CuraPatient

National Artificial Intelligence Institute (NAII)

Veterans Health Administration

Date PIA submitted for review:

March 8, 2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Nancy Katz-Johnson	Nancy.Katz-Johnson@va.gov	202-632-7661
Information System Security Officer (ISSO)	Andrew Vilailack	Andrew.Vilailack@va.gov	813-970-7658
Information System Owner	Rob Maas	Rob.mass@va.gov	352-672-3028

Abstract

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

CuraPatient is a Commercial-Off-The-Shelf (COTS), hosted, cloud-based, COVID-19 Care Plan Management solution that utilizes Artificial Intelligence (AI) techniques and technologies through a Software as a Service (SaaS) delivery model. CuraPatient includes a mobile app (iOS and Android) with versions for patients and providers, a web-based, patient-facing component, along with a web-based, clinician-facing component.

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.

System name is CuraPatient IT System Name, and the Program Office is the office is the National Artificial Intelligence Institute (NAII) within the Office of Research and Development (ORD) under the Veterans Health Administration (VHA)

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

- The purpose of this system is to engage patients (Veterans), gather information about their health, use Artificial Intelligent techniques to optimize Veterans' health interventions, and improve VHA resource utilization.

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

- CuraPatient is a SaaS solution owned by Composite Apps and licensed to the VA.

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.

- CuraPatient collects personal data to aid in the user's registration (NOTE: if end users come through the VA with SSO, then this will be limited) and collection of answers to health-related questions aimed at improving the provider's ability to give the best care to the patient.

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

- The purpose of this system is to engage patients (Veterans), gather information about their health, use Artificial Intelligent techniques to optimize Veterans' health interventions, and improve VHA resource utilization.

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

- Every Veteran's data will be shared only with the Veteran and Veteran's provider/care team to enable care. The data is only gathered and analyzed in the IT system and will not be shared.

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.

- CuraPatient is designed to work with all the VHA facilities and shares a common database so that the data will be consistent across all facilities. However, the system is designed so that every facility can control specific parts related to individual facilities

3. Legal Authority and SORN

A. The IT system name and the name of the program office that owns the IT system.
System name is CuraPatient IT System Name, and the Program Office is the office is the National Artificial Intelligence Institute (NAII) within the Office of Research and Development (ORD) under the Veterans Health Administration (VHA)

B. .All privacy and security laws, directives, and policies for the VA will apply to the software being developed and for implementation by CuraPatient Inc.

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. AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 38, United States Code, Sections 501(b) and 304

Security and Privacy Requirement:

It has been determined that protected health information may be disclosed or accessed and a signed Business Associate Agreement (BAA) shall be required. The Contractor shall adhere to the requirements set forth within the BAA, referenced in Section D of the contract, and shall comply with VA Directive 6066.

A. 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?

The SORN is cited in the PTA as 24VA 10A7. The SORN does not require amendment

D. System Changes

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

- The completion of the PIA will not result in the requirement of system changes to the business processes for development and implementation of the application. Failure to complete the PIA will impact the ability for CuraPatient to implement at VA and interface with VA software and systems.

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

The completion of the PIA will potentially result in the changes if guidance is provided by VA PIA Team to consider implementing into the application.

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 (User Profile Information)
☒ Mother's Maiden Name (User Profile Information)
☒ Personal Mailing Address (User Profile Information)
☒ Personal Phone Number(s) (User Profile Information)
☒ Personal Fax Number (User Profile Information)
☒ Personal Email Address (User Profile Information)
☒ Emergency Contact Information (Name, Phone Number, etc. of a different individual) (User Profile Information)
☒ Financial Information (User Profile Information)
☒ Health Insurance Beneficiary Numbers Account numbers (User Profile Information)
☒ Certificate/License numbers*(User Profile Information)

☒ Vehicle License Plate Number (User Profile Information)
☒ Internet Protocol (IP) Address Numbers (User Profile Information)
☒ Medications
☒ Medical Records
☒ Race/Ethnicity (User Profile Information)
☒ Tax Identification Number (User Profile Information)
☒ Medical Record Number (User Profile Information)
☒ Gender (User Profile Information)
☒ Integrated Control Number (ICN) (User Profile Information)
☒ Military History/Service Connection (User Profile Information)
☒ Next of Kin (User Profile Information)
☒ Other Data Elements (list below)

