Privacy Impact Assessment for the VA IT System called:

3D Wound Care Management Solution Assessing

Veterans Health Administration

National Office for Telehealth, Asynchronous Telehealth

eMASS ID: 665

Date PIA submitted for review:

March 28, 2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Allan Castellanos	Allan.Castellanos@va.gov	858-642-3941
Information System Security Officer (ISSO)	Amine Messaoudi	Amine.Messaoudi@va.gov	202-815-9345
Information System Owner	Tony Sines	Tony.Sines@va.gov	316-249-8510

Abstract

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

3D Wound Care Management Solution Assessing is a software solution provided by the vendor Parable Health, comprised of a hand-held USB scanning device, a mobile app (running on iPads / iPhones) and a web app that allows clinicians to better measure, monitor, and manage their wound care population. 3D Wound Care Management Solution Assessing enables the capture, via either the scanner or VA mobile devices, of 2D images and 3D scans of wounds, as well as clinical assessment data. After data is captured, it is transmitted to the web service running in VAEC AWS, at which point it may be assessed from other iPads / iPhones running the 3D Wound Care Management Solution Assessing app or on the web using the 3D Wound Care Management Solution Assessing web app. Data is also sent to Veterans Information Systems and Technology Architecture (VistA), VistA Imaging (VIX) and Centralized VistA Imaging Exchange (CVIX) and, subsequently for Cerner patients, to the Cerner CVIX Integration Adaptor (CCIA) which ultimately transmits data to Cerner systems. Data is sent regularly from the 3D Wound Care Management Solution Assessing web service to CVIX + CCIA (images + assessment data) whenever new data is received from the mobile applications. Patient demographic data (name, dob, sex, ICN, consult info, site/VISN info, and last 4 digits of SSN) is regularly transmitted and fetched from CVIX by the web service whenever users initially register new VistA patients in the application for the first time to allow patient selection in the app and consequently linkage of wound assessment data collected with the corresponding patient record. The web service (REST API) also receives HL7 ORM and ADT (discharge and transfer only) messages from Cerner via CCIA over HTTPS, which is how Cerner patients from sites using the application are added to the 3D Wound Care Management Solution Assessing system and archived after discharge or transfer.

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 system name is 3D Wound Care Management Solution Assessing and is owned by the National Office for Teleheatlh; Asynchronous Telehealth

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 business purpose of 3D Wound Care Management System is to enhance wound management within the VA by enabling clinicians to more consistently and accurately measure and document wounds, collaboratively monitor healing progress with other care team

members, standardize treatment protocols and better prioritize wound care patients on a population level through an analytical dashboard and proactive alerts. 3D Wound Care Management System for Ambulatory Follow-Up also enables post-surgical monitoring to happen remotely on mobile devices, in veterans' own homes and on their own schedules. This supports the mission of facilitating access to care and improving the health of veterans

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

The system is hosted in the VAEC but the vendor owns the systems

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 whose information is stored in the system depends on how many sites/facilities this technology is deployed to and how many patients within each facility are managed with this. The potential total would be all veterans with some sort of acute or chronic wound. Given the 8.9 million veterans served by 1,233 health care facilities (including the 168 VA Medical Centers) and 1,053 outpatient sites within the VA, and assuming 5-10% of veterans served experience some form of acute or chronic wound, we can estimate 450,000-900,000 records stored in the system. The typical affected individual, in terms of data stored within the system, is a veteran experiencing a chronic or acute wound which would commonly include pressure injuries (bed sores) typical of Spinal Cord Injury (SCI) patients. Patient's can expect to have the following pieces of data associated with their record: patient name, sex, date of birth, patient Integrated Control Number (ICN), medical record number (MRN),Electronic Data Interchange Personal Identifier (EDIPI), Internal Patient ID (IPI), prior patient ID internal, prior patient account number, last 4 digits of Social Security Number (SSN), consult information, wound information (wound type, anatomical location, clinical assessment information, photographs, order control, placer order number, date of transaction, universal service ID, event type code, event date/time, event reason code), patient visit fields (patient class, patient location, patient type, admit date/time, discharge date/time), 3D scans. VA employee users of the system can expect the following data to be associated with them while using the system: name, email, Identity and Access Management (IAM) SecID, IAM VAUID, Active Directory (AD) Domain (VISN), site number, IP address, application event information, operator ID, event facility.

