Privacy Impact Assessment for the VA IT System called:

Clinical Assessment Reporting and Tracking Program (CART)

Veterans’ Health Administration

Office of Quality and Patient Safety (QPS), Office of Analytics and Performance Integration (API)

1808

Date PIA submitted for review:

March 11, 2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Nancy Katz-Johnson	Nancy.Katz-Johnson@va.gov	203-535- 7280
Information System Security Officer (ISSO)	Roland Parten	Roland.Parten@va.gov	(205) 534- 6179
Information System Owner	Gregory Noonan	Gregory.Noonan@va.gov	(303) 202- 8390

Abstract

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

Clinical Assessment, Reporting, and Tracking (CART) is a multifaceted VHA program whose mission is to monitor and enhance the quality and safety of specialty care for Veterans through clinical analytics and information technology. CART collects and analyses the data entered by clinicians in medical documentation and leverages the data to create operational reports for Sites, VISNs, VACO and Specialty Care Services leadership. This facilitates oversight of the care veterans receive in the VA. CART works with various specialty care services to carry out the above mission. CART has developed and maintains the clinical documentation application (Clinical Assessment, Reporting, and Tracking Applications (CART-Apps)), used to provide direct clinical support for clinical staff evaluating veterans for, and conducting cardiovascular procedures across the VA enterprise.

Overview

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

1 General Description

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

Clinical Assessment, Reporting, and Tracking Applications (CART-Apps) is under the VA Office of Quality and Patient Safety (QPS), Office of Analytics and Performance Integration (API).

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

The mission of the CART Program is to monitor and enhance the quality and safety of specialty care for Veterans through clinical analytics and information technology.

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

Clinical Assessment, Reporting, and Tracking (CART-Apps) is funded by Veterans Health Administration (VHA)

2. Information Collection and Sharing

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

Clinical Assessment, Reporting, and Tracking Applications (CART-Apps) contains approximately 700,000 Veterans that are seen in specialty care clinics.

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

Clinical Assessment, Reporting, and Tracking Applications (CART-Apps) collects and analyses cardiac pre-procedural and procedural information entered by clinicians to become the source of the clinical note placed in CPRS. Data elements are:

Veterans:
Patient Name
Social Security Number
Date of Birth
Date of Death
Gender
Race
Current Medications
Medical Record Number (VistA legacy field DFN (Data File Number))
Patient ICN (Integrated Control Number)
Patient EDIPI (Electronic Data Interchange Personnel Identifier)
Patient Record Dates (Date of cardiac procedure)
Corporate Data Warehouse(CDW) PatientId
Veterans Administration Site
Date of Exam
Exam Type
Genotype/Phenotype
Historical Dates or elements of dates for:
Prior cardiac health, History of cardiac procedures, History of risk factors and co-morbidities, History of cardiac related lab tests, History of Cardiac related medication, Other Cardiac related procedure notes.
Device lot and serial number

Providers:
Name
Veterans Administration Site
Provider DUZ (local/facility provider Record number)
Provider EDIPI (Electronic Data Interchange Personnel Identifier)

Trainees:
Name
Veterans Administration Site
Provider DUZ (local/facility provider Record number)
Provider EDIPI (Electronic Data Interchange Personnel Identifier)

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

CART-Apps shares information with Veterans Health Information Systems and Technology Architecture, Oracle CERNER and the VA Corporate Data Warehouse.

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

Clinical Assessment, Reporting, and Tracking Applications (CART-Apps) is used across the VA enterprise. CART-Apps is centrally managed by the CART Program Office and enforces a standard format for all data acquisition across the CART system.

3. Legal Authority and SORN

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

Legal authority: Title 38, United States Code, Section 501. System of Record Name: National Patient Databases - VA. 121VA10

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

No

4. System Changes

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

No business processes will be impacted or changed.

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

There are no anticipated changes to technology.

Section 1. Characterization of the Information

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

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

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

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

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

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

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

Other PII/PHI data elements:
Date of Death
Corporate Data Warehouse(CDW) PatientId
Patient EDIPI
Patient Record Dates and elements of dates
Date of Exam
Type of Exam
Date of Event
Type of Event
Genotype/Phenotype
Veterans Administration Site
Device lot and serial number
Provider ID Numbers, specifically the DUZ field used by VistA Legacy or the Provider EDIPI
Historical Dates or elements of dates for:

Prior cardiac health, History of cardiac procedures, History of risk factors and co-morbidities, History of cardiac related lab tests, History of Cardiac related medication, Other Cardiac related procedure notes.

