Privacy Impact Assessment for the VA IT System called:

Cardiac Device Monitoring System (CDMS)

National Cardiac Device Surveillance Program

Veterans Health Administration

eMASS ID #:1192

2/15/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Kimberly Murphy	Kimberly.Murphy@va.gov	781-331-3206
Information System Security Officer (ISSO)	Amine Messaoudi	Amine.Messaoudi@va.gov	202-815-9345
Information System Owner	Merritt Raitt M.D.	Merritt.Raitt@va.gov	503-220-8262 x57571

Abstract

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

The National Cardiac Device Surveillance Program (NCDSP) - Cardiac Device Monitoring System manages the home remote monitoring of implanted pacemakers or defibrillators and other important clinical events.

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?*

Cardiac Device Monitoring System is owned by the National Cardiac Device Surveillance Program

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

Medtronic Optima PaceArt Application is a key component of CDMS. Under VHA DIRECTIVE 1189, January 13, 2020: NCDSP manages the 24/7 home remote monitoring of Veterans with implanted pacemakers or defibrillators. Remote monitoring replaces in person clinic follow up and allows for monitoring for arrhythmias, lead and battery problems, device recalls and other critical clinical events. The CDMS uses Veterans Administration Enterprise Cloud (VAEC) hosting technology and maintains VAEC Azure databases of Veterans with pacemakers and defibrillators and partners with Department of Veterans Affairs (VA) National Safety Office to formulate and execute the official VA response to Food and Drug Administration (FDA) and industry recalls and alerts. It enables the continued delivery of critical patient care nationally and further enhances the NCDSP patient experience. CDMS is hosted within the private VAEC Microsoft Azure FedRAMP authorized Infrastructure as a Service (IaaS) solution.

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

VA Owned and VA Operated

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?*

Information Technology Operations and Services (ITOPS) provides crucial support for over 190,000 remote transmissions each year for over 60,000 Veterans and 100 VA clinics.

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

CDMS shares data externally with approved vendors via an Memorandum of Understanding & Information security Agreement (MOU / ISA). In addition, CDMS shares data internally with VistA.

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

Disclosure of CDMS data would significantly impact the reputation of the VA and the patient.

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?*

The CDMS is dependent on servers that run sophisticated monitoring Commercial Off the Shelf (COTS) software that includes 6 terabyte sequel (SQL) database, software for documenting the review of transmissions, Memorandum of Understanding/Information Security Agreement (MOU/ISA to import remote monitoring data from the manufacturers and the need for XML and HL7 connections.

3. Legal Authority and SORN

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

The legal authority that applies to the system are: Health Insurance Portability and Accountability Act (HIPAA) Security Rule, 45 C.F.R. Part 160; Privacy Act of 1974, 5 U.S.C.§552a, as amended, Title 38 United States Code (U.S.C.) 1730C, 7301(b).

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?*

The SORN covers cloud usage and storage. The applicable SORN to the system is 24VA10A7, "Patient Medical Records – VA" 2020-21426.pdf (govinfo.gov). https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

4. System Changes

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

No

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

No

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: Health information related to their implanted cardiac device; readings, measurements, and metrics.

PII Mapping of Components (Servers/Database)

Cardiac Device Monitoring System (CDMS) has one component that collects PII and that component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by CDMS 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.

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

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
(Server name: CDMS Integration Server, Centralized VistaA Imaging Exchange (CVIX))	**Yes**	**YES**	• **Name** • **Social Security Number** • **Addresses** • **Date of Birth** • **Sex** • **Phone Number** • **Health information related to their implanted cardiac device.**	**Collect home remote monitoring of Veterans with implanted pacemakers or defibrillators.**	**VAEC Azure Security intrusion prevention, User authentication and passwords, inactivity lockout**

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?

CDMS collects its data from clinicians, staff and approved external partners.

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.

Patient name, social security number and phone number (PII) are provided by the local clinic staff and entered by NCDSP. Patient health information (PHI) is also entered by the NCDSP staff and in addition comes to CDMS via ISA/MOU approved data transfers from the cardiovascular implantable electronic devices (CIEDs) manufacturer(s).

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

Once the patient is registered in CDMS, model and serial number data is copied from the manufacturer of the patients implanted device (e.g., pacemaker or defibrillator).

1.3 How is the information collected?

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

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

The information is collected by the manufacturer(s), external of the VA. Once a patient is identified and registered, their device data copies into CDMS. CDMS itself does not collect information from patients. The clinicians that register the patient into CDMS does. Data from the referring VA clinic is sent securely to the NCDSP via CDMS clinic interface application and encrypted email. Data from the manufacturer(s) is either transmitted via a secure connection to the NCDSP (covered by an existing MOU/ISA) or staff of the NCDSP review the data at the company secure web portal and type it into the Optima application and it is stored in the Optima database.

