Privacy Impact Assessment for the VA IT System called:

Venous Care Pathway Digital Health Platform (Venous-CPDHP)

Veterans Health Administration

National Center for Collaborative Healthcare Innovation (NCCHI), VHA Innovation Ecosystem (VHA IE), VA Palo Alto Healthcare System (VAPAHCS)

Date PIA submitted for review:

4/07/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Kimberly Murphy	Kimberly.Murphy@va.gov	(781)-331-3206
Information System Security Officer (ISSO)	Mark McGee	James.McGee5@va.gov	(520)-358-3237
Information System Owner	Sirish Kishore	Sirish.Kishore@va.gov	(314)-791-0290

Abstract

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

The Venous Care Pathway Digital Health Platform is composed of mobile health applications for veterans, care dashboards for VHA practitioners, and clinical and economic outcome dashboards for VA Palo Alto Healthcare System (VAPAHCS). The system will support the in-hospital implemented care pathway protocol by connecting veterans to their care teams, providing disease education materials, tracking health outcomes, integrating longitudinal clinical and economic data, and displaying outcomes of the venous care pathway compared to a retrospective standard of care control group. The digital health system and all Veteran PHI will be hosted on the VHA GovCloud servers.

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. The IT system name and the name of the program office that owns the IT system.

The IT system, Venous Care Pathway Digital Health Platform (Venous-CPDHP), is owned by Impact Health and program office ownership is not applicable.

B. 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 the care pathway improvement program and the IT system is to improve clinical outcomes for veterans, improve patient experience, reduce burden on health workers, and realize cost efficiencies for longitudinal Venous Disease management. The Office of Quality and Performance aligns directly to the program's goal of implementing and monitoring the results of an improved venous care management strategy and using the gathered medical research insights and factual information to positively impact patient outcomes.

C. Indicate the ownership or control of the IT system or project.

While the IT system is owned by Impact Health, the system will be deployed and operated from within the VA Enterprise Cloud environment. As such, the IT system will be owned by Impact Health but jointly controlled by the VA and Impact Health.

2. Information Collection and Sharing

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

The total number of individuals whose information is stored in the system depends on the final number of sites and facilities to which the technology is deployed. For the initial deployment within VAPAHCS, there will be an estimated 500-1000 total end users with records stored in the system. These users include Veteran (patient) users, VA healthcare professional (practitioner) users, and VA leadership users. The typical users include veteran patients with one or more included venous diseases (deep vein thrombosis (DVT), pulmonary embolism (PE), post-thrombotic syndrome (PTS), and venous leg ulceration (VLU)). The practitioner and leadership users will include members of the care team that provide healthcare services to veterans with venous disease and VA leadership that oversee the venous disease populations.

E. A general description of the information in the IT system and the purpose for collecting this information.

The information contained in the IT system will compose of patient demographic information (e.g., name, address, email, phone number, gender, date of birth, etc.) for patient identification and user system settings. Additionally, health information (e.g., medical history, health visit details, diagnostic and procedure history, clinical outcomes, images, treatment adherence reporting) will be collected to provide users with a longitudinal view of health encounters, care decisions made, and resulting patient outcomes. All information will be generated from the system itself through user data input.

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

Information is shared between the various components of the system – below is a breakdown of the components, their connections, and a description of each.

Components & Descriptions

- **Web Service**
  - The Web Service runs in AWS GovCloud and is a collection of AWS services and Impact Health software. It is hosted within the VA Enterprise Cloud and provides the backend necessary to facilitate data collection, storage, analysis, transmission, and display by the Mobile and Web Apps further described below.
  - Connections: Mobile App and all Web Apps
- **Mobile App – Veteran Patients**
  - An iOS and Android supported application allows veterans/patients to access a mobile-based app to view health tasks, log clinical metrics, track treatment compliance, view previous encounters, access educational content, contact their practitioners, and more. The mobile app stores encrypted data in a secure AWS GovCloud environment hosted by the VA.
  - Connections: Web Service
- **Web App – Administrator**

    - Administrators are able to assign roles to users created within the system and are responsible for managing organizational settings including user access.
    - Connections: Web Service
- **Web App – Practitioner**
    - Practitioner users will have access to web-based dashboards that allow them to oversee their patient populations with venous disease, providing information related to population and individual health status, progression along the care pathway, and prompts for next steps to maximize patient outcomes. The practitioner app stores encrypted data in a secure AWS GovCloud environment hosted by the VA.
    - Connections: Web Service
- **Web App – VA Leadership**
    - VA leadership users will have access to dashboards that provide summaries of venous population health and compare outcomes to historical quality benchmarks. The VA leadership web application stores encrypted data in a secure AWS GovCloud environment hosted by the VA.
    - Connections: Web Service
- **Web App – Wound Image Tracer**
    - Wound image tracers will have read-only access to images submitted by practitioner or patient users. The tracer is responsible for assisting in measurement of wound surface area for use by patients and practitioners.
    - Connections: Web Service

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

The system will be deployed to sites within the VA Palo Alto health system, with additional facilities within VA Palo Alto, VISN 21, and broader VA healthcare systems to be onboarded upon successful completion of the project. PII is securely maintained and managed across all sites with the same controls.