PII Mapping of Components (Servers/Database)

Clinical Assessment Reporting and Tracking Program consists of eight key components (servers/databases/instances/applications/software/application programming interfaces (API). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII

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

collected by the Clinical Assessment Reporting and Tracking Program and the reasons for the collection of the PII are in the table below.

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

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	**Does this system collect PII? (Yes/No)**	**Does this system store PII? (Yes/No)**	**Type of PII (SSN, DOB, etc.)**	**Reason for Collection/ Storage of PII**	**Safeguards**
RTLS_1	Yes	Yes	Patient ICN Exam Date Device lot and serial number	Identify the patient and the devices implanted.	Encrypted data. Restricted access.
CARTPro4	Yes	Yes	Patient Name Social Security Number Date of Birth Date of Death Medical Record Number (VistA legacy field DFN (Data File Number)) Patient ICN (Integrated Control Number) Patient EDIPI (Electronic Data Interchange Personnel Identifier) CDW Patient ID Date of Exam Type of Exam Veterans Administration Site Provider DUZ (local/facility provider Record number)	To identify a patient and document the cardiac care provided to the patient.	Encrypted data. Restricted access.

			Device lot and serial number Genotype/Phenotype Historical Details, Dates or elements of dates for: Prior cardiac health, History of cardiac procedures, History of risk factors and co-morbidities, History of cardiac related lab tests, History of Cardiac related medication, Other Cardiac related procedure notes		
GICon	Yes	Yes	Patient Name Veterans Administration Site Medical Record Number (VistA legacy field DFN (Data File Number)) Patient ICN (Integrated Control Number) Social Security Number Date of Birth Date of Death CDW Patient ID Provider DUZ (local/facility provider Record number) Date of Exam Type of Exam	To identify a patient and procedures to provide quality and safety of care oversite in GI procedures.	Encrypted data. Restricted access.
CartWebMAE	Yes	Yes	Patient Name Social Security Number Patient ICN (Integrated Control Number) Date of Birth	To identify a patient and procedural complications to provide quality and safety of care	Encrypted data. Restricted access.

			Date of Event Type of Event Veterans Administration Site Provider DUZ (local/facility provider Record number)	oversite in specialty care procedures.	
CART_CART2	**Yes**	**Yes**	Patient Name Date of Birth Date of Death Medical Record Number (VistA legacy field DFN (Data File Number)) Patient ICN (Integrated Control Number) Patient EDIPI (Electronic Data Interchange Personnel Identifier) CDW Patient ID Date of Exam Type of Exam Veterans Administration Site Provider DUZ (local/facility provider Record number) Device lot and serial number Historical Details, Dates or elements of dates for: Prior cardiac health, History of cardiac procedures, History of risk factors and co-morbidities, History of cardiac related lab tests, History of Cardiac related medication, Other	**To identify a patient and procedures to provide quality, safety of care and longitudinal reporting of patient care.**	**Encrypted data. Restricted access.**

			Cardiac related procedure notes		
VistA	Yes	Yes	Medical Record Number (VistA legacy field DFN (Data File Number)) Provider DUZ (local/facility provider Record number)	To identify patients in the VistA EHR.	Encrypted data. Restricted access.
CERNER	Yes	Yes	Patient EDIPI (Electronic Data Interchange Personnel Identifier)	To identify patients in the CERNER EHR.	Encrypted data. Restricted access.
VINCI_PGx	Yes	Yes	Patient ICN Genotype/Phenotype Date of Exam	Identify the patient and their gene type for quality of care.	Encrypted data. Restricted access.

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 or Primary Subject
Veterans' Health Information Systems and Technology Architecture (VistA)
Oracle Cerner (CERNER)
VA Corporate Data Warehouse (CDW)
Real Time Location Services (RTLS)
Endowriter Databases (EDB)

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.

All data contained in the CART system is from VA data sources. All data collected is used for the purposes of providing and improving patient care, and patient safety.