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?

All information is collected electronically.

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.

Through current data connections all information is shared and updated via automation, regular audit checks that replicate information across all sources for integrity.

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?

For data to be transferred from the manufactures to the NCDSP, there has to be exact matches in both databases for patient ID and implanted device identification. This ensures that data is accurate and only matched with the appropriate patient.

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

Health Insurance Portability and Accountability Act (HIPAA) Security Rule, 45 C.F.R. Part 160; Privacy Act of 1974, 5 U.S.C.§552a, as amended VA SOR 24VA10A7; VA Claims Confidentiality Statute, 38 U.S.C § 5701 and 38 U.S. Code § 7332 Confidentiality of certain medical records.

VHA DIRECTIVE 1189, January 13, 2020: NATIONAL CARDIAC DEVICE SURVEILLANCE PROGRAM and Title 38 United States Code (U.S.C.) 1730C, 7301(b).

This Veterans Health Administration (VHA) directive provides policy to ensure that all VA patients with CIEDs are registered with the VHA National Cardiac Device Surveillance Program (NCDSP) and that when appropriate they are enrolled in a remote monitoring program.

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

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

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

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

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

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

<u>Principle of Data Quality and Integrity:</u> 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: CDMS contains sensitive personal information. Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or if the data was otherwise breached, serious harm or even identity theft may result.

Mitigation: Users must be an authorized employee of the Department of Veteran Affairs. Then they request login credentials by a person in a CDMS Clinician Management Role to receive username/password access to the application.

MOU / ISA secures and encrypts the traffic giving the ability to monitor the ports and shut down the network interfaces.

To access the information user must have access through two factor authentication via PIV cards, and they must also have login information (username/password) to access the application. External connections with access to the VA network require Site-to-Site VPN accounts which uses encrypted tunnels and firewalls and are routed through the Trusted Internet Gateways (TIC).

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	Used to register the patient with the device, monitoring system and appointment reminders.	Not used
Social Security Number	Used to register the patient with the device, monitoring system and appointment reminders.	Not used
Date of Birth	Used to register the patient with the device, monitoring system and appointment reminders.	Not used
Personal Mailing Address	Used to register the patient with the device, monitoring system and appointment reminders.	Not used
Personal Phone	Used to register the patient with the device, monitoring system and appointment reminders.	Not used
Personal Email	Used to register the patient with the device, monitoring system and appointment reminders.	Not used
Device Information	Used to review device reports on readings, measurements, metrics, etc. to determine performance, patient needs and general care.	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?

CDMS is a comprehensive workflow solution that efficiently compiles and manages patients' cardiac device 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.

The system can collect, store, and retrieve data from device programmers and remote monitoring systems from all major cardiac device manufacturers but, no analysis is performed on the data. The data stored in the relational database can then be sent to VA Electronic Health Record via HL7 connection to VistA/CPSR.

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?

CDMS is hosted in the VAEC Azure and utilizes approved technology.

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

Connections to the manufacturer(s) are documented by fully executed MOU/ISA and occur over 443 HTTPS.

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

Access to the system and/or data is restricted to VA staff users.

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?

Username and password with elevated privileges for administrator access. PIV Card for Patient Registration portal.

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

System Administrators or other users accessing CDMS, must be processed for a Federal Background investigation, complete annual VA Privacy training, and submit annual VA documentation before access could be granted.

2.4c Does access require manager approval?

System access is only provided to individuals with a business purpose request approved by CDMS Program Management as per the Access Control Standard Operating Procedures (SOP).

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

Access is monitored by Azure Monitor as per the Audit Control Standard Operating Procedures (SOP)

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

All CDMS staff is responsible for safeguarding PII information, or they shall face disciplinary actions.

Section 3. Retention of Information

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

Identify and list all information collected from question 1.1 that is ***retained*** *by the system.*
This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal

Name, Social Security, Date of Birth, Personal Mailing, Personal Phone Number(s), Personal Email Address, device information (PHI).

3.2 How long is information retained?

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

Records are maintained and disposed of in accordance with records disposition authority approved by the Archivist of the United States and are retained for 75yrs.

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?

When managing and maintaining VA data and records, healthcare facilities follow the guidelines established in the NARA-approved VA Record Control Schedule RCS 10-1 which can be found at: http://www.oprm.va.gov/docs/RCS005-1-OIT-8-21-09.pdf

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

VHA Records Control Schedule (RCS 10–1) 6000.1d (N1–15–91–6, Item 1d) and 6000.2b (N1–15–02–3, Item 3)

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.

