Privacy Impact Assessment for the VA IT System called:

Medical Modernization Zone 6B Interface (MedMOD Zone 6B Int)

VA Office of Information Security (OIS) Specialized Device Cybersecurity Department (SDCD) – Veterans Affairs Central Office (VACO)

Date PIA submitted for review:

July 12, 2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Julie Drake	Julie.drake@va.gov	*202-632- 8431*
Information System Security Officer (ISSO)	Katherine Vollmer	Katherine.Vollmer@va.gov,	605-890-0079
Information System Owner	Trimaine McFadden	Trimaine.McFadden@va.gov	803-223-1438

Abstract

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

The VA Medical Modernization Zone 6B Interface, hereafter referred to as MedMOD Zone 6B Int, is the Department of Veterans Affairs' (VA) medical authorization isolation zone boundary at the VA enterprise level for those medical devices that communicate to the DoD Medical Community of Interest (MedCOI) via a custom developed interface through Defense Health Agency (DHA) connectivity compliant with Joint Security Architecture (JSA) firewalls deployed at VA medical facilities for management of unified electronic health records. This system will consist of the various medical devices to communicate to Cerner servers and databases within a separate DHA approved security enclave.

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:

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *Indicate the ownership or control of the IT system or project.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *A general description of the information in the IT system and the purpose for collecting this information.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.*
- *A citation of the legal authority to operate the IT system.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*
- *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?*

Medical Modernization Zone 6B Interface is VA medical authorization isolation zone boundary at the VA enterprise level for those medical devices that communicate through MedCOI compliant architecture via a custom developed interface for management of unified electronic health records.

This MedMOD Zone 6B Int system consists of various medical devices to communicate to servers and databases within the Cerner security enclave thru the MedCOI connection utilizing the JSA firewalls at various VA medical centers and Community Based Outpatient Clinics (CBOC). This system will include those servers and medical devices with an approved Enterprise Risk Analysis (ERA). This system will include, but not limited to, those servers and medical devices such as GE (General Healthcare) Cardiac Assessment System for Exercise (CASE) testing, GE MUSE, Natus NeuroWorks, Heidelberg Heyex, BreezeConnect, Zeiss, CareStream PACS (Picture Archiving and Communication System), Omnicell, Nuance PowerScribe 360, ScriptPro, Remote Automated Lab System (RALS), Aranz Silhouette, Highland PACS Gear, and various lab instruments.
These medical devices require isolation from general IT systems and cannot be managed using a VA-approved secure configuration baseline and cannot accept automatic vulnerability patching (i.e., automated installation of operating system and/or application updates, security patches, Office of Information Technology (OIT)-management via SCCM, BigFix, etc.)

- This system, MedMOD Zone 6B Int, inherits from the VA Enterprise Network (VAEN) enclave, which provides segmentation of the logical data flow of network-connected medical devices through VA Local Area Network (LAN) and Wide Area Network (WAN) to the unified electronic health records hosted by CERNER in Kansas City. MedMOD Zone 6B Int system also communicates internally with VistA (Veterans Health Information Systems Technology and Architecture)/CPRS (Computer Patient Record System) at various VA medical centers and Community Based Outpatient Clinics (CBOC). The VA program office system owner is the Office of Information Security (OIS) Specialized Device Cybersecurity Department (SDCD) in conjunction with the Veterans Health Administration (VHA) Healthcare Technology Management (HTM) Program Office.
- The purpose of this Platform IT (PIT) system is to provide a pathway for VA network-connected medical components to communicate to the Unified Electronic Health Record (EHR). This system is a VA enterprise-level system of networked medical devices that directly affect the Agency's mission to provide healthcare to Veterans, specifically these devices to provide direct treatment, diagnostics and monitoring of patients and impact the health and safety of individual patients and the quality of healthcare services provided by VHA. Networked medical devices may contain Protected Health Information (PHI) or Personally Identifiable Information (PII) locally on the device in varying quantities but are not the System of Record (SOR) for this data. Networked medical devices need to be able to connect to other network devices to transmit and receive data, provide automated medical record updates, pull work lists, generate data for clinical decision support processes, and allow remote vendor maintenance for support.
- This system is VA owned and operated Information System network-connected component that operates in health care facilities across VHA facilities. The same controls will be used consistently across the VA sites through the management from the VHA HTM Program Office. The records are those of Veterans and VA Employees. The expected number of individuals whose information will be stored in the system will be in the millions of unique records and a total of 100,000 users will have access to this information.
- MedMOD Zone 6B Int operates under the following system authority: The legal authority is Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule Parts 160 and 164. Title 38, United States Code, Sections 501(b) and 304. Patient Medical Records including Consolidated Health Records (CHR) for patients including Social Security Number (SSN), medical history, employment history, medical benefit and eligibility information, and