List of Data Elements listed in the Privacy Threshold Analysis (PTA) for CuraPatient in Section 3.4

- Health Education Materials
- Name
- Medications
- Provider Instructions
- Health Conditions
- SSN
- User profile information (PII)
- Answers to health questionnaires (PHI)
- Scheduling information
- Allergy Intolerance
- Immunizations
- Diagnostic reports
- Conditions
- Observations
- Medications
- Procedures
- Progress Notes
- Assessments
- Interventions

PII Mapping of Components (Servers/Database)
CuraPatient consists of 0 key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by CuraPatient 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 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	N/A	N/A	N/A	**N/A**	**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?

Health Education Materials

- • Name
- • Medications
- • Provider Instructions
- • Health Conditions
- • SSN
- • User profile information (PII)
- • answers to health questionnaires (PHI)
- • scheduling information
- • allergy Intolerance
- • immunizations
- • diagnostic reports
- • Conditions
- • observations
- • medications
- • procedures
- • progress notes
- • assessments
- • interventions

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.

This system does not collect data from a commercial aggregator or sources outside of the VA.

This system does not collect data from a commercial aggregator or sources outside of the VA.
1.2c If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

CuraPatient does create information for the VA by creating reports, score, analysis using Artificial intelligence.

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?

Currently, the only information not created by the CuraPatient system is requested from the VA system(s) and will be read from VA CPRS. If the data does not exist in VA CPRS, they will be collected directly from individuals in the system. The information is checked when it is entered into the system. For data that can change (i.e. address, phone, or email) the user can maintain those items directly, so it is believed to be up to date at all times. The data collected from VA CPRS are routinely checked to ensure the CuraPatient system's data is accurate.

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.

Currently unaware of a form needed subject to the Paperwork Reduction Act for this project.

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.

The information is checked when it is entered into the system. For data that can change (i.e. address, phone, or email) the user can maintain those items directly, so it is believed to be up to date at all times. The data collected from VA CPRS are routinely checked to ensure the CuraPatient system's data is accurate. CuraPatient is in the process of FedRAMP High authorization, to be sure all the requirements for the collection of information will be met.

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.

There is currently no verbiage for accessing a commercial aggregator of information and levels of process required in the contract as the current contract is a base contract to develop and test the application.

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 SORN is as 24VA 10A7.

CuraPatient is in the process of FedRAMP High authorization, to be sure all the requirements for the collection of information will be met. Included will be the security and privacy requirement outlined in the agreed contract between the VA and CuraPatient Inc below:

Security and Privacy Requirement:

It has been determined that protected health information may be disclosed or accessed and a signed Business Associate Agreement (BAA) shall be required. The Contractor shall adhere to the requirements set forth within the BAA, referenced in Section D of the contract, and shall comply with VA Directive 6066.

All privacy and security laws, directives, and policies for the VA will apply to the software being developed and for implementation by CuraPatient Inc.

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. AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 38, United States Code, Sections 501(b) and 304

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: The system will collect and handle PII and PHI.

> Risk: The system collects, processes, and retains PII and PHI. If this information was breached or accidentally disclosed to inappropriate parties or the public, it could result in personal and financial harm to the individuals impacted and adverse negative effect to the VA.

Mitigation:
CuraPatient mitigates the risk by applying appropriate controls to comply with all FedRAMP High controls.

> Mitigation: Data collected, processed, and retained will be protected in accordance with VA Handbook 6500 and FIPS 140-2 encryption and data in-transit protection standards. All systems and individuals with access to the system will be approved, authorized, and authenticated before access is granted. VA annual privacy and security training compliance will be enforced for all VA employees, contractors, and vendors.

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.

Besides the demographic and socio-economic data of each Veteran, CuraPatient collects data related to pre-existing conditions, ability to perform self-care, and post-COVID symptoms. Based on this information, and using Artificial Intelligence techniques, the best care for each Veteran will be predicted. The routine check-ins provide updated information about a Veteran's health. By analyzing new data, if there are any changes in care for the Veteran's needs, the system will make suggestions to the provider.