The System Manager will take immediate action to have the disposition of records in the system reviewed and paperwork initiated to obtain an approved records disposition authority in accordance with VA Handbook 6300.1, Records Management Procedures. The VA Office of Policy and Planning (OPP) will publish an amendment to this notice upon issuance of National Archives and Records Administration (NARA)-approved disposition authority. The records may not be destroyed until VA obtains an approved records disposition authority. OPP destroys electronic files when no longer needed for administrative, legal, audit, or other operational purposes. In accordance with title 36 CFR 1234.34, Destruction of Electronic Records, “electronic records may be destroyed only in accordance with a records disposition schedule approved by the Archivist of the United States, including General Records Schedules." Within this process data is retained and archived or maintained for seventy-five (75) years after the last episode of patient care and then destroyed/or deleted.

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

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

PII is not used for the purposes of testing and training. Test patients are created for this purpose.

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 information may not conform to currently identified NARA standards listed in the records control schedule, RCS-10.

Mitigation: To mitigate the risk posed by information retention, CDMS adheres to the VA Records Controls Schedules (RCS) for data it maintains. When the retention data is reached for a record Infrastructure Operations (IO) Platforms will carefully dispose of the data as described in VHA Directive 6300, Section 8, Records Disposition Program.

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***
VA Centralized VistA Imaging Exchange (CVIX)	Clinical review and follow-up, scheduling reminders	• Name • social security number • date of birth • sex • health information related to their implanted cardiac device.	Electronically transmitted from CDMS to Computerized Patient Record System (CPRS) through the ISI Importer

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: PII or VA employee information could be displayed during system use and viewed by someone who is not authorized to work on the scheduling system.

Mitigation: Data is transferred "via HTTPS and encrypted end-to-end with Transport Layer Security (TLS)." In addition, all personnel with internal access to Veteran information must complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually.

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***
Medtronic Carelink	Pull device information from vendor	• Name • social security number • date of birth • sex • health information related to their implanted cardiac device.	VHA Directive 1189, MOU / ISA	TLS / secure SSL (Business Partner Gateway)
Abbott Laboratories	Pull device information from vendor	• Name • social security number • date of birth • sex • health information related to their implanted cardiac device.	VHA Directive 1189, MOU / ISA	TLS / secure SSL
Biotronik	Pull device information from vendor	• Name • social security number • date of birth • sex • health information related to their implanted cardiac device.	VHA Directive 1189, MOU / ISA	TLS / secure SSL
Boston Scientific	Pull device information from vendor	• Name • social security number • date of birth • sex • health information related to their implanted cardiac device.	VHA Directive 1189, MOU / ISA	TLS / secure SSL

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.

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

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

Follow the format below:

Privacy Risk: Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or if the data was otherwise breached, serious harm or even identity theft may result.

Mitigation: MOU / ISA secures and encrypts the traffic giving the ability to monitor the ports and shut down the network interfaces.

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.

VHA is required to send out the VHA Notice of Privacy Practices every three (3) years. In this Notice it specifically addresses how VHA will use and disclose health information. Attached is a copy of the most recent VHA Notice of Privacy Practices.

SORN 24VA10A7 Patient Medical Records-VA

Link; Notice of Privacy Practices 10-163p_(004)_-Notices_of_Privacy_Practices-_PRINT_ONLY.pdf

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

Notice is provided

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

This Privacy Impact Assessment (PIA) also serves as notice of CDMS. 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."

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.

By receiving services from NCDSP / CDMS for implanted device procedures at the VA. The individuals have already provided answers to the questions and the information is supplied to VistA by VA clinicians / clinical staff; therefore, they have already given their implied consent. If a person declines to provide the requested information, they will be denied service.

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.

Once information is provided to the VA, records are used as necessary, to ensure the administration of statutory benefits to all eligible Veterans, Service members, Reservists, and their spouses, surviving spouses and dependents. As such, CDMS does not provide individuals with the direct opportunity to consent to particular uses of information. However, if an individual wish to remove consent for a particular use of their information, they should contact the nearest VA regional office or medical center. A list of VA regional offices and state medical centers can be found at http://benefits.va.gov/benefits/offices.asp or va.gov/health/vamc/.

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

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

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

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

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

<u>Privacy Risk:</u> Without publication of the PIA for CDMS there is a risk that individuals could be unaware that their sensitive information was being collected by the system.

<u>Mitigation:</u> Veterans and other beneficiaries are provided with multiple forms of notice of information collection, retention, and processing. The three main forms of notice are discussed in detail in question 6.1 and include the Privacy Act statement, a System of Record Notice, and the publishing of this Privacy Impact Assessment. As a Veteran, they get a Notice of Privacy Practice where it lists what the data, they give VHA may be used for. The notices sent to veterans list the purposes and the uses for the data, and if the information is not received the Veterans will not know their privacy rights.