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

CART-Apps creates the Assessment or Procedural report for any veteran consider for or undergoing a cardiac procedure. CART data and Endowriter data is used to produce operational reports for leadership showing current and historical trends and patterns in patient care.

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?
Information is collected from the Veteran verbally and/or through internal VA data sources such as VistA, CERNER, CDW, RTLS and EDBs via secured data transfer methods.

1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, what is the form's OMB control number and the agency form number?
Forms are not used in the collection of CART data.

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.
Data is entered and reviewed by the clinical staff before submission to the CART-Apps system. Once submitted it becomes part of the patients' medical record and a statement of fact. On a monthly basis, feedback reports containing counts of patients entered and procedures performed are provided to each specialty care service for which CART is collating data. Each specialty care service is responsible for reviewing these feedback reports and making corrections. All data imported to the CART system from other VA systems is imported using synchronist methods. This requires the servers to verify the transmission prior to committing the data to the database.

1.4b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?

No

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

CART has the legal authority to collect data under Title 38, United States Code, Section 501.
System Of Recorded Number: 121VA10
System Of Record Name: National Patient Databases - VA

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: Collection of PHI\PII and unintended disclosure. 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: 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. The data is stored on encrypted drives, in a database behind VA firewalls and not accessible to those outside the VA intranet. Collection of information is limited to PHI\PII needed to successfully treat the patient and enhance the overall outcome and safety of the treatment. When and where possible, for assessing the patient, information is collected verbally from the patient. Additionally, all data entry is through a set of pre-defined elements. All 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 that will be used in support of the program's business purpose.

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

PII/PHI Data Element	Internal Use	External Use
Name	Name is used to identify the patient.	Not used
SSN is used to identify the patient.	SSN is used to identify the patient.	Not used
Date of birth	Date of birth is used to identify the patient.	Not used
Date of Death	Date of Death is used for safety event monitoring and case reviews.	Not used
Gender	Gender is used to categorize patients when reporting on information in the CART database and used in calculations on the patient's data.	Not used
Race	Race is used to categorize patients when reporting on information in the CART database and used in calculations on the patient's data.	Not used
Patients Medical Record Number (VistA legacy field DFN)	Patients Medical Record Number (VistA legacy field DFN) is used by CART to identify patient data that is imported from other VA Files/Databases.	Not used
Corporate Data Warehouse(CDW) PatientId	Corporate Data Warehouse(CDW) PatientId is used by CART to identify patient data that is imported	Not used

	from other VA Files/Databases.	
Integrated Control Number (ICN)	Integrated Control Number (ICN) is used by CART to identify patient data that is imported from other VA Files/Databases.	Not used
Patient EDIPI	Patient EDIPI to identify for identification in the CERNER EHR.	Not used
Patient Record Dates	Patient Record Dates and elements of dates are used on reports generated with CART.	Not used
Exam type	Exam type is used on reports generated with CART.	Not used
VA site	VA site is used on reports generated with CART.	Not used
Previous Medical Records	Previous Medical records are used to calculate procedure risk factors.	Not used
Current Medications	Current Medications are imported for procedural documentation.	Not used
Device Lot and serial numbers	Device Lot and serial numbers are used for cross reference in the event of a device recall.	Not used
Provider ID Numbers,.	Provider ID Numbers, specifically the DUZ field used by VistA Legacy or the Provider EDIPI are used to uniquely identify providers at a facility and in reporting.	Not used
Genotype/Phenotype	Use to determine a patient’s tolerance to certain drug classes.	Not used

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

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

reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis?
Predefined queries are used to report on workloads, procedural volumes and complication rates. Reports are created from de-identified, aggregated data.

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.
CART-Apps uses the data entered into the CART-Apps clinical application (Cardiology only) to produce the Assessment of a patient prior to treatment or the procedural documentation of a patient's cardiac intervention. The medical note is uploaded to the patients' medical record in Computerized Patient Record System (CPRS) by the Attending Physician or automatically uploaded into the Millennium EHR for those sites with CERNER. The note is immediately available to all care providers who have access to the CPRS or Millennium and the need to know.

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?

All data is stored in a Sequential Query Language database using encryption technology mandated and baselined by VA OIT and only traverses the VA intranet.

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

All data at rest or in transit is encrypted using encryption technology mandated and baselined by VA OIT. Data only traverses the VA intranet.