3. Legal Authority and SORN

H. A citation of the legal authority to operate the IT system.

The Venous Care Pathway Digital Health Platform is currently undergoing the eMASS process with the goal of receiving Authority to Operate (ATO) approval during the 2023 calendar year. No IT system is in production at the time of this document submission.

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?

N/A - A SORN is not needed for this system.

4. System Changes

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

Completion of this PIA will not result in circumstances that require changes to business processes.

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

Completion of this PIA will not result in circumstances that require technology changes.

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.

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*
- ☐ 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)

Profile photo, time zone, health visit details (e.g., ICD, CPT, date, location, practitioner, etc.), clinical outcomes (e.g., wound size, quality of life measures), unique identifiers for SSOI/SSOE single sign on process

PII Mapping of Components (Servers/Database)

The IT system does not connect, receive, or share PII with another internal VA organization, system, website, or application.

If the IT system is updated to connect, receive, or share PII with another internal VA organization, the PTA and PIA will be updated accordingly.

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

Internal Database Connections

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
N/A					

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 such as name, DOB, sex, identification numbers, and clinical data (images, visit history, PHI) are collected from the veteran by either direct input from the veteran a clinician using the system. Practitioner demographic information such as name and email address will be collected from VHA clinicians.
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.

Demographic information will be primarily used to identify users of the system so that additional collected data can be linked to the right individual. Clinical data is collected and analyzed to provide a longitudinal view of venous-related healthcare to the users on the web application in the form of dashboards and reports. Additionally, data collected will be used to provide protocol recommendations to practicing clinicians.

1.2c If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

VA employee information such as name, email, and identifiers needed for SSOI/SSOE are transmitted to the Web Service from the VA IAM SSOi system. This connection is not yet established. The Venous-CPDHP system will also create reports using user inputted data.

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?

Data will be collected directly through the system as veteran (patient) users and VA employees (practitioners) manually enter data. Data will additionally be created by the system based on analyses performed on manually collected information. There is currently no information being collected through other technologies.

1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form's OMB control number and the agency form number.

The information collected is not subject to the Paperwork Reduction Act

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 will be checked for accuracy by the patient and practitioner users during routine healthcare visits. Based on the nature of the data (personal medical records), the accuracy of the data will primarily be verified by these two users and will be done at scheduled health visits.

1.4b If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

N/A

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 Privacy Act of 1974, as amended, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. The authority of maintenance of the system listed in question 1.1 falls under 45 CFR § 164.502 (3) and 45 CFR § 164.510

Venous Care Pathway Digital Health Platform is in the process of completing necessary documentation to receive VA Authority to Operate (ATO). Users of the platform will provide informed consent of data collection and uses of data upon first log-in to the platform.

1.6 <u>PRIVACY IMPACT ASSESSMENT: Characterization of the information</u>

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:

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

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

<u>Principle of Individual Participation:</u> 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 user (veteran, practitioner) personally identifiable information (PII) such as name or DOB. Additionally, a risk of unauthorized access or disclosure of patient (veteran) protected health information (PHI), such as medical history, healthcare visits, wound images, reported symptoms, and treatments received.

Mitigation: PII collected is necessary in order to ensure that users can log into their own profile and interact with components containing their, or their patient's, information. Additionally, practitioners must be able to view a list of veterans under their care and be able to view data, enter data, and perform assessments relevant to providing high quality care for venous disease – 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 will be manually collected from veterans and reviewed by practitioners to ensure the information is accurate and up to date. Additionally, for patients (veterans), the PHI collected is necessary as this supports the primary function of the platform – to integrate and display health-related information to practitioners and patients to guide best practice decision making and ensure all veterans receive the best possible care. These data are collected from veterans directly via the mobile application and are directly inputted by practitioners via the web application.