patient admission and discharge information is used as a medical record identifier as required in the following SOR Notice (SORN): VA System of Records Notice (SORN) 24VA10A7/ 85 FR 62406. (https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf)

- MedMOD Zone 6B Int is not cloud hosted, the data flows from the VA owned medical device thru the Joint Security Architecture and into the MEDCOI where it will then be routed to the Joint Electronic Health Record that is hosted by CERNER in Kansas City. Each medical system's PPS and topology diagram found in the applicable Enterprise Risk Assessment (ERA).
- MedMOD Zone 6B Int meets confidentiality and integrity objectives by using encrypted virtual private network between VA WAN router in the CERNER Federal Enclave and WAN router in VA Medical Center (VAMC). The cryptographic technology is the Group Encrypted Transport VPN (GETVPN). GETVPN is designed specifically for the Multi-Protocol Label Switching (MPLS) network.
- The completion of this PIA will not result in circumstances that require changes to business processes, and the completion of this PIA will not result in technology changes.

Section 1. Characterization of the Information

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

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

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

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

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

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

☒ Name
☒ Social Security Number
☒ Date of Birth
□ Mother's Maiden Name
□ Personal Mailing Address
□ Personal Phone Number(s)
□ Personal Fax Number
□ Personal Email Address
□ Emergency Contact Information (Name, Phone

Number, etc. of a different individual)
☐ Financial Account Information
☐ Health Insurance Beneficiary Numbers Account numbers
☐ Certificate/License numbers
☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☐ Current Medications
☐ Previous Medical Records
☐ Race/Ethnicity
☐ Tax Identification Number
☒ Medical Record Number
☒ Gender
☐ Integration Control Number (ICN)
☐ Military History/Service Connection
☐ Next of Kin
☒ Other Unique Identifying Information (list below)

Other Unique Identifying Information - Prescription Information, Medical Information (Diagnostic date), and Biometric Health Data/Vital Signs

PII Mapping of Components

MedMOD Zone 6B Int consists of thirty-six (36) multiple key components. Each component has been analyzed to determine if any elements of that component collect PII. Each connection has been reviewed by the Enterprise Risk Analysis (ERA) team. The type of PII collected by MedMOD Zone 6B Int and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

Note: Due to the PIA being a public facing document, please do not include the server names in the table.

PII Mapped to Components

Database Name of the information system collecting/storing PII	**Does this system collect PII? (Yes/No)**	**Does this system store PII? (Yes/No)**	**Type of PII (SSN, DOB, etc.)**	**Reason for Collection/ Storage of PII**	**Safeguards**
GE Healthcare MUSE (Mobile Ultrasonic Equipment)	yes	yes	• Patient First and Last Name • Social Security Number • Date of Birth (DOB) • Gender • Biometric Health Data/Vital Sign	Provide direct treatment, diagnostics and monitoring of patients	Encryption at rest and in transit; MDIA (Medical Device Isolation Architecture) and ACLs (Access Control List) on ports and protocols to limit communication outside of VLAN (Virtual Local Area Network)
DICOM Gateway Pro	yes	yes	• Patient First and Last Name • SSN • DOB	Provide direct treatment, diagnostics and	Encryption at rest and in transit; MDIA and ACLs on ports and protocols to limit