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

The system stores patient demographic information (e.g. patient name, medical record number), medical images, assessment information (e.g. wound type, location, measurements), and clinical notes and communications. Other than the demographic information, which is retrieved from VistA, all of the other clinical information is information generated / originating from the system itself.

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

Information is shared within the various components of the system, as well as with VistA. Below is a breakdown of the various components, their connections, and a description of each.

3D Wound Care Management Solution Assessing Web Service

- Connections
  - 3D Wound Care Management Solution Assessing Mobile Apps

- 3D Wound Care Management Solution Assessing Web Apps
- VA IAM SSOi SAML interface (indirect)

The 3D Wound Care Management Solution Assessing Web Service functions to provide a backend for 3D Wound Care Management Solution Assessing Mobile Apps (running on VA GFE iPads) and Web Apps (running in browsers). The Web Service runs in the VAEC AWS and is a collection of AWS services and 3D Wound Care Management Solution Assessing software. It stores data collected using the 3D Wound Care Management Solution Assessing Mobile App, transmits data to the mobile app, renders data to both the Mobile App and Web App for analysis, and transmits data to VistA and VistA Imaging through the CVIX interface.

The 3D Wound Care Management Solution Assessing Web Service also integrates with the VA IAM SSOi system via a SAML interface to facilitate authentication using standard VA 2fa (two factor authentication such as PIV). This interface is an indirect integration, meaning 3D Wound Care Management Solution Assessing Web Service does not communicate directly with VA IAM SSOi and instead relies on the SAML protocol whereby the client's browser is redirected to VA IAM SSOi system, performs authentication on that system, and is then redirected back to the Web Service and relays authentication information from VA IAM SSOi in the process of this redirection. This indirect interface is used for authentication on both the web and mobile applications.

3D Wound Care Management Solution Assessing Mobile App

- Connections
  - 3D Wound Care Management Solution Assessing Web Service
  - VA IAM SSOi SAML interface

The 3D Wound Care Management Solution Assessing Mobile App is a native iOS app that allows clinicians to capture 3D scans and photos of wound/lesions, perform measurements, record clinical assessments, and view previous assessments. The Mobile App stores data locally (with encryption) and transmits data to the 3D Wound Care Management Solution Assessing Web Service (with encryption) for long term storage, rendering, and subsequent transmission to VistA and VistA imaging. The Mobile App also downloads assessment data from the 3D Wound Care Management Solution Assessing Web Service for display. The Mobile App authenticates users via the VA IAM SSOi SAML interface as described in the 3D Wound Care Management Solution Assessing Web Service section.

3D Wound Care Management Solution Assessing Web App

- Connections
  - 3D Wound Care Management Solution Assessing Web Service
  - VA IAM SSOi SAML interface

The 3D Wound Care Management Solution Assessing Web App is an HTML and Javascript application loaded from the 3D Wound Care Management Solution Assessing Web Service and run in web browsers. It functions primarily as an interface to view and analyze data collected using the 3D Wound Care Management Solution Assessing Mobile App, including 3D wound scans/images, measurements, and clinical assessments. It also provides aggregate analytical and reporting tools to

segment and examine patient wound data. 3D Wound Care Management Solution Assessing Web App authenticates users via the VA IAM SSOi SAML interface as described in the Parable Web Service section.

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?

At the moment, 3D Wound Care Management Solution Assessing is deployed in the following VA sites: San Diego, Tucson, Phoenix, Prescott, Las Vegas, Loma Linda, Long Beach, Tomah, Reno, St Louis, and Kansas City with additional facilities set to be onboarded soon. Due to the 3D Wound Care Management Solution Assessing secure cloud infrastructure within the VAEC, PII is securely maintained and managed across all sites with the same controls. For the 3D Wound Care Management Solution Assessing web application, no data persists locally. Upon a terminal receiving data it is processed, stored in persistent database or file storage, and then removed from the application server. All data is encrypted prior to storage in the database using 256-bit AES encryption. For the mobile application, data stored locally on the mobile device is encrypted with 256-bit AES encryption. The encryption key is not stored locally and only retrieved upon login. Login attempts are rate-limited and six (6) consecutive unsuccessful login attempts temporarily locks the user for one (1) hour.