Section 2. Uses of the Information

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

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

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

- *Name* – for unique identification of veterans using the application
- *Address* – for unique identification of veterans using the application and for contact with clinical outcome tracking
- *IP Address* – used during audit logging
- *Email* – for unique identification of veterans using the application, for veteran logging into the system, and for contact with clinical outcome tracking
- *Phone Number* – for unique identification of veterans using the application, for veteran logging into the system, and for contact with clinical outcome tracking
- *DOB* – for unique identification of veterans using the application

- *Race/ethnicity* – provides context for the patient health journey and ability to provision personalized medicine based on elevated risk factors in target populations
- *Medical Record Number* – Used for unique identification of veterans using the application and potential linkage of information to their VHA health record
- *PHI* – Medical history, health visit details, clinical outcomes, treatment adherence – used to assess the clinical state, determine management recommendations to practitioners, and provide quality of care reports for the participating healthcare systems
- *Profile photo (optional)* – for display on web applications for veterans and clinicians
- *VA employee name, email, unique identifiers for SSOI/SSOE* – will be used to facilitate single-sign-on and user identification throughout system usage
- *SSOI/SSOE Identifiers* – will be used to facilitate single-sign-on and user identification throughout system usage
- *Medical Records* – see "PHI" above
- *Health Visit Details* - see "PHI" above
- *Clinical Outcomes* - see "PHI" above
- *Medications* - Used to determine management recommendations to practitioners and assess patient clinical adherence
- *Gender* – Used in the patient digital health solution profile to provide clinical context for patient management
- *Time Zone* – used during audit logging and for maintenance of digital health solution user account functionality such as time-based task assignments

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 collects and aggregates patient medical information to provide a longitudinal view of venous disease related healthcare and provide protocol recommendations to practicing clinicians. Additional data will be generated by the system (wound images, wound measurement, quality of life questionnaires, symptom tracking, treatment adherence tracking, etc.) and will compiled into reports to be accessible to users via the web-based portal. Data may also be exported in the form of PDFs from the system and attached to existing EHR records, if requested. These reports will additionally be used to inform VA Palo Alto Healthcare System on key outcomes (clinical, economic) that they are achieving related to management of their venous disease population.

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.

Newly derived information will be placed in the individual's record in the Impact Health Digital Health Solutions. Information created via the Digital Health Solutions will be provided and accessible to VHA employees through a combination of database access (i.e., access to production databases), PDF report generation, EHR integration (of documents and individual elements) of clinical fields, and practitioner user access to the Digital Health Solution interfaces, which they will use while providing routine clinical care. The information collected will consist of data including patient clinical progression, clinical outcome tracking, adherence to medications, and other clinical data to inform provisioning of high-quality clinical care by practitioners.

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 and at rest will be encrypted. SSL/TLS protocol version to use is TLS 1.2.

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

The system does not collect Social Security Numbers

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

All PHI and PII will be stored within the VA Enterprise cloud and adherent to VA security protocols, including data encryption. All database data shall be encrypted with industry standard AES-256 encryption algorithm.

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. ***<u>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.</u>***

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?

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?

Access to PII is determined based on user credentials and access controls and is automatically enforced. Users granted access to the system and the access controls they are granted is currently determined by the System Owner and/or their Delegates. Access to the system requires the approval of the System Owner and/or their Delegates, who in this capacity function as managers whose approval is required to access PII. All users receive onboarding training conducted by the Privacy Officer, System Owner, or Delegates which covers access and usage of data within the system. Violations may result in access being revoked at which point automated systems will prevent further access to PII and PHI. Violations may also result in disciplinary action consistent with the nature of the offense.

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

Yes

2.4c Does access require manager approval?

Yes, access to PII requires manager approval. Access to PII as a software developer requires approval from the System Owner, and access to PII as a user (practitioner) requires account provisioning by the Web App Administrator who is assigned by the System Owner.

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

All access to PII and PHI is monitored, tracked, and recorded in the form of audit logs of all CRUD actions (Create, Remove, Update, Delete). Audit log anomalies are regularly reviewed by the System Owner, Delegates, and/or Privacy Officer.

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

The primary parties responsible for assuring safeguards for PII are the VHA, Impact Health, and Digital Health Solution Users. As the system is stored in the VA Enterprise Cloud, the VHA is responsible for security controls for this cloud environment. Additionally, a representative from the VHA will be assigned the role of Web App Administrator and will assign user accounts with access to patient PII/PHI to qualifying practitioners. Impact Health, as the developer and maintainer of the Digital Health Solution software is similarly responsible for assuring safeguards for the PII and does so by following best security practices like encryption of data in rest and in transit. Lastly, the users themselves (patients and practitioners) are responsible for safeguarding their username and password information to ensure that a separate entity does not access their account.