			• Gender • Medical Record Number (MRN)	monitoring of patients	communication outside of VLAN
CARESCAPE Gateway	yes	yes	• Patient First and Last Name • SSN • DOB • Gender • Biometric Health Data/Vital Sign	Provide direct treatment, diagnostics and monitoring of patients	Encryption at rest and in transit; MDIA and ACLs on ports and protocols to limit communication outside of VLAN
Natus EEG Server	yes	yes	• Patient First and Last Name • SSN • DOB • Gender • Biometric Health Data/Vital Sign	Provide direct treatment, diagnostics and monitoring of patients	Encryption at rest and in transit; MDIA and ACLs on ports and protocols to limit communication outside of VLAN
Heidelberg Heyex PACS Spectrails	yes	yes	• Patient First and Last Name • SSN • DOB • Gender	Provide direct treatment, diagnostics and monitoring of patients	Encryption at rest and in transit; MDIA and ACLs on ports and protocols to limit communication outside of VLAN
Natus EMG Server Synergy Nicolet EDX EMG Wks.	yes	yes	• Patient First and Last Name • SSN • DOB • Gender • Biometric Health Data/Vital Sign	Provide direct treatment, diagnostics and monitoring of patients	Encryption at rest and in transit; MDIA and ACLs on ports and protocols to limit communication outside of VLAN
Roche Diagnostics – AccuCheck	yes	yes	• Patient First and Last Name • SSN • DOB	Provide direct treatment, diagnostics and monitoring of patients	Encryption at rest and in transit; MDIA and ACLs on ports and protocols to limit communication outside of VLAN
Roche Diagnostics – Cobras Analyzer	yes	yes	• Patient First and Last Name • SSN • DOB	Provide direct treatment, diagnostics and monitoring of patients	Encryption at rest and in transit; MDIA and ACLs on ports and protocols to limit communication outside of VLAN
MGC Diagnostics - BreezeConnect	yes	yes	• Patient First and Last Name • SSN	Provide direct treatment, diagnostics	Encryption at rest and in transit; MDIA and ACLs on ports and

			• DOB • Gender • MRN	and monitoring of patients	protocols to limit communication outside of VLAN
Hyland PACSGEAR	yes	yes	• Patient First and Last Name • SSN • DOB • Gender	Provide direct treatment, diagnostics and monitoring of patients	Encryption at rest and in transit; MDIA and ACLs on ports and protocols to limit communication outside of VLAN
ARANZ	yes	yes	• Full Name • Phone number • Date of Birth • Electronic Data Interchange Personal Identifier (EDIPI) •Information regarding wound location •Patient wound imaging	Provide direct treatment, diagnostics and monitoring of patients	Encryption at rest and in transit; MDIA and ACLs on ports and protocols to limit communication outside of VLAN
Vyaire SentryConnect	yes	yes	• Patient First and Last Name • SSN • DOB • Gender • MRN	Provide direct treatment, diagnostics and monitoring of patients	Encryption at rest and in transit; MDIA and ACLs on ports and protocols to limit communication outside of VLAN
OmniCenter	yes	yes	• Patient First and Last Name • SSN • DOB • Gender • Medication Lists	Provide direct treatment, diagnostics and monitoring of patients	Encryption at rest and in transit; MDIA and ACLs on ports and protocols to limit communication outside of VLAN
Connect RX	yes	yes	• Patient First and Last Name • SSN • DOB • Gender • Medication Lists	Provide direct treatment, diagnostics and monitoring of patients	Encryption at rest and in transit; MDIA and ACLs on ports and protocols to limit communication outside of VLAN
Phillips Health Vue PACS	yes	yes	• Patient First and Last Name • SSN • DOB • Gender	Provide direct treatment, diagnostics and monitoring of patients	Encryption at rest and in transit; MDIA and ACLs on ports and protocols to limit communication outside of VLAN