3. Legal Authority and SORN

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

3D Wound Care Management received Authority To Operate (ATO) in July 2019 which covers all components of the system and its interactions with external information systems such as VistA. The ATO has been re-approved and extended every 6 – 12 months since then, most recently in August 2023 for a 3 year ATO.VA SORN: 79VA10; Veterans Health Information Systems and Technology Architecture (VistA) Records - VA

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

No, the SORN will not require amendment or revision. Yes the SORN covers the use of cloud systems and storage, specifically VA Enterprise Cloud hosted applications.

4. System Changes

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

No it will not

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

No it will not

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: Electronic Data Interchange Personal Identifier (EDIPI) or Internal Patient ID (IPI) (rare), consult information, Site/VISN information, wound information (type, anatomical location, assessment information, photographs, 3D scans, Order Control, Placer Order Number, Date of Transaction, Universal Service ID, Event Type Code, Event Date/Time, Event

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

Reason Code, Operator ID, Event Facility, Prior Patient ID Internal, Prior Patient Account Number), Email, IAM SecID, IAM VAUID, AD Domain (VISN), Site Number, Patient Visit Fields (Patient Class, Patient Location, Patient Type, Admit Date/Time, Discharge Date/Time)

PII Mapping of Components (Servers/Database)

3D Wound Care Management Solution Assessing consists of 3 key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by 3D Wound Care Management Solution Assessing 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**
Web Service	Yes	Yes	Name, DOB, IP, partial SSN, Medical Record Number (MRN), images in some cases, SAML SSOi SecID	Enabling patient navigation and selection in the platform, storage + transmission to other components, single sign on, and maintaining audit trail	Encryption at rest and in transit, authentication, authorization, system hardening, network isolation, standard operating procedures, physical security protections (managed by AWS).
Mobile Application	Yes	Yes	Name, DOB, partial SSN, IP, MRN, images	Collecting and rendering clinical assessment data, identifying patient to	Encryption at rest and in transit, authentication, authorization, containerization, system

			in some cases	clinician, and maintaining audit trail	hardening, standard operating procedures
Web Application	Yes	No	Name, DOB, partial SSN, IP, MRN, images in some cases	Collecting and rendering clinical assessment data, identifying patient to clinician, and maintaining audit trail	Encryption at rest and in transit, authentication, authorization, system hardening, network isolation, standard operating procedures, physical security protections (managed by AWS).

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?

Veteran (patient) demographic information listed above are retrieved from VistA via CVIX and from DHA via CCIA

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.

3D Wound Care Management Solution Assessing mirrors the data gathered from VistA/CVIX/CCIA in order to identify the patient. This information is not gathered from the veteran as it already exists within VistA.

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

Scores and reports are generated by the system based on clinical assessment data and scoring systems selected and configured by the VA. The system is a source of information.

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?

Veteran (patient) demographic information such as name, DOB, sex, and MRN are retrieved from VistA electronically via CVIX or CCIA over an encrypted communication system within a private VA network.

Clinical assessment data such as wound images, 3D data ascertained from the images, and clinical assessment questionnaires are collected from the veteran by the clinician using the system (e.g. taking a photograph, answering a question). Clinicians use a native iOS mobile application running on VA iPads with an attachable 3D scanner to scan the wound (like taking a 3D photograph) and respond to several clinical assessment questions, also within the application.

VA employee information such as name, email, and SecID are transmitted to the 3D Wound Care Management Solution Assessing Web Service from the VA IAM SSOi SAML interface via the web or mobile applications through use of the SAML protocol.

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?

N/A, the information is retrieved from VistA electronically via CVIX or CCIA over an encrypted communication system within a private VA network.

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 checked for accuracy at the TCP packet level and information coming from Cerner through HL7 protocols through checksums. For patient demographic information that is constantly checked through every HL7 transaction for Cerner. For VistA records the latest records are polled against the stored record for accuracy at a given interval.

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?

N/A, no it does not check for accuracy against a commercial aggregator of information.

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
3D Wound Care Management has a VA ATO (Authority To Operate) which includes specific documents such as a BAA (Business Associates Agreement), and a general contract with the vendor outlining the data collected and stewardship of said data. Information collection is also covered by VistA SORN: https://www.govinfo.gov/content/pkg/FR-2000-11-24/pdf/00-29945.pdf - Veterans Health Information Systems and Technology Architecture (VistA) Records-VA (79VA10).

VA IAM SSOi SAML integration is governed by an SSOi integration agreement in place between Parable Health and the Department of Veterans Affairs.