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.***

All information that is submitted to CDMS originates in the health record. Requests for information can be requested through the privacy officer at their facility. A list of VA regional offices and state medical centers can be found at http://benefits.va.gov/benefits/offices.asp.

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)?

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?

System complies with Privacy Acy system.

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.

All information that is submitted to CDMS originates in the health record. An amendment request may be requested if the information is incorrect, the process is that the individual must make the request in writing to the Privacy Officer at the facility where they are receiving care and then it will be amended if the information is incorrect.

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

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

The individual can contact the Privacy Officer where they receive their care and requests an amendment to their record. They are also notified in their Notice of Privacy Practice documentation.

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 Privacy Act and HIPAA law allow right of access to an individual's record as well as for making an amendment request. This is done through the facility Privacy Officer and by following a formal redress process that is already in place.

7.5 <u>PRIVACY IMPACT ASSESSMENT: Access, redress, and correction</u>

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:
<u>Principle of Individual Participation:</u> Is the individual provided with the ability to find out whether a project maintains a record relating to him?

<u>Principle of Individual Participation:</u> 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?

<u>Principle of Individual Participation:</u> 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:

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

<u>Mitigation:</u> The privacy risk is mitigated by Notice of Privacy Practices and contact the Privacy Officer to access or correct their information.

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?

- ICD Remote Clinician Role or Standard User Accounts (SUA) – issued for routine non-privileged access. These accounts allow users to read only access to patients that belong to their own panel.

• Clinic Management Role or Administrator/Privileged Accounts – Highest rights allowed on CDMS issued to accomplish administrative tasks requiring privileged access on VA information systems. These accounts are separate from the SUA and are Non Mailboxed Enabled Accounts (NMEA).

• Office Staff Role – Provides patient support in person and over the phone, such as home monitoring transmissions and cell adapters for monitors. Accepts web submissions to set up activations for remote monitoring, verify incoming data, registering patient on manufacturer web sites. Scheduling medical follow-up appointments.

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?

Outside agencies do not have access to the system, the only exception is a read only access for research purposes per an agreement.

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 above users facing application is managed by NCDSP Program Analyst System Administrator. NCDSP Program Analyst is responsible for creating, modifying and deleting user accounts. Initial access is granted with PIV card to log on Government Furnished Equipment (GFE) or VA Citrix Server. Then further access is controlled by request only. Once user account request is approved by Program Managers the Administrator grants permissions based on username, password accounts with roll-based permissions. Standard Operating Procedure (SOP) will be enhanced as new Active Directory integration and two (2) factor authentication is developed.

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, all contractors (Who) attended Mandatory VA security training and reoccurring annual mandatory training. There is no disclosure agreement or NDA that gets signed for contractors. They just undergo the same privacy training as employees. Contractors are reviewed every 90 days per the contract requirements. Currently at this present time, there are no contractors that have access to CDMS.

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 employees complete initial and annual Cyber Security, Privacy, and HIPAA training and sign the VA Rules of Behavior agreement.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* is approved.
2. *The System Security Plan Status Date:* 31 Jan 2024
3. *The Authorization Status:* Authorization to Operate (ATO)
4. *The Authorization Date:* 27 Oct 2023
5. *The Authorization Termination Date:* 24 April 2024
6. *The Risk Review Completion Date:* 25 Oct 2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Overall Moderate

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

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

N/A

Section 9 – Technology Usage

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

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

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

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

Yes, CDMS is hosted in the VA Enterprise Cloud (VAEC) Azure environment within the Infrastructure as a Service (IaaS) model.

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

N/A

9.3 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.

This question is related to privacy control DI-1, Data Quality.

N/A

9.4 NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

N/A

9.5 If the system is utilizing Robotics Process Automation (RPA), please describe the role of the bots.

Robotic Process Automation is the use of software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. For example, will the automation move or touch PII/PHI information. RPA may also be referred to as "Bots" or Artificial Intelligence (AI).

No

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 provided in this Privacy Impact Assessment is true and accurate.

Digitally signed by Kimberly E. Murphy 183320
Date: 2024.03.12 06:54:12 -04'00'

Privacy Officer, Kimberly Murphy

AMINE MESSAOUDI

Digitally signed by AMINE MESSAOUDI
Date: 2024.03.11 09:24:56 -05'00'

Information Systems Security Officer, Amine Messaoudi

MERRITT RAITT

Digitally signed by MERRITT RAITT
Date: 2024.03.08 16:00:39 -08'00'

Information Systems Owner, Merritt Raitt M.D.

APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy; a Privacy Act notice on forms; screen shot of a website collection privacy notice).

https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

HELPFUL LINKS:

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

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

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

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

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