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, profile photo, home address, email, phone number, gender, date of birth, full medical history, medical records, medications, health visit details (e.g., ICT, CPT, date, location, practitioner, etc.), Clinical outcomes (e.g., wound size, quality of life measures), treatment adherence (e.g., compression stockings, pharmaceuticals), medical record number, race/ethnicity, IP address, time zone, VA employee name, email, and unique identifiers needed for SSOI/SSOE

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.*

All information is used to support functioning of the system within the VA Enterprise Cloud (VAEC) and will be retained in accordance with the VA's record control guidelines. The information will be retained for the duration of the project (anticipated ~3+ years) at a minimum. Data will be retained to ensure that patients and practitioners have access to captured health data, dashboards, and analytic tools to provide best-in-class healthcare services.

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?

The retention schedule has not yet been approved by the VA records office.

3.3b Please indicate each records retention schedule, series, and disposition authority.
The retention schedule has not yet been approved by the VA records office.

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. 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. 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. The VA is the primary data controller and as such is responsible for elimination of SPI.

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 and PHI for these purposes, we utilize a deidentification process designed in accordance with the HIPAA Privacy Rule to minimize risk of patient re-identification.

3.6 <u>PRIVACY IMPACT ASSESSMENT: Retention of information</u>

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 is retained by the system for at least 3 years, during which it 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 to as great a degree as possible. A suite of technical and process controls are in place to harden the platform and processes as much as possible without impacting business function. These controls will be in place for the entire duration that data is retained in the system.

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***
N/A		N/A	N/A

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: N/A

Mitigation: N/A

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***
N/A				

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

Discuss the privacy risks associated with the sharing of information outside the Department and what steps, if any, are currently being taken to mitigate those identified risks.

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum Of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.
Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.
This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

Privacy Risk: N/A

Mitigation: N/A

Section 6. Notice

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

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an Appendix-A 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.

Yes the patients are provided with a notice of collection of information as part of the sign-up flow on the Digital Health Solutions. See Appendix A-6.1 for more information.

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

A notice is provided.

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.

Yes, notices (see Appendix A-6.1) are provided to the individual when they use the mobile health application for the first time. They guides the Veteran (patient) through a series of screens that describe the application purpose, data being gathered, privacy of data collected, intended uses of data, withdrawal of data, and obtains user consent.

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, patients have the opportunity to decline to provide information during the introduction screens (see appendix). If patients decline to provide information, they will be unable to create an account and use the mobile application. The care that they receive from health facilities should remain unchanged, but the quality of health outcome tracking and coordination with care teams will likely suffer. No further penalty or denial of service is 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.

The patient's identifiable information is only used to create and maintain an account for them to access via a mobile application. Further specific consent is not required.

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?

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: Insufficient notice of related to capture and use of information may result in patient data being inappropriately accessed or used in a manner not approved by patients.

Mitigation: Patients are notified of the data that is collected and the intended uses of such data, in layman's terms. They are additionally notified of their rights to decline to provide information, cease using the digital applications, and request for revision/deletion of information.

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.***

Individuals will have access to their information by logging into the digital health solutions using their account credentials (i.e., web portals for VA professionals, mobile application for veteran patients). There will be a settings page where users are able to view all collected PII and update/edit this information which will be automatically reflected across the system.

Patients are able to view logged health information via the mobile applications which will display logged health metrics (i.e., treatment adherence, patient reported outcome measures, images) as well as health visit details collected during encounters. For veteran patients wishing to change documented health information, they will coordinate to change this information with their healthcare providers in the same manner that they do so with currently in place EHR systems.

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 is not exempt from the access provisions of the Privacy Act. Individuals will be permitted to gain access to "his record or to any information pertaining to him" that is contained in a system of records indexed and retrieved by his name or personal identifier per 5 U.S.C. § 552a(d)(1)

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.

N/A

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 directly captured and editable by users of the system; all users have access to their PII for updating/editing via a settings page viewable through the digital health solutions.

Patients wishing to change documented health information will coordinate to change this information with their healthcare providers in the same manner that they do so with currently in place EHR systems.

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.

Individuals will be notified via the "settings" icon on the primary application screen, where it will display all collected PII with a button marked "edit," indicating their ability to correct this information.

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.

This project allows users to directly access and correct/update their information via the digital health solutions to ensure data accuracy.

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: Data captured or entered by users may be inaccurate, leading to incorrect conclusions about clinical care and medical history.

Mitigation: The project allows individual access and editing of PHI and PII. The system also allows for viewing of health information and allows for change of health records via coordination with their practitioner.

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 will be documented within the security controls in eMASS as part of the system's ongoing 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?

Users from other agencies will not have access to the system unless they fit a user type with a role mentioned below.