VA CCIA integration is governed by an agreement in place between Cerner and the Department of Veterans Affairs.

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: Unauthorized access or disclosure of veteran personally identifiable information (PII) such as name or DOB.

Mitigation: PII collected is necessary in order to present an interface of identifiable veterans so clinical users can select a veteran to perform an assessment or review previous assessments – the primary purpose of the platform. Only the minimum necessary PII is collected to support this functionality (e.g. SSN is not collected as it is not necessary to uniquely identify a veteran). These data are not collected from veterans directly, but imported from VistA via CVIX, and DHA via CCIA, to ensure accuracy and integrity and to avoid unnecessary and potentially error-prone additional data collection.

Privacy Risk: Unauthorized access or disclosure of veteran protected health information (PHI) such as wound images or clinical assessment information.

Mitigation: PHI collected is necessary as this is the primary purpose of the platform – to collect and analyze wound/tissue information. Only the minimum necessary PHI is collected to support this functionality (e.g. drug allergies are not collected as this information is already available through VistA and not core to the wound assessment process). These data are collected from veterans directly through photography and clinical assessments conducted by clinicians.

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	Assists in uniquely identifying the veteran within the application	Not used
Date of Birth	Assists in uniquely identifying the veteran within the application	Not used
Partial SSN	Assists in uniquely identifying the veteran within the application	Not used
Medical Record Number	Assists in uniquely identifying the veteran within the application. Uniquely identifies the veteran record for electronic data transmission to/from VistA via CVIX (integration)	Not used

IP	Used as metadata in audit logging to enhance log fidelity	Not used
Wound Images + Clinical Assessment Data	Used to assess the state and trajectory of wound healing	Not used
VA Employee Name + Email + SecID	Facilitates single sign on and user identification throughout system usage	Not used

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?

The system analyzes wound scans to perform volumetric measurements through complex computer vision / spatial algorithms. Additionally, clinical assessment data are combined with measurement data to compute a total score for a wound. This score, the measurements, and the component clinical assessment data are compiled into a report which is stored in VistA (via CVIX) as a note that is associated with the relevant patient record and / or consult. These reports are accessible to, and used by, VA clinical staff to augment their clinical decision making

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.

These reports are accessible to, and used by, VA clinical staff to augment their clinical decision making.

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?
Data in transit is protected using HTTPS or HL7 over TLS. Data at rest is encrypted at the EBS volume, RDS, and S3 bucket level within AWS. The iOS file system is also encrypted for the mobile devices. Within the iOS file system, the application also encrypts the database and image files.

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

Full SSN are not used or collected. Partial SSN is used in assisting to identify the veteran patient

2.3c How is PII/PHI safeguarded in accordance with OMB Memorandum M-06-15?
3D Wound Care Management Solution Assessing utilizes AWS safeguards such as S3 Bucket level encryption and EBS volume encryption by default on all buckets and instances respectively. Data in transit is protected using HTTPS or HL7 over TLS to secure the traffic. In addition to technical safeguards, there are administrative safeguards to include policies in place to prevent the circumvention of least privilege, role based access controls, and need to know principles.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

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

2.4a How is access to the PII determined?
The facility telehealth coordinator (FTC) is delegated the role of managing access to PII. They, then, can pass that role to other users within their region or general scope of data access. If the FTC is not available the Office of Connected Care manages the access request for PII access.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented?
Yes, in the Parable 'Getting Started Guide'

2.4c Does access require manager approval?
Yes, anyone who has equal or greater access or oversight to the area requested can provision the access request

2.4d Is access to the PII being monitored, tracked, or recorded?
Yes, audit logs are available containing the required metadata to identify who, what, when, where, and how

2.4e Who is responsible for assuring safeguards for the PII?
The Facility Telehealth Coordinator (FTC) assures safeguards for the PII at the VA level and is touched on in specific HIPAA and other VA trainings.

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*

- Name
- Date of Birth
- IP Address
- Medical Record Number
- Wound Images
- IP Addresses
- VA employee name, email, and SecID

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.*

3D Wound Care Management Solution Assessing retains information in accordance with applicable record control guidelines:
Department of Veterans Affairs, Veteran Health Administration Record Control Schedule (RCS) 10-1.

