, diagnostic, and treatment of Veterans for store and forward telehealth care and to increase communication between services. MirthConnect is a cross-platform interface engine used in the healthcare industry that enables the management of information using bi-directional sending of many types of messages. Connection to Oracle's Cerner Millennium Electronic Health Record (EHR) consists of MirthConnect software as described above and Centralized VistA Imaging Exchange (CVIX). The connection is bidirectional.

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.*

Silhouette captures images of wounds and wound measurements. This data is upload into the VA EHR.

2.3 How is the information in the system secured?

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

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

The PII/PHI is located within a VAEC cloud environment, protected by various defense in depth devices and agents, and further encrypted. The servers have installed specific security applications: Trellix, firewall implementation, Dynatrace, Microsoft Monitoring Agent, Splunk, and Venafi. Access to the to the server also requires additional access approvals and authentication.

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

The ARANZ system does NOT collect, process, or retain Social Security Numbers. ARANZ utilizes EDIPI.

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

The PII/PHI is located within a VAEC cloud environment, protected by various defense in depth devices and agents, and further encrypted. The servers have installed specific security applications: Trellix, firewall implementation, Dynatrace, Microsoft Monitoring Agent, Splunk, and Venafi. Access to the to the server also requires additional access approvals and authentication.

2.4 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u>

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:

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

<u>Principle of Use Limitation:</u> 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?

Specific sites utilizing Oracle Health Millennium will have access through Millennium. Individuals who will use the ARANZ system will be identified through their sites and will be able to capture images using the ARANZ SilhouetteConnect software. MirthConnect is a cross-platform interface engine used in the healthcare industry that enables the management of information using bi-directional sending of many types of messages. Connection to Oracle's Cerner Millennium Electronic Health Record (EHR) consists of MirthConnect software as described above and Centralized VistA Imaging Exchange (CVIX). The connection is bidirectional.

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

Users will need to complete a LEAF access request and TMS course to gain access to Silhouette. Silhouette access is established utilizing Microsoft Identity Manager (MIM) to update records in Microsoft Entra ID, not local user accounts. Once access is approved, verified, and granted by the ARANZ Administrator (VA government employee), they will be able to use the system. There are regular reviews of user access to evaluate whether users have accessed the system within the past 35 days. If no access with 35 days user access is disabled.

The system will be managed by Office of Information and Technology (OI&T) via the cloud server by system administrator utilizing two-factor authentication (2FA) NEMA with zero account tokens for accessing the servers. Azure dashboard or via direct RDP (CyberArk). Access to ARANZ is monitored, tracked, and recorded through audit logging at system, network, and application level. User access is managed via MIM/LEAF applications. The software is TRM approved as well. Minimal information regarding patient information will be collected. VA guidelines regarding PII will be observed.

All VA personnel including employees, volunteers, and students must be trained, at least on privacy policies to include the requirements of Federal privacy and information laws, regulations, and VA policy. New personnel must be trained within 30 days of employment. All VA personnel are responsibility for compliance with VA's IT Security and Privacy Training and policies which extend to networked medical devices and must be done annually. VA personnel are aware of their HIPAA responsibilities and recognize proper and improper handling of PHI through the Privacy Training. The patient medical records are covered under the SORN of Patient Medical Records – VA SORN (24VA10A7), October 2, 2020, 2020-21426.pdf (govinfo.gov)

2.4c Does access require manager approval?

The designees of the ARANZ PM will be controlling access and safeguarding of PII.

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

Access to ARANZ is monitored, tracked, and recorded through audit logging at system, network, and application level. Explicit access for business purpose to PII is tracked and monitored through access control logs and remote access session approvals.

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

ARANZ System Owner is responsible for assuring safeguards are in place to protect PII.

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 by the system are patient name (Last, First, Middle), Date of Birth, EDIPI, Birth Sex, Self-Identified Gender Identity and Images regarding the wound, wound location and other notes/charting are also stored. Cloud storage on Silhouette Server allows for archiving into the VAEC. The official wound assessment reports (PDF) are stored within Cerner Millennium for the sites that utilize Millennium. For the sites that do not engage with Cerner Millennium, it is a manual process and can vary by location.