2.3c How is PII/PHI safeguarded in accordance with OMB Memorandum M-06-15?
The VA assigns TMS courses to employees on their responsibilities in this area. In particular, the Privacy Act requires each agency to establish: This memorandum reemphasizes your many responsibilities under law and policy to appropriately safeguard sensitive personally identifiable information and train your employees on their responsibilities in this area. In particular, the Privacy Act requires each agency to establish: "rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or maintaining any record, and instruct each such person with respect to such rules and the requirements of [the Privacy Act], including any other rules and procedures adopted pursuant to this [Act] and the penalties for noncompliance", and "rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or maintaining any record, and instruct each such person with respect to such rules and the requirements of [the Privacy Act], including any other rules and procedures adopted pursuant to this [Act] and the penalties for noncompliance", and "appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to

their security or integrity which could result in substantial harm, embarrassment, inconvenience or unfairness to any individual on whom information is maintained." (5 U.S.C. § 552a(e)(9)-(10)) Each CART employee signs their Rules of Behavior and completes assigned TMS courses before access to PHI\PII data is granted.

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?

Cardiac Clinicians who have a need to use the Clinical Assessment, Reporting, and Tracking Applications (CART-Apps) system are assigned electronic keys that specify their access within the Clinical Assessment, Reporting, and Tracking system. Keys are assigned by their local Automated Data Processing Application Coordinator. In addition, cardiac clinicians are only permitted to view information submitted from the cardiac catheterization lab where they are accessing the Clinical Assessment, Reporting, and Tracking system. Patient information must exist in Veteran Health Information System and Technology Architecture Legacy before it can be added to the Clinical Assessment, Reporting, and Tracking system. When using the Clinical Assessment, Reporting, and Tracking system, you must first launch the Veteran Health Information System and Technology Architecture Legacy Computerized Patient Record System interface; select the patient that will be entered into the Clinical Assessment, Reporting, and Tracking system, and then select the "CART" option for the Tools menu. At this point patient information is passed into the Clinical Assessment, Reporting, and Tracking system through standard Remote Procedure Call Broker calls. In addition to the protections provided by the Veteran Health Information System and Technology Architecture Legacy system (access logs, warnings on sensitive patients, etc.), the Clinical Assessment, Reporting, and Tracking system maintains a log including the user who accessed the system, the identification of the patient whose data was accessed, the date and time of the access, the duration of the access, and what major activities were performed.

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

Clinical Assessment Reporting and Tracking Applications has Standard Operating Procedures covering system access.

2.4c Does access require manager approval?

At the facility level access is approved by the clinical leadership in the Cardiology department. For all others approval must be obtained from the CART Program Office.

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

CART Apps maintains an internal log of who accessed PII information and on what date/time.

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

The CART Program Office ensures the safeguards for PII it controls.

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

The CART system retains all patient information, including all items listed in 1.1, as part of the patient's permanent medical record.

Name
Social Security Number
Date of Birth
Current Medications
Previous Medical Records
Race/Ethnicity
Medical Record Number
Genotype/Phenotype
Other Unique Identifying Information
 Patient gender
 Integrated Control Number
 Patient EDIPI
 Patient Record Dates
 Provider ID Numbers

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.*
The CART system retains all patient records indefinitely as part of the patient's permanent medical record or 75 years after the patient is deceased.

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 CART Program is covered under "National Patient Databases-VA'' (121VA10). According to 121VA10, the following Retention and Disposal must be followed: The records are disposed of in accordance with General Records Schedule 20, item 4. Item 4 provides for deletion of data files when the agency determines that the files are no longer needed for administrative, legal, audit, or other operational purposes.

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

General Records Schedule, Transmittal 34, GRS 4.1 for clinical records. (DAA-GRS-2013-0002-0007)
General Records Schedule, Transmittal 34, GRS 5.1 for Program Office records. (DAA-GRS-2016-0016-0001)
See HELPFUL LINKS section for the link to the National Archives (Federal Records Management)

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 CART records are electronic. In the event a record needs to be purged, only CART personnel with administrative access to the database can remove the record. Backup copies are purged as the backup set is rotated through and overwritten. Currently, that is 42 days. Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and VA Handbook 6500.1 Electronic Media

Sanitization. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destruction.
GRS5.1 Item 010 provides for deletion of data files when the agency determines that the files are no longer needed for administrative, legal, audit, or other operational purposes.