6000.2: Interim Electronic Source Information (IESI) is retained with the following disposition: Temporary; destroy/delete after migration of information to another electronic medium. Destruction of interim version of information is not to occur until it has been determined that the migrated information represents an exact duplicate of the previous version of the migrated information. (N115-02-3, Item 2)

Acting as a business associate, 3D Wound Care Management Solution Assessing retains information temporarily, until it can be determined that the information migrated to VistA and VistA Imaging represents an exact duplicate of the pre-migrated information and the vendor no longer provides service to the VA.

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?

Yes

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

Records Retention Schedule: RCS 10-1, Series: 6000.2, Disposition Authority: N1-15-02-3, item 2; DAA-0015-2015-0005-0003 (rcs10-1.pdf (va.gov))

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.

All records are electronic in nature and elimination / destruction involves logical removal from the electronic storage medium. Destroy/delete after migration of information to another electronic medium. Destruction of interim version of information is not to occur until it has been determined that the migrated information represents an exact duplicate of the previous version of the migrated information per the records retention schedule. 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. When the storage medium is to be destroyed at the end of its use, physical destruction of underlying physical storage is handled by Amazon as covered by our BAA and detailed in their data destruction policies.

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.

PII is not used for testing, training, or research. To avoid the need to use PII or PHI for these purposes, we have developed test data generators, data cloners, and data redactors which enable the

creation of testing / research & development datasets that mimic the "shape" of real data without containing any PII or PHI.

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: Data retained by the system is at risk of unintended access, disclosure or breach.

Mitigation: Only the minimum PII necessary is retained, minimizing the magnitude of harm. Access controls are in place to limit access automatically and to as great a degree as possible. A suite a technical and process controls are in place to harden the platform and processes as much as possible without impacting business function.

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***
VistA (via CVIX)	Receive demographic info for veteran identification. Transmit clinical assessment information to store data collected in the system in the veteran's record within VistA.	Receive PII: name, DOB, sex, Integrated Control Number (ICN), MRN (patient IEN). Transmit PII: MRN/IEN and PHI: clinical assessment information, Site/VISN information	CVIX REST interface over authenticated + encrypted HTTPS (TCP 443)
VistA Imaging (via CVIX)	Transmit wound images collected by the system for storage within the veteran's VistA record.	Transmit wound image data in JPG and PDF formats as well as a identifiers indicating image attachment destination.	CVIX REST interface over authenticated + encrypted HTTPS (TCP 443)
DHA (via Cerner CVIX Integration Appliance (CCIA))	Receive demographic info for patient identification. Transmit clinical assessment information to store data collected in the system in the	Receive PII: name, DOB, sex, MRN (patient IEN). Transmit PII: IEN and PHI: clinical assessment information. Transmit wound image data in JPG and PDF formats as well as a identifiers indicating	CCIA interface over authenticated + encrypted HTTPS (TCP 443)

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*
	patient's record within GENESIS/MedCOI. Transmit wound images collected by the system for storage within the patient's GENISIS/MedCOI record.	image attachment destination, Site/VISN information	
iPad/iPhone GFE	Receive demographic info for veteran identification. Transmit clinical assessment information to store data collected in the system in the veteran's record within VistA. Also transmits the VA employee data to the system.	Employee name, Employee email, Employee IAM SecID, Employee IAM VA UID, Employee AD Domain (VISN), Clinical Trainee Name, Clinical Trainee Email, Clinical Trainee IAM SecID, Clinical Trainee IAM VA UID, Clinical Trainee AD Domain (VISN), Patient name, sex, DOB, IEN, EDIPI, IPI, partial (last 4) SSN, wound information, consult information, Site/VISN Information, Application Event Information	HTTPS via TCP 443 The Parable application running on iPads / iPhones connects to the backend Parable web service through the VAEC over HTTPS on TCP 443. It also connects directly to VA IAM during the SAML SSOi authentication process over HTTPS on TCP 443.
Identity and Access Management (IAM) Single Sign On Internal (SSOi)	Authenticate the user of the application	Employee name, Employee email, Employee IAM SecID, Employee IAM VA UID, Employee AD Domain (VISN), Clinical Trainee Name, Clinical Trainee Email, Clinical Trainee IAM SecID, Clinical Trainee IAM VA UID, Clinical Trainee AD Domain (VISN)	HTTPS via TCP 443 Transmission occurs via SAML protocol and is mediated by the user's browser, meaning the Parable web

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*
			service does not connect directly to VHA IAM, but rather the user's browser (on iOS or computer) connects to Parable and IAM and relays data between them via redirects (i.e. the SAML protocol)

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: The automated data sharing between the system and VistA and VistA imaging (via CVIX) could potentially be intercepted by a man-in-the-middle style network attacks.