Phillips Intellibridge (IBE)	yes	yes	• Patient First and Last Name • SSN • DOB • Gender • Biometric Health Data/Vital Sign	Provide direct treatment, diagnostics and monitoring of patients	Encryption at rest and in transit; MDIA and ACLs on ports and protocols to limit communication outside of VLAN
Phillips IntelliVue (PIIC)	yes	yes	• Patient First and Last Name • SSN • DOB • Gender • Biometric Health Data/Vital Sign	Provide direct treatment, diagnostics and monitoring of patients	Encryption at rest and in transit; MDIA and ACLs on ports and protocols to limit communication outside of VLAN
Phillips IntelliSpace Critical Care and Anesthesia	yes	yes	• Patient First and Last Name • SSN • DOB • Gender • Biometric Health Data/Vital Sign	Provide direct treatment, diagnostics and monitoring of patients	Encryption at rest and in transit; MDIA and ACLs on ports and protocols to limit communication outside of VLAN
Phillips Xper IM Application Server and Xper Interface Production Server	yes	yes	• Patient First and Last Name • SSN • DOB • Gender • Biometric Health Data/Vital Sign • Medication Lists	Provide direct treatment, diagnostics and monitoring of patients	Encryption at rest and in transit; MDIA and ACLs on ports and protocols to limit communication outside of VLAN
ScriptPro Central	yes	yes	• Patient First and Last Name • SSN • DOB • Gender • Medication Lists	Provide direct treatment, diagnostics and monitoring of patients	Encryption at rest and in transit; MDIA and ACLs on ports and protocols to limit communication outside of VLAN
Zeiss Forum Database	yes	yes	• Patient First and Last Name • SSN • DOB • Gender • Biometric Health Data	Provide direct treatment, diagnostics and monitoring of patients	Encryption at rest and in transit; MDIA and ACLs on ports and protocols to limit communication outside of VLAN

Zeiss IOL 700 Master	yes	yes	• Patient First and Last Name • SSN • DOB • Gender • Biometric Health Data	Provide direct treatment, diagnostics and monitoring of patients	Encryption at rest and in transit; MDIA and ACLs on ports and protocols to limit communication outside of VLAN
Zeiss OCT Cirrus 5000	yes	yes	• Patient First and Last Name • SSN • DOB • Gender • Biometric Health Data	Provide direct treatment, diagnostics and monitoring of patients	Encryption at rest and in transit; MDIA and ACLs on ports and protocols to limit communication outside of VLAN
Zeiss HFA3 Review Software	yes	yes	• Patient First and Last Name • SSN • DOB • Gender • Biometric Health Data	Provide direct treatment, diagnostics and monitoring of patients	Encryption at rest and in transit; MDIA and ACLs on ports and protocols to limit communication outside of VLAN
Oculus Pentacam	yes	yes	• Patient First and Last Name • SSN • DOB • Gender • Biometric Health Data	Provide direct treatment, diagnostics and monitoring of patients	Encryption at rest and in transit; MDIA and ACLs on ports and protocols to limit communication outside of VLAN
Optos Advance	yes	yes	• Patient First and Last Name • SSN • DOB • Gender • Biometric Health Data	Provide direct treatment, diagnostics and monitoring of patients	Encryption at rest and in transit; MDIA and ACLs on ports and protocols to limit communication outside of VLAN
Siemens Syngo Dynamics Application Integration	yes	yes	• Patient First and Last Name • SSN • DOB • Gender	Provide direct treatment, diagnostics and monitoring of patients	Encryption at rest and in transit; MDIA and ACLs on ports and protocols to limit communication outside of VLAN
Cadwell CadLink	yes	yes	• Patient First and Last Name • SSN • DOB • Gender	Provide direct treatment, diagnostics and monitoring of patients	Encryption at rest and in transit; MDIA and ACLs on ports and protocols to limit communication outside of VLAN