PII/SPI and justification are listed below:

Health Education Materials – Health education materials will be incorporated to assist with the care coordination and management of Long COVID symptoms for Veterans enrolled and using the CuraPatient application.

Name – The full name of the Veteran is required for user profile information to enroll into the CuraPatietn application.

Medications – Medication information is required for the CuraPatient application to assist with the care coordination/management of treating Long COVID symptoms.

Provider Instructions – Provider Instruction information is required for the CuraPatient application to assist with the care coordination/management of treating Long COVID symptoms.

Health Conditions – Health Conditions information is required for the CuraPatient application to assist with the care coordination/management of treating Long COVID symptoms, and for data collection.

SSN – SSN of the Veetran is required for user profile information to enroll into the CuraPatient application.

User Profile Information (PII) – Information is required for the Veteran to enroll into the CuraPatient application.

Answers to Health Questionnaires – Information it required to assist with the care coordination/management of the application.

Scheduling Information - Scheduling information is required for the CuraPatient application to assist with the care coordination/management of treating Long COVID symptoms.

Allergy Tolerance – Allergy Tolerance information is required for the CuraPatient application to assist with the care coordination/management of treating Long COVID symptoms.

Immunizations - Immunization information is required for the CuraPatient application to assist with the care coordination/management of treating Long COVID symptoms.

Diagnostic Reports – Diagnostic Reports information is required for the CuraPatient application to assist with the care coordination/management of treating Long COVID symptoms.

Conditions – Health Conditions information is required for the CuraPatient application to assist with the care coordination/management of treating Long COVID symptoms.

Observations – Medical Observations information is required for the CuraPatient application to assist with the care coordination/management of treating Long COVID symptoms.

Procedures – Medical Procedures information is required for the CuraPatient application to assist with the care coordination/management of treating Long COVID symptoms.

Progress Notes – Medical provider documentation information is required for the CuraPatient application to assist with the care coordination/management of treating Long COVID symptoms.

Assessments – Medical Assessments information is required for the CuraPatient application to assist with the care coordination/management of treating Long COVID symptoms.

Interventions – Medical Interventions information is required for the CuraPatient application to assist with the care coordination/management of treating Long COVID symptoms.

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.

CuraPatient uses AI techniques to perform data processing and append records to user profiles when making analytics decisions. The new results of the analysis do not replace existing records. However, recent results will be created as progress notes and sent back to the CPRS system.

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.

If new or previous information is available and appropriate to capture out of the best interest of the patients, the information will be stored in the VA's EMHR and the CuraPatient application as both platforms will interface and share information.

2.3 How is the information in the system secured?

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

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

The data is encrypted: at rest, in transit, and in backups with TLS 1.2+ transmissions and FIPS validated tools and cryptography modules.

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

CuraPatient protect all sensitive PII, ePHI, and SSN with the same high standards and encryption methods

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

SC-9 is not included in FedRAMP High SSP, but the following is the SC-8 Transmission confidentiality and Integrity (M) (H)

SSP: SC-8 What is the solution, and how is it implemented?

The CuraPatient system protects the confidentiality AND integrity of transmitted information. CuraPatient is utilizing a combination of encryption at rest via AWS KMS and encryption in transit via TLS v1.2+ with Perfect Forward Secrecy.

SC-28 What is the solution, and how is it implemented?

The Composite Apps DevOps team leverages AWS KMS to perform encryption at rest for all CuraPatient system content. KMS utilizes FIPS 140-2 validated HSMs.

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?

Access to PII from the CuraPatient side is heavily restricted to limited roles and only performed when absolutely necessary with elevated permissions. Access to PII within the CuraPatient app is designated to higher privileged roles (i.e., Organization Admins) and is not available to lower roles. Each end user can see their own data but not the data of other users.

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

Criteria, procedures, controls, and responsibilities regarding access will be documented and monitored.

2.4c Does access require manager approval?

Access will require Manager approval on the VA level to ensure business procedures and access are controlled.