Mitigation: CVIX authentication relies on pre-shared cryptographic certificates which enables public-key validation of private key signatures and mitigates man-in-the-middle attacks. Successful authentication establishes a secure, encrypted, private communication channel between Parable systems and CVIX.

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***
Cerner, Defense Health Agency	Core functionality of the system. This web service provides central coordination for mobile	<u>Patient Identification Fields:</u> Patient name, sex, DOB, ICN, EDIPI, IPI, MRN, Account Number (Cerner Financial Number), Account Number Assigning Authority and Type <u>Patient Visit Fields:</u> Patient Class, Patient Location (point of service location, patient room,	National MOU/ISA, BAA, ATO, SSOi integration agreement	End-to-end HTTPS (TLS/SSL) in-transit encryption Public-key cryptographic validation of remote party to

	apps, CVIX integration appliance, and web applications.	patient bed, facility ID), patient type, admit date/time, discharge date/time <u>Order Control Fields (ORM messages):</u> Order Control, Placer Order Number (Unique Placer ID, Placer Application ID), Date of Transaction <u>Observation Request Fields:</u> Placer Order Number, Universal Service ID <u>Event Type Fields (ADT messages):</u> Event Type Code, Date/Time of Event, Event Reason Code, Operator ID, Event Facility <u>ADT Merge Information Fields:</u> Prior patient ID Internal, Prior Patient Account Number		prevent man-in-the-middle attacks. Pre-shared credentials to establish cryptographic sessions and sign data transmissions

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:

<u>Privacy Risk:</u> The sharing of data with a vendor outside the VA creates a potential for data interception during transmission to/from the vendor.

<u>Mitigation</u>: Data sharing between the VA and vendor takes place only over cryptographically authenticated sessions with end-to-end TLS encryption to protect data in transit and ensure it is impossible to intercept. Additionally, to prevent a man in the middle attack, public key cryptography

and pre-shared certificates are used to validate the other party is who they say they are, and both sides know they are talking to the correct party and not a would-be thief/imposter.

Privacy Risk: The VA must evaluate the security and privacy posture of the vendor and ensure the vendor has appropriate security and privacy controls in place.

Mitigation: The vendor has undergone extensive validation of security and privacy controls and has received an ATO granting the vendor authority to operate the system and manage the data. The ATO has been reviewed and extended several times. Additionally, there is an MOU/ISA, a BAA, an SSOi integration agreement, and a contract in place governing the data exchange, data stewardship, roles and responsibilities, and liabilities.

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.

The system does not collect PII from users directly, nor does it result in the collection of additional PII that would not otherwise be collected. All the PII is imported from VistA via CVIX.

In terms of PHI, this is also data that was already being collected previously, this system simply provides a more robust and efficient collection + analysis mechanism. As a result, the system has not introduced any new privacy / consent notices compared to those already in place.

Information collection is covered by VistA SORN: https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf - Veterans

6.1b If notice was not provided, explain why. If it was provided, attach a copy of the current notice.
N/A, the system does not collect PII from users directly, nor does it result in the collection of additional PII that would not otherwise be collected.

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.

N/A, the system does not collect PII from users directly, nor does it result in the collection of additional PII that would not otherwise be collected.

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

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

Yes, individuals have the opportunity and right to decline photographic wound assessments without a penalty or denial of service attached

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

This question is directed at whether an individual may provide consent for specific uses, or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent

.

No, consent covers all uses and there is not currently an ability to control consent at a more granular level.

6.4 <u>PRIVACY IMPACT ASSESSMENT: Notice</u>

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:

<u>Principle of Transparency:</u> Has sufficient notice been provided to the individual?

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

<u>Privacy Risk:</u> Without providing sufficient notice, the patient may not understand whether or not PII is being collected and what its intended uses are.

<u>Mitigation:</u> PII in the 3D Wound Care Management Solution system is a read only mirror of the information stored in VistA, the system source of truth, which provides notice as per the SORN.

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.***

No PII is collected directly from the individual by the system. The only PII in the system is imported from VistA and used solely for identification of veteran records by clinical staff. Because the information is a mirror of information maintained in VistA, there are no procedures in place to allow individuals to gain access to their PII held in the system and instead they may gain access to this information within the canonical source / final destination: VistA.