3.2 How long is information retained?

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

Records are maintained and disposed of in accordance with the records disposition authority approved by the Archivist of the United States. The retention and disposal statements are pursuant to National Archives and Records Administration (NARA) General Records Schedule GRS 3.2 items 30 and 31. Records are maintained and disposed of after 7 years. NARA guidelines as stated in VA Record Control Schedule (RCS) 10-1 requires retention for 75 years. The data retention period has been approved by NARA and is processed according to the following links:

- Department of Veterans Affairs, Records Control Schedule (RCS) 10-1, January 2020, 6000.2 https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf
- Department of Veterans Affairs, Office of Information & Technology Record Control Schedule 005-1 (August 3, 2009) https://www.oprm.va.gov/docs/RCS005-1-OIT-8-21-09.pdf

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

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner. Please work with the system Privacy Officer and VA Records Officer to answer these questions.
This question is related to privacy control DM-2, Data Retention and Disposal.

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

ARANZ uses the approved VA Health NARA approved retention schedules:

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

ARANZ uses the approved VA Health NARA approved retention schedules:

- Records Control Schedule (RCS) 10-1, January 2020, Chapter Six – Healthcare Records, 6000.2 Electronic Health Record, (EHRS) https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf
- Department of Veterans Affairs, Office of Information & Technology Record Control Schedule 005-1 (August 3, 2009) https://www.oprm.va.gov/docs/RCS005-1-OIT-8-21-09.pdf

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.

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

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

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

ARANZ Wound Management System is not intended to be used for research and testing. Office of Information and Technology (OIT) documents and monitors individual information system security training activities including basic security awareness training and specific information system security training performed using Talent Management System (TMS). These requirement training are done annually per VA policy. VA Research investigators may use PII for VA Institutional Review Board (IRB) approved research.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

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

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

Follow the format below:

Privacy Risk: There is risk that the information maintained by ARANZSilhouette could be retained for longer than is necessary to fulfill the VA mission. Records held longer that required are at greater risk of being unintentionally released or 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 medical devices. Cloud storage on Silhouette Server allow for archiving into the VAEC. The official wound assessment reports (PDF reports) are stored within Cerner Millennium for the sites that utilize Cerner Millennium. For the sites that do not engage with Cerner Millennium, it is a manual process and can vary by location.

Safeguards or compensating controls that are in place are encryption of hard drives, physical security measures to secure medical devices, device sanitization, and awareness and training. None of the information is retained permanently in the medical devices or system on the local workstation. To further mitigate the risk, ARANZ adheres to the VA Records Control Schedule (RSC) 10-1 for each category or data it maintains. https://vaww.va.gov/vhapublications/rcs10/rcs10-1.pdf

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

NOTE: Question 3.9 (second table) on Privacy Threshold Analysis should be used to answer this question.

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Veterans Healthcare Administration (VHA)	To allow for clinical input and review of data collected using ARANZ	Name – Last, First, Middle, Date of Birth, EDIPI, Wound Images	Central VistA Imaging Exchange (CVIX) & Cerner CVIX integration Adaptor (CCIA)

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: Standard risk management for VAEC cloud data protection. PII/PHI is captured manually by VA Personnel from the patient through Cerner Millennium through Personal Identification Verification (PIV) protected access. Unintended exposure of patient PII to unauthorized programs or unauthorized users. Information is transmitted from Cerner Millennium to ARANZSillouette via ADT.

Mitigation: The principle of need-to-know is strictly adhered to by VA personnel. All paper reports are handled according to privacy training and responsibilities in maintaining confidentiality. Employees take the annually required Privacy and HIPAA Training, VA Privacy and Information Security Awareness, and Rules of Behavior Training provided through the TMS portal. In addition, safeguards implemented to ensure data is not shared with unapproved or incorrect organizations are disabling unused ports and restricting access. Business Associate Agreement (BAA) and background investigation are done on vendors who have remote access.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a

Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?

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

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
Oracle Health Corporation: Veteran Health Administration (VHA) – Unified Electronic Health Record (EHR)	To allow for clinical input and review of data collected using ARANZ	• Name – Last, First, Middle • EDIPI • Date of Birth • Birth Sex • Self-Identified Gender Identity	National ISA/ MOU – Cerner VA ISA/MOU – ID: E-2168	Group Encrypted Transport VPN - IPSec tunnel utilizing Joint Security Architecture (JSA) across MedCOI CVIX/CCIA
DoD Defense Health Agency: VHA – Unified EHR	To allow for clinical input and review of data collected using ARANZ	• Name – Last, First, Middle • EDIPI • Date of Birth • Birth Sex • Self-Identified Gender Identity	Interagency Agreement DOD DHA VA National MEDCOI ISA – ID 733	Group Encrypted Transport VPN - IPSec tunnel utilizing Joint Security Architecture (JSA) across MedCOI CVIX/CCIA

5.2 <u>PRIVACY IMPACT ASSESSMENT: External sharing and disclosure</u>

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: Sharing information externally may result in an increased risk of unintended exposure of patient PII to unauthorized programs or persons.