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.

CART testing is completely autonomous and does not use patient data for testing. CART data is not used for research unless an institutional review board or an approved data use agreement exists. CART uses zzTestPatients' as stored in and access from the electronic health record for training.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

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

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

Follow the format below:

Privacy Risk: Retention of PII as part of the patient medical record.

Mitigation: Technical controls to safeguard the information include individual access authentication, logging, password protection (content and life restricted), monitoring unsuccessful login attempts, restriction by security keys, file access restriction, session time-outs, and separation of user from data storage devices.

Administrative controls that protect collected information include the use of the Rules of Behavior signed by those with access to the system, VA procedures for establishing user accounts on the VistA hospital information system, and yearly user training on Privacy and IT Security issues.

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***
CART Program Office	Patient safety and quality of care.	Patient Name Social Security Number Date of Birth Date of Death Race Gender Medical Record Number (VistA legacy field DFN (Data File Number)) Patient ICN (Integrated Control Number) Patient EDIPI (Electronic Data Interchange Personnel Identifier) CDW Patient ID Date of Exam Type of Exam Date of Event Type of Event Veterans Administration Site Provider DUZ (local/facility provider Record number) Device lot and serial number Genotype/Phenotype Historical Details, Dates or elements of dates for: Prior cardiac health, History of cardiac procedures, History of risk factors and co-morbidities, History of cardiac related lab tests, History of Cardiac related medication, Other Cardiac related procedure notes	Encrypted internal VA network
National Gastroenterology	Patient safety and quality of care.	Patient Name Veterans Administration Site	Encrypted internal VA network

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*
and Hepatology Program		Medical Record Number (VistA legacy field DFN (Data File Number)) Patient ICN (Integrated Control Number) Social Security Number Date of Birth Date of Death Race Gender CDW Patient ID Provider DUZ (local/facility provider Record number) Date of Exam Type of Exam	
VistA	Patient medical record	Patient Name Social Security Number Date of Birth Medical Record Number (VistA legacy field DFN (Data File Number)) History of cardiac related lab tests, History of Cardiac related medication Provider DUZ (local/facility provider Record number) ProviderName	RPC Broker via Encrypted internal VA network
CERNER	Patient medical record	Patient EDIPI (Electronic Data Interchange Personnel Identifier)	Encrypted internal VA network
Corporate Data Warehouse	Longitudinal Patient Care	Patient Name Date of Birth Date of Death Race Gender Medical Record Number (VistA legacy field DFN (Data File Number)) Patient ICN (Integrated Control Number)	Encrypted internal VA network

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
		Patient EDIPI (Electronic Data Interchange Personnel Identifier) Date of Exam Type of Exam Veterans Administration Site Provider DUZ (local/facility provider Record number) Genotype/Phenotype Device lot and serial number Historical Details, Dates or elements of dates for: Prior cardiac health, History of cardiac procedures, History of risk factors and co-morbidities, History of cardiac related lab tests, History of Cardiac related medication, Other Cardiac related procedure notes	

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: Inappropriate sharing of information

Mitigation: All data is shared in accordance with the Data Use Agreement and/or IRB signed between CART and other internal agencies.

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***
None				

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

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

If no External Sharing listed on the table above, ***(State there is no external sharing in both the risk and mitigation fields).***

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

Follow the format below:

<u>**Privacy Risk**</u> Inappropriate sharing of information

<u>**Mitigation:**</u> All data is shared in accordance with the Data Use Agreement signed between CART and other external agencies. No PHI\PII is shared by CART with any outside agencies or groups.

Section 6. Notice

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

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

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

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

Notice is also provided in the Federal Register with the publication of the System of Records Notice 121VA10. National Patient Databases -VA.

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

Notice are provided. See Appendix A for copy.

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.
The comprehensive notice is provided as described above in 6.1 a.

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.
Information is requested when it is necessary to administer benefits to veterans and other potential beneficiaries. While an individual may choose not to provide information, this may prevent them from obtaining the benefits necessary to them. The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VHA an SSN (see 38 CFR 1.575(a)).

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

This question is directed at whether an individual may provide consent for specific uses, or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent.
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: Individual is not aware of how their information is going to be collected, shared and maintained.