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

The system does not collect PII from the individual, it is a mirror of the information found in VistA. In order to access, redress, or correct information the individual would need to contact the system source of truth, in this case VistA.

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

The system does not collect PII from the individual, it is a mirror of the information found in VistA. In order to access, redress, or correct information the individual would need to contact the system source of truth, in this case VistA.

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.

PII is only imported from IAM (users) or VistA (patients). PII is regularly updated from IAM or VistA on an hourly basis so any changes will be reflected in the system within an hour. There is no

ability to modify PII within the system as it is a read-only mirror of the data managed by IAM or VistA

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.

N/A – No PII is collected directly from the individual and PII within the system is a read-only mirror of the minimum VistA data necessary to identify the veteran.

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.

N/A – No PII is collected directly from the individual and PII within the system is a read-only mirror of the minimum VistA data necessary to identify the veteran.

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.

Privacy Risk: The patient does not have the ability to directly access, correct, or attempt redress of the PII the system uses for identification.

Mitigation: No PII is collected directly from the individual and PII within the system is a read-only mirror of the minimum VistA data necessary to identify the veteran. The clinicians who use the system are trained in updating patient information in the system source of truth for the patient PII or directing the patient to the appropriate point of contact for access, correct, or redress.

Section 8. Technical Access and Security

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

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

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

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

Access to the system is currently determined at the discretion of the System Owner and/or their Delegates. Access to the system requires the approval of the System Owner and/or their Delegates. The access controls for a user are also determined by the System Owner, including the user's role and restrictions affecting the scope of veterans the user may access. In addition to management by the System Owner / Delegates, SAML integration with VA's Identity and Access Management (IAM) system and authenticates users using approved VA 2fa processes as well as preventing user access if their account is disabled or access revoked within the centralized VA IAM system. All of this is documented in Parable's compliance policies as well as the security controls documented in eMASS as part of the system's ATO.

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?

N/A, no other agencies will utilize the system deployed in the VA AWS tenant

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.

The available roles are:

- **Administrator** - Administrators are privileged accounts that can view and create patient, case, and assessment data, perform case-management operations which include moving and merging, and manage organizational settings including managing user access.
- **Standard** - Standard accounts are non-privileged accounts which can view and create patient, case, and assessment data.

- **Mobile Only** - Mobile Only accounts are non-privileged accounts which can view and create patient, case, and assessment data but are limited to the mobile application only and are not granted web application access.
- **Restricted** - Restricted accounts are non-privileged, read-only accounts which can view patient, case, and assessment data but cannot create new data.

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.

Some employees of the vendor, Parable Health, will have access to the system and the PII. The vendor is primarily responsible for the design and maintenance of the system. There is not an explicit NDA in place, however there is a BAA and MOU/ISA in place which both cover disclosure of protected information. Employees of the vendor Parable Health who have access to production systems and the PII therein are considered High Risk. High Risk employees are kept as limited as possible, and in addition to standard employee training and HIPAA training, they undergo standard background checks which include SSN trace, sex offender search, and national and international criminal watchlist checks.

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.

Because of the minimal and mirrored nature of the PII, there is no system-specific privacy training for VA users. The vendor, Parable Health, provides general Health Insurance Portability and Accountability Act (HIPAA) training to all employees with access to the system and/or PII as well as specific training on Parable's security and privacy controls and policies

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 7 June 2023
3. *The Authorization Status:* Authorized

4. *The Authorization Date:* 11 August 2023
5. *The Authorization Termination Date:* 10 August 2026
6. *The Risk Review Completion Date:* 1 August 2023
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.***

N/A

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)*

3D Wound Care Management Solution Assessing is hosted within the VAEC AWS GOVCLOUD HIGH and is an 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.

N/A

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**
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.

ALLAN CASTELLANOS

Digitally signed by ALLAN CASTELLANOS
Date: 2024.05.15 08:38:51 -07'00'

Privacy Officer, Allan Castellanos

AMINE MESSAOUDI

Digitally signed by AMINE MESSAOUDI
Date: 2024.05.20 06:17:21 -05'00'

Information System Security Officer, Amine Messaoudi

TONY SINES

Digitally signed by TONY SINES
Date: 2024.05.15 12:20:45 -05'00'

Information System Owner, Tony Sines

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).

HELPFUL LINKS:

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

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

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

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

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