			• Biometric Health Data/Vital Signs		
ATP Solution Client database (tCGRx Pharmacy)	yes	yes	• Patient First and Last Name • SSN • DOB • Gender • Medication Lists	Provide direct treatment, diagnostics and monitoring of patients	Encryption at rest and in transit; MDIA and ACLs on ports and protocols to limit communication outside of VLAN
EndoPRO IQ7	yes	yes	• Patient First and Last Name • SSN • DOB • Gender	Provide direct treatment, diagnostics and monitoring of patients	Encryption at rest and in transit; MDIA and ACLs on ports and protocols to limit communication outside of VLAN
Sysmex XN Analyzer PIM Application	yes	yes	• Patient First and Last Name • SSN • DOB • Gender • Biometric Health Data/Vital Signs	Provide direct treatment, diagnostics and monitoring of patients	Encryption at rest and in transit; MDIA and ACLs on ports and protocols to limit communication outside of VLAN
Siemens Clinitek Status Connect	yes	yes	• Patient First and Last Name • SSN • DOB • Gender • Biometric Health Data/Vital Signs	Provide direct treatment, diagnostics and monitoring of patients	Encryption at rest and in transit; MDIA and ACLs on ports and protocols to limit communication outside of VLAN
Methasoft Treatment Management	yes	yes	• Patient First and Last Name • SSN • DOB • Medication Lists	Provide direct treatment, diagnostics and monitoring of patients	Encryption at rest and in transit; MDIA and ACLs on ports and protocols to limit communication outside of VLAN
Polysmith DMS	yes	yes	• Patient First and Last Name • SSN • DOB • Gender • Biometric Health Data/Vital Signs	Provide direct treatment, diagnostics and monitoring of patients	Encryption at rest and in transit; MDIA and ACLs on ports and protocols to limit communication outside of VLAN
Abbott	yes	yes	• Patient First and Last Name	Provide direct treatment,	Encryption at rest and in transit; MDIA and

			• SSN • DOB	diagnostics and monitoring of patients	ACLs on ports and protocols to limit communication outside of VLAN
EndoSoft Endovault	yes	yes	• Patient First and Last Name • SSN • DOB • Gender	Provide direct treatment, diagnostics and monitoring of patients	Encryption at rest and in transit; MDIA and ACLs on ports and protocols to limit communication outside of VLAN

1.2 What are the sources of the information in the system?

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?

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 1.3 indicate why the system is using this source of data.

If the system creates information (for example, a score, analysis, or report), list the system as a source of information.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

MedMod Zone 6B Int can collect and receive information from Cerner, and VistA/CPRS via Health Level 7 (HL7) messaging, or by manual entry from the patient medical record.

1.3 How is the information collected?

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 technology used in the storage or transmission of information in identifiable form?

If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form's OMB control number and the agency form number.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

Information is collected via electronically via transfer (HL7 messaging transmission) from other systems and also by manual entry by the clinical staff into the medical device.

1.4 How will the information be checked for accuracy? How often will it be checked?

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.

If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.
This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

MedMOD Zone 6B Int system allows the clinicians to manage/monitor the information included in the patient's profile. The Veterans' identifying information is checked for accuracy by the Clinicians and is cross-referenced with information on Veterans each time the clinicians see their patients.

1.5 What specific legal authorities, arrangements, and agreements defined the collection of information?

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders.
This question is related to privacy control AP-1, Authority to Collect

The MedMOD Zone 6B Int system operates under the following system authority:
The legal authority is HIPAA Privacy Rule Parts 160 and 164. The patient medical record information is found under the SORN of 24VA10A7/85 FR 62406 - Patient Medical Records-VA https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf .
Legal Authority: Title 38, United States Code, Sections 501(b) and 304. VETERANS' BENEFITS Part II Chapter 17 Subchapter I and Subchapter II HOSPITAL, NURSING HOME, OR DOMICILIARY CARE AND MEDICAL TREATMENT.

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.

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.

This information is collected via the applications interfaces (HL7), and through direct manual entry from clinical personnel with the purpose of patient care and treatment. The information is directly relevant and necessary to accomplish the purposes of patient care and treatment. The medical devices, to the extent possible and practical, collect information directly from the individual. However, most information is collected electronically via HL7, and not directly from the patient as the patient provides minimal information. Personal Identifiable Information (PII) is taken directly from VistA and is verified by local facility staff.