Mitigation: All external connections are approved via Inter-Service Agreements (ISA) and/or Memorandum of Understandings (MOU). This provides an additional level of trust between the Department and Oracle Health. Additionally, all external connections currently use a Group Encrypted Transport VPN - IPSec tunnel utilizing Joint Security Architecture (JSA) across the MedCOI and CVIX/CCIA.

Section 6. Notice

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

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an Appendix-A 6.1 on the last page of the document. Also provide notice given to individuals by the source system (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

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

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

Notice of Privacy Practice (NOPP) is provided to the Veterans at the time of enrollment on VA Form 10-10EZ - VA_Form_10-10EZ.pdf.
(https://www.oprm.va.gov/privacy/systems_of_records.aspx).
SORN 24VA10A7 / 85 FR 62406, "Patient Medical Records-VA"

NOPP: https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

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

A copy of the form can be found online at https://www.va.gov/find-forms/about-form-10-10ez/
About VA Form 10-10EZ | Veterans Affairs

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

Written consent is not required to take a photograph or record video or voice for treatment purposes. Photographs, video, voice recordings, digital images, and other non-written media images when obtained for treatment purposes must be placed in the health record and are subject to all the same privacy regulations for use and disclosure as the entire content of the patient's health record, accordance to VHA Handbook 1907.01, Authority: 38 U.S.C. 305, 5735(d). 5723(d), 5727(9); 44 U.S.C. 3102(1). The VA policy is not to disclose any personal information to third parties outside VA without their consent, except to facilitate the transaction, to act on Veteran's behalf at their request, or as authorized by law. Any questions or concerns regarding VA Privacy Policy can be made by contacting Privacy Service via email at privacyservice@va.gov or by mailing at Department of Veterans Affairs, Privacy Service, 810 Vermont Avenue, N.W. (005R1A) Washington, DC 20420. The VA Privacy Service administers its programs are based on the Privacy Act of 1974. The patient medical records are covered under the SORN of Patient Medical Records – VA SORN (24VA10A7), October 2, 2020, https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress

.
Yes, all patients have the opportunity and right to decline treatment and/or right to provide information at any point. Individuals who decline will not be provided wound assessment treatment.

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.

Patients have the right to consent to wound imaging. If patient is unable to consent due to medical condition wound imaging can be completed based on need for treatment.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

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

Privacy Risk: Risk that Veterans will not know that medical devices/systems exist or that if they collect, maintain and or disseminate PII.

Mitigation: The information collected is from the System of Records for Patient Medical record 24VA10A7, October 2,2020 at the local facility's Cerner Millennium EHR. This PIA will be posted online for the public to view. Patients and families are educated on the process of medical devices/systems when they are being treated for care. All information collected comes from Cerner Millennium EHR by manual entry of the information or from the Veterans. NOPP are discussed at the individual Cerner Millennium EHR sites and documented in their respective PIAs.

Section 7. Access, Redress, and Correction

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

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

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

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

Access to the ARANZ cloud is limited to clinicians and Information Technology personnel. Patients do not have access to the information in the medical devices/systems as it is for clinical use only. Veterans could request information on their wound assessment treatment through Release of Information (ROI) offices at facilities to assist Veterans with obtaining access to their health records and other records containing personal information.

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)?

ARANZ is NOT exempt from access provisions of 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?

ARANZ is a Privacy Act system. The VHA established MyHealtheVet (MHV) program to provide Veterans remote access to their health records. The Veterans must enroll in MHV to obtain access to all the available features. In addition, Directive 1605.01 Privacy and Release of Information establishes procedures for Veterans to have their records amended when appropriate.

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

Inaccurate or erroneous information can be corrected within the ARANZ SilhouetteCentral application. The users would not have direct access to the medical devices/systems information to allow for corrections, Any information would be within the Cerner Millennium EHR for the sites that utilize Cerner Millennium EHR, and the sites that do, don't utilize Cerner Millennium EHR in the same way, therefore, veterans must contact local Facility Telehealth Coordinator (FTC) or reach out to national ARANZ Wound Management System Subject Matter Experts (SMEs). Information can be modified to align with what is correct.

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 ROI at facilities to assist Veterans with obtaining access to their health records and other records containing personal information. In addition, Directive 1605.01 Privacy and ROI establishes procedures for Veterans to have their records amended when appropriate.