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 different roles with access to the system will be:

- **Administrator** – Administrators are privileged accounts that can view and create users within the system. They are able to assign roles to users created within the system and are responsible for managing organizational settings including user access.
- **Practitioner** – Practitioner accounts are non-privileged accounts with access to a web-based portal where they can create patient users as well as view, add, and edit patient healthcare information for patients under their care. Practitioner users are also able to view and edit their own individual PII as well as patient PII for patients under their care.
- **Patient** – Patient accounts are non-privileged accounts with access to a mobile application used on their personal phone. These accounts are able to view and edit their own PII and are able to view, submit, and edit their own health information. These users are not granted web-based portal access and are not granted access to information about other users.
- **Wound Image Tracer** – Wound Image Tracer (WIT) accounts are non-privileged accounts which have read-only access to images submitted by practitioner or patient users. The WIT is able to create data in the form of wound outlines and surface area measurements for viewing in the practitioner and patient applications.
- **Leadership –** Leadership users are non-privileged read-only accounts that can view aggregated population information entered by practitioner, patient, and WIT users. These users have access to a web-based portal where they are able to view summary metrics of the population, such as total number of patients, aggregated clinical outcome rates, and economic outcomes, but this user 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 and subcontractors of the vendor, Impact Health, will have access to the system and the PII of users. The vendor is primarily responsible for the design and maintenance of the system. There is a Cooperative Research and Development Agreement (CRADA) in place which covers disclosure of protected information. Employees and subcontractors of the vendor Impact Health who have access to production systems and the PII therein are considered High Risk. High Risk individuals are kept as limited as possible and receive standard HIPAA training to ensure protection of PII and other sensitive information.

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.

The vendor, Impact 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 Impact Health's security and privacy controls and policies. Employees with access to the system are also required to take annual VA Rules of Behavior training.

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

8.4a If Yes, provide:

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

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

8.4b If No or In Process, provide your ***Initial Operating Capability (IOC) date.***

This system does not yet have Authority to Operate and is currently undergoing ATO approval via the standard eMASS process. The expected date of Initial Operating Capability (IOC) is currently set to 9/1/2023.

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 will be hosted within the VA Enterprise Cloud – AWS GovCloud West

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 – VAEC Hosted

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 – VAEC Hosted

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 – VAEC Hosted

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 – VAEC Hosted

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.

Digitally signed by Kimberly E. Murphy 183320
Date: 2023.05.24 06:19:58 -04'00'

Privacy Officer, Kimberly Murphy

James M. McGee 926698

Digitally signed by James M. McGee 926698
Date: 2023.05.11 09:26:50 -07'00'

Information System Security Officer, Mark McGee

Sirish A Kishore 3494219

Digitally signed by Sirish A Kishore 3494219
Date: 2023.05.11 08:46:04 -07'00'

Information System Owner, Sirish Kishore

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).

These pages will be displayed on the mobile application for Veterans (patients) upon first login. It informs the user around data that will be captured and obtains informed consent for collection and use of PII and PHI from the users. In addition to the below, a Notice of Privacy Practice (NOPP) will be provided to users (https://www.hhs.gov/hipaa/for-individuals/notice-privacy-practices/index.html).

- **Welcome**
  - We are working to advance personalized medicine by developing digital tools to support patients as they pursue better health.
  - This app will help to set expectations for your healthcare journey, receive the best possible care for your disease, monitor your health over time, view your health info, and connect you with your care team.
- **What you should know**
  - This app works in partnership with your hospitals and care teams
  - As a patient, you'll be asked to complete occasional short surveys about your health to ensure that your care teams understand your health changes over time
  - Your care team will receive your health data from the app to inform the best care decisions for you.
  - The more you use the app, the more informed your care team will be.
- **Data Gathering**
  - Impact Health collects information which can be used to understand your health status. This data is gathered when you answer questions and interact with the application and is shared with your care team.
- **Privacy**
  - Your care team can access your personal information along with your health data.
  - Limited Impact Health members will also have access to your personal information.
- **Data Usage**
  - Your health data from the app will be shown to your care team to inform the best possible care decisions. Your health improvement is the primary goal.
  - Your anonymized and deidentified health data may be used in broader research studies to benefit other patients like you.
  - Your personal health data will never be sold.
- **Withdrawing**
  - You may stop using the app at any time and may request removal of personally identifiable information from our database.
- **Consent and Signature**

HELPFUL LINKS:

Record Control Schedules:

https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

General Records Schedule 1.1: Financial Management and Reporting Records (FSC):

https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

National Archives (Federal Records Management):

https://www.archives.gov/records-mgmt/grs

VHA Publications:

https://www.va.gov/vhapublications/publications.cfm?Pub=2

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