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

Access to PII is being monitored, tracked, and recorded from the VA applications backend using a SPARQ report.

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

Access to the system is restricted to authorized VA Medical Center personnel who have access to the underlying data. The system is encrypted using best practices . In addition, project managers and approving bodies are responsible for vetting personnel who have access to PII/PHI. Personnel who

have access to PII/PHI on this system are required to undergo training and are beholden to VA policies and procedures

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*

Due to HIPAA rules, Composite Apps Inc. (CuraPatient)will retain all information entered into CuraPatient for at least seven years or until instructed to remove data by the data owner/end user. Data to be collected includes demographics, communication between the patient and provider, and health factor data points that will assist the application generate treatment plans for the patients. Other information can be entered by VA staff into the patient's profile to best manage the care and coordination along with the treatment plan(s).

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.*

Due to HIPAA rules, the vendor will retain all CuraPatient information for at least seven years or until instructed to remove data by the data owner/end user. VA sites can specify changes to the retention period since their database is separate from any other customer's database

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?

According to the SORN: POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: In accordance with the records disposition authority approved by the Archivist of the United States, paper records and information stored on electronic storage media are maintained for seventy-five (75) years after the last episode of patient care and then destroyed/or deleted. VHA Records Control Schedule (RCS 10–1), Chapter 6,

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

Please provide response here

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.

CuraPatient data is all stored electronically. The data would be removed from the system by the end user, the Organizational Admin, or after a request to Composite Apps to remove data.

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.

CuraPatient leverages only synthetic data for feature development and testing. Training data is sanitized to scrub identifiable fields which provide no relevance.

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: The system will retain PII/PHI

The information is maintained in accordance with the SORN: POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: In accordance with the records disposition authority approved by the Archivist of the United States, paper records and information stored on electronic storage media are maintained for seventy-five (75) years after the last episode of patient care and then destroyed/or deleted. VHA Records Control Schedule (RCS 10–1), Chapter 6

Mitigation: The system will be certified as FedRAMP High and will follow all VA and industry best practice procedures.
PII/PHI which is no longer relevant is stored within archives within the CuraPatient System and is retained for the length of required US Laws. Relevant data purge mechanisms have been defined in the vendor SSP.

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***
CPRS	Health Information	User profile information (PII), answers to health questionnaires (PHI), scheduling information, allergy Intolerance, immunizations, diagnostic reports, conditions, observations, medications, procedures, progress notes, assessments, interventions	Lighthouse API

4.2 <u>PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure</u>

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: Data is shared with unauthorized individuals
Normal risks associated with data sharing apply, and to prevent data sharing within the department, all users of the system will have unique identifiers (VA SSO), which will leave an appropriate audit trail.

Mitigation: Access to data is limited to those approved and authorized
All users receive their own accounts, and policies are put in place to prevent data sharing to unauthorized individuals

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***
Composite Apps	Need PII/PHI for patient profile	Name, Health Conditions, medications, care plan	VA Contract	A secure method defined by the VA

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: No external sharing at this time

Mitigation: No external sharing at this time

Section 6. Notice

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

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

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

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

Notice is covered under 24VA10A7/85 FR 62406, Patient Medical Records-VA
https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

The VHA Notice of Privacy Practice (NOPP)
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946
explains the collection and use of protected health information to individuals receiving health care from VA. The NOPP is mailed every three years or when there is a major change to all enrolled Veterans. Non Veterans receiving care are provided the notice at the time of their encounter.

This Privacy Impact Assessment (PIA) also serves as notice As required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means."

A Privacy Act Statement is provided on all forms that collect information that will be maintained in a privacy act system of records. The statement provides the purpose, authority and the conditions under which the information can be disclosed.

Notice is also provided in the Federal Register with the publication of the SORN:
provide the citation.

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

Please provide response here

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.

Upon enrollment, the patient will acknowledge and confirm their approval to participate utilizing the application and will be informed that data collected can be used for data review via consent notification when using the application.

Notice was provided and can be found here:

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

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.