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.

The Veteran would utilize the procedures in the NOPP, which every patient receives when they enroll for care. The users would not have direct access to the medical devices/systems information to allow for corrections. Any information would be within the Cerner Millennium EHR for the sites that utilize Cerner Millennium EHR and the sites that do, don't utilize Cerner Millennium EHR in the same way, therefore, veterans must contact a local FTC or reach out to national 3D wound imaging SMEs. VHA staff distributes a ROI at facilities to assist Veterans with obtaining access to their health records and other records containing personal information. In addition, Directive 1605.01 Privacy and ROI establishes procedures for Veterans to have their records amended when appropriate.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that Veterans 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 a ROI at facilities to assist Veterans with obtaining access to their health records and other records containing personal information. In addition, Directive 1605.01 Privacy and ROI establishes procedures for Veterans to have their records amended when appropriate. The VHA established 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.

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

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

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

Completing the annual VA Privacy and Information Security Awareness training, and HIPAA Privacy Training. Supervisor/manager or Contracting Officer Representative (COR) will document and monitor individual specific information system security and training activities. This documentation and monitoring are performed using the TMS. Access to the software is granted to VA employees and contractors for the application after the supervisor/COR authorizes this access once requirements have been met. All application users must have at least a Public-level clearance plus a Personal Identification Verification (PIV) card for multifactor authentication.

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?

PII is NOT shared with 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.

Roles and responsibilities are managed by Active Directory groups.

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

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access *to the PII. This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

Contracts are reviewed based on the timeline established in the specific contract and may vary slightly from one contract to another. When reviewed, they are reviewed by the appropriate contract authority (i.e., COR, Contracting Officer). ARANZ vendors could have remote access to the system, for which there is a national VPN agreement as well as a business agreement with the vendor. Contractors (vendors, nursing staff, etc) can have access to the system only after completing mandatory information security and privacy training, VHA HIPAA training as well as appropriate background investigation to include fingerprinting. Certification that this training has been completed by the contractors must be provided to the VHA COR. Vendor access is for maintenance activities, support and upgrades until this product is no longer needed by the VA. In addition, a BAA which includes the mandatory nature of the training and the potential penalties for violating patient privacy. The VA established ARANZ Wound Management System with the vendor under contract # V17-01041-001.

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 who have access to VA computers must complete the onboarding and annual mandatory privacy and information security training. In addition, all employees who have access to PHI must complete the VHA mandated Privacy and HIPAA Focused training. Finally, all new employees receive face-to-face training by the facility Privacy Officer (PO) and Information System Security Officer (ISSO) during new employee orientation. The PO and ISSO also perform subject specific trainings on an as needed basis.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 14 Dec 2023
3. *The Authorization Status:* Authorized to Operate (ATO)
4. *The Authorization Date:* 30 June 2022
5. *The Authorization Termination Date:* 29 June 2025
6. *The Risk Review Completion Date:* 06 June 2022
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

8.4b If No or In Process, provide your ***Initial Operating Capability (IOC) date.***
System has been in Production – see information in 8.4a.

Section 9 – Technology Usage

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

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

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

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

The system uses the VA Enterprise Cloud (VAEC) Azure Cloud, Infrastructure as a Service (IaaS).

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

N/A

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.

VA owns all data.

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.

N/A

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).

N/A

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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

Signature of Responsible Officials

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

DENNIS LAHL Digitally signed by DENNIS LAHL
Date: 2024.06.17 08:56:39 -04'00'

Privacy Officer, Dennis Lahl

OLIVER PATAGUE Digitally signed by OLIVER PATAGUE
Date: 2024.06.13 13:55:06 -07'00'

Information System Security Officer, Oliver Patague

HARPREET SODHI Digitally signed by HARPREET SODHI
Date: 2024.06.17 10:40:35 -04'00'

Information System Owner, Harpreet Sodhi

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).

System of Records Notice

1. VA SORN (24VA10A7 (previously 24VA10P2)): Patient Medical Records – VA
   a. Effective Date: 08/14/2014
   b. Link to Printed Version: https://www.gpo.gov/fdsys/pkg/FR-2014-08-14/pdf/2014-19283.pdf

2. VHA Handbook 1605.4 Notice of Privacy Practices, September 6, 2015.
   https://www.va.gov/vhapublications/publications.cfm?pub=2&order=desc&orderby=pub_Number

HELPFUL LINKS:

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

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

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

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

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