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.***

There are several ways a veteran or other beneficiary may access information about them. Access procedures are stated in the System of Records Notice 121VA10. National Patient Databases -VA. The Department of Veterans' Affairs has created the MyHealthEVet program to allow online access to their medical records. More information on this program and how to sign up to participate can be found online at https://www.myhealth.va.gov/index.html. Veterans and other individuals may also request copies of their medical records and other records containing personal data from the medical facility's Release of Information (ROI) office.

VHA Directive 1605.01, Privacy and Release of Information, 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.

Employees should contact their immediate supervisor and Human Resources to obtain information. Contractors should contact Contract Officer Representative (COR) to obtain information upon request.

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)?

CART Apps is not exempt for the Privacy Act provisions.

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?

CART Apps is not exempt for the Privacy Act provisions.

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.

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.

Individuals seeking information regarding access to and contesting of records in this system may write the:
Director of National Data Systems (10P2C)
Austin Information Technology Center
1615 Woodward Street
Austin, Texas 78772

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

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

Veterans are informed of the amendment process by many resources to include the VHA Notice of Privacy Practice (NOPP). Additional notice is provided through the SORN 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.

The CART system does not directly interact with veterans. Redress is provided as stated above.

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?

Users of the CART-Apps system are assigned electronic keys that specify their access within the CART-Apps system. In addition, users are only permitted to view information submitted from the cardiac catheterization lab where they are accessing the CART-Apps system. Physician are granted Read/Write permissions, Fellows Read, and on a case-by-case basis, Write permissions, and Nurses are granted Read permissions.

In addition to the protections provided by the Vista Legacy system (access logs, warnings on sensitive patients, etc), the CART-Apps system maintains a log including the user who accessed the system, the ID of the patient whose data was accessed, the date and time of the access, the duration of the access, and what major activities were performed.

By mandate, Information Technology Operations, Back Office Database Team has administrative privileges on CART-Apps server through a group account.

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?

There are no users from other agencies.

8.1c Describe the different roles in general terms that have been created to provide access to the system? For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

Physician are granted Read/Write permissions, Fellows Read, and on a case-by-case basis, Write permissions, and Nurses are granted Read permissions. By mandate, Information Technology Operations, Back Office Database Team has administrative privileges on CART-Apps server through a group account.

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.
Yes. Contracts are reviewed yearly by the CART Program Office and clearance extended or revoked. A contractor performs the application programing, or one could be employed by VA IT Operations unbeknown to the CART Program Office. VA IT Operations is responsible for vetting their contractors.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately.
This question is related to privacy control AR-5, Privacy Awareness and Training.

All users are required to take the privacy and security training and have varied degrees of access based on their background check and level of security. Users sign rules of behavior documents and undergo annual IT security training programs. As needed TMS courses are assigned to users according to job functions.

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

*8.4a If Yes, provide:*Yes

1. *The Security Plan Status: Approved*
2. *The System Security Plan Status Date: 08-Nov-2022*
3. *The Authorization Status: Authorization to Operate (ATO)*
4. *The Authorization Date:* 20-Apr-2023
5. *The Authorization Termination Date:* 19-Apr-2025
6. *The Risk Review Completion Date:* 3-Apr-2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* 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.***

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)*

CART does not utilize the VAEC. CART uses physical and virtual servers located in VA data facilities.

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.*

CART does not utilize the VAEC.

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.

CART does not utilize the cloud services.

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.

CART does not utilize the cloud services.

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).

CART does not utilize bots or AI technologies.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

NANCY KATZ-JOHNSON

Digitally signed by NANCY KATZ-JOHNSON
Date: 2024.04.22 09:33:33 -04'00'

Privacy Officer, Nancy Katz-Johnson

ROLAND PARTEN

Digitally signed by ROLAND PARTEN
Date: 2024.04.19 14:18:54 -05'00'

Information System Security Officer, Roland Parten

GREGORY NOONAN

Digitally signed by GREGORY NOONAN
Date: 2024.04.19 12:53:52 -06'00'

Information System Owner, Gregory Noonan

APPENDIX A-6.1

The VA Notice of Privacy Practices can be found at this link.
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=8928

HELPFUL LINKS:

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

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

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

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