CuraPatient is designed to help patients engage with providers and services, manage their care, and to ensure their providers deliver the best possible care. Without providing personal information, the system cannot perform as designed. The system is not mandatory for the Veteran so declining to use the system will not prevent treatment or access to providers.

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.

CuraPatient does not use the information outside the scope of managing the care for the patient, so there is no partial use defined.

Information is used, accessed and disclosed in accordance with the Privacy Act, 5 USC 552a, Title 38 USC 5701, Confidential Nature of Claims, Title USC 7332 and the HIPAA Privacy Rule 45 CFR.
Individuals are provided with a copy of the Notice of Privacy Practices that indicates when information will be used without their consent and when they will be asked to provide consent. Information is used, accessed and disclosed in accordance with the

Privacy Act, 5 USC 552a, Title 38 USC 5701, Confidential Nature of Claims, Title USC 7332 and the HIPAA Privacy Rule 45 CFR.

Individuals or their legal representative may consent to the use or disclosure of information via a written request submitted to their facility Privacy Officer. Individuals also have the right to request a restriction to the use of their information. The written request must state what information and/or to whom the information is restricted and must include their signature and date of the request. The request is then forwarded to facility Privacy Officer for review and processing. Individuals may also request to Opt-Out of the facility directory during an inpatient admission. If the individual chooses to opt-out, information is not disclosed from the facility directory unless otherwise required by law.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

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

Privacy Risk: There is a risk that an individual may not receive notice that their information is being collected, maintained, processed, or disseminated by the Veterans' Health Administration and the local facilities prior to providing the information to the VHA.

Mitigation: This risk is mitigated by the common practice of providing the NOPP when Veterans apply for benefits. Additionally, new NOPPs are mailed to beneficiaries at least every 3 years and periodic monitoring is performed to check that all employees are aware of the requirement to provide guidance to Veterans and that the signed acknowledgment form, when applicable, is scanned into electronic records, The NOPP is also available at all VHA medical centers from the facility Privacy Officer.
The System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) are also available for review online, as discussed in question 6.1.

Section 7. Access, Redress, and Correction

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

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

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.***

Users may always log into their accounts to review their information. Additionally, they can talk to their provider to gain access to any information that the provider has collected for them. The information posted to the EHR is also assessable to Veterans when they access their medical records using existing systems such as the Blue Button Data on MyHealtheVet.

> Veterans and other individuals may also request copies of their medical records and other records containing personal data from the medical facility's Release of Information (ROI) office.
> VHA Directive 1605.01, Privacy and Release of Information, Paragraph 7 outlines policy and procedures for VHA and its staff to provide individuals with access to and copies of their PII in compliance with the Privacy Act and HIPAA Privacy Rule requirements. VHA also created VA form 10-5345a for use by individuals in requesting copies of their health information under right of access.VA Form 10-5345a is voluntary but does provide an easy way for individual to request their records.

By leveraging the SSOi and SSOe from the VA, CuraPatient information access is controlled by the access granted by the VA, which would include the agency's FOIA/Privacy Act practices but may also include additional access provisions if needed necessary or appropriate.

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.

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 will follow guidelines and directives of the Privacy Act to ensure patients PII PHI are protected.

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.

Users can update all their information directly in the system. Any data collected by a provider may need to be updated by the provider themself.

Individuals are required to provide a written request to amend or correct their records to the appropriate Privacy Officer or System Manager as outlined in the Privacy Act SOR. Every Privacy Act SOR contains information on Contesting Record Procedure which informs the individual who to contact for redress. Further information regarding access and correction procedures can be found in the notices listed in Appendix A. The VHA Notice of Privacy Practices also informs individuals how to file an amendment request with VHA.

7.3 How are individuals notified of the procedures for correcting their information?

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

As part of user training, it is made clear that they can create and change their data as necessary by informing VA staff who can correct the information in the electronic medical health record (e.g., demographics and contact information. Individuals will be educated on how to verify their information is correct during user training and onboarding.

Veterans are informed of the amendment process by many resources to include the VHA Notice of Privacy Practice (NOPP) which states:

Right to Request Amendment of Health Information.
You have the right to request an amendment (correction) to your health information in our records if you believe it is incomplete, inaccurate, untimely, or unrelated to your care. You must submit your request in writing, specify the information that you want corrected, and provide a reason to support your request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains your information.

If your request for amendment is denied, you will be notified of this decision in writing and provided appeal rights. In response, you may do any of the following:

- File an appeal
- File a "Statement of Disagreement"
- Ask that your initial request for amendment accompany all future disclosures of the disputed health information

Individuals seeking information regarding access to and contesting of VA benefits records may write, call or visit the nearest VA regional office.

Additional notice is provided through the SORS listed in 6.1 of this PIA and through the Release of Information Office where care is received.

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.

Users can redress their own data. Providers can address the data that they own for a patient.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?

This question is related to privacy control IP-3, Redress.

Follow the format below:

Privacy Risk: There is a risk that members of the public will not know the relevant procedures for gaining access to, correcting, or contesting their information.

Mitigation: the risk of incorrect information in an individual's records is mitigated by authenticating information when possible, Additionally, staff verifies information in medical records and corrects information identified as incorrect during each patient's medical appointments.
The NOPP discusses the process for requesting an amendment to one's records.

The*]* Release of Information (ROI) office is available to assist Veterans with obtaining access to their health records and other records containing personal information.
The Veterans' Health Administration (VHA) established MyHealtheVet program to provide Veterans remote access to their medical records. The Veteran must enroll and have access to the premium account to obtain access to all the available features. In addition, VHA Directive 1605.01 Privacy and Release of Information establishes procedures for Veterans to have their records amended where appropriate.

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.

CuraPatient has an invitation process that will define a user's role when they register (default user role is "patient"). Those accounts will be tied to a security role from the VA SSO and will be mapped to a CuraPatient role.

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?

The VA Privacy Office will establish the criteria for what PII can be shared.

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 VA Privacy Team along with VA IT will determine who is appropriate to gain access to this information collaborating with VA leadership at the NAII and Medical Centers.

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.

The VA will be in control of granting access to contractors via the SSO functionality. The only vendor slotted to have the ability to design and maintain the system is Composite Apps, Inc. The vendor has a BAA with the VA and will also adhere to the contract provisions regarding privacy.

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.

End users are provided the privacy policy and terms of use for the system. VA personnel are to be trained by the VA. Composite Apps' personnel are trained by Composite Apps' internal training department.

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

8.4a If Yes, provide:

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

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

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

1. The Security Plan Status: Being Reviewed by the VA & FedRAMP PMO
2. The Security Plan Status Date: July-14-2022
3. The Authorization Status: WIP
4. The Authorization Date: TBD
5. The Authorization Termination Date: TBD
6. The Risk Review Completion Date: TBD
7. The FIPS 199 classification of the system (LOW/MODERATE/HIGH): HIGH

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)*

CuraPatient is SaaS hosted on AWS in their GovCloud space. AWS GovCloud is FedRAMP authorized at a HIGH impact level.

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.*

AWS standard agreements include that AWS does not own the data in the CuraPatient system. Composite Apps would be the owner of the CuraPatient data with the VA as the Customer and Business Associate.

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.

All data collected by the CuraPatient system is for the intended use of managing the care for individuals. Composite Apps would be the owner of the CuraPatient data with the VA as the Customer and Business Associate.

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.

This is addressed in the Contract. Current contract is 36C10B21C0018 P00002.

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).

The system uses AI to analyze the data and compare a patient's journey to recommend the best care plan. The information the AI suggests can be acted upon by the provider or Veterans at their discretion.

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

ID	Privacy Controls
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.

NANCY KATZ-JOHNSON

Digitally signed by NANCY KATZ-JOHNSON
Date: 2023.06.10 22:15:44 -04'00'

Privacy Officer, Nancy Katz-Johnson

ANDREW VILAILACK

Digitally signed by ANDREW VILAILACK
Date: 2023.06.07 07:09:19 -04'00'

Information System Security Officer, Andrew Vilailack

Robert J. Maas 516033

Digitally signed by Robert J. Maas 516033
Date: 2023.06.26 15:47:02 -04'00'

Information System Owner, Rob Maas

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).

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