<u>Privacy Risk:</u>
Medical devices and medical systems collect the minimal amount necessary of both Personally Identifiable Information (PII) and Protected Health Information (PHI). Due to the highly sensitive nature of this data, there is a risk that, this collected, process, or retained data is not accurate, not complete, nor current.

<u>Mitigation:</u>
The VA is careful to only collect the information necessary to assist in the care of patients and provide an updated status to clinical health care providers. By only collecting the minimum necessary information, the VA can better protect the Veterans' information. Once information is collected, process, or retained, there are security safeguards in place, i.e., transmitted using encryption and stored in secure, encrypted servers behind VA firewalls.
The information collected is via the applications interfaces (HL7), and through direct manual entry from clinical personnel with the purpose of patient care and treatment. The information is directly relevant and necessary to accomplish the purposes of patient care and treatment. The medical devices, to the extent possible and practical, collect information directly from the individual. However, most information is collected electronically via HL7, and not directly from the patient as the patient provides minimal information but the clinical staff can verify and correct their information prior, during and after the procedures with the medical devices. Personal Identifiable Information (PII) is taken directly from VistA and is verified by local facility staff.

Section 2. Uses of the Information

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

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

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

Name: Used as an identifier
SSN: Used as an identifier
DOB: Used as an identifier
Medical Record Number: Used as an identifier
Gender: Used as an identifier
Prescription Information: used in treatment of patient
Medical Information: used in decision of treatment of patient
Biometric health data: used in treatment of patient

The data allows for decision support and early intervention of our most critically ill patients. System information is required to identify individual patients and allow for patient charting and continuity of care between shifts and transfer to other health care providers. Use is in line with VA practices for caring.

2.2 What types of tools are used to analyze data and what type of data may be produced?

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.

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.
This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

MedMOD Zone 6B Int is a network-connected medical devices/systems which are essential to providing Veterans' healthcare services as they support patient monitoring, management, diagnostic, and treatment of Veterans, which is the core mission of the VA's Veterans Health Administration. Network-connected medical devices/systems provide data integrity to the field of healthcare by eliminating the need for manually inputting patient diagnostics and treatment into VA's electronic healthcare record and allows clinicians to focus on their primary task of providing comprehensive patient care. Networked medical devices/systems may contain Protected Health Information (PHI) locally on the device in varying quantities but are not the system of record for this data.

The sources of information are from VistA/CPRS/Unified EHR (Cerner) to a combination of medical devices/systems, and this information is sent and received by medical devices/systems in the forms of health information, and then sent back to VistA/CPRS/Unified EHR (Cerner) for clinicians to use in patient monitoring, management, diagnostic, and treatment of Veterans. Health information will be placed back in the individual existing medical record.

MedMOD Zone 6B Int does not analyze data but provides data to the clinicians as stated above.

2.3 How is the information in the system secured?

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

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

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

This question is related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest

For meeting confidentiality and integrity objectives, the specified system interconnection is an encrypted VPN (Virtual Private Network) between the VA WAN (Wide Area Network) router in the Cerner Federal Enclave and WAN router in VAMC. The cryptographic technology is the Group Encrypted Transport VPN (GETVPN). GETVPN is designed specifically for the Multi-Protocol Label Switching (MPLS) network where Cisco implements the IPSec (Internet Protocol Security) Tunnel Mode with Address Preservation (RFC 5374 and RFC 4301). IP Address Preservation enables encrypted packets carry the original source and destination IP addresses in the outer IP header rather than replacing them with tunnel endpoint addresses. (FIPS 140-2 certification #: 2176). In addition, access to medical devices is on a need-to-know basis and limited to clinical staff, Biomedical staff, and others with a legitimate need-to-know.

2.4 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u> How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

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

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

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

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

Access to medical devices is on a need-to-know basis, and limited to clinical staff, Biomedical staff, and others with a legitimate need-to-know. MedMOD Zone 6B Int system is restricted to personnel with VA Privacy and Information Security Awareness training and Rules of Behavior, and Privacy and HIPAA training, certified annually. The access control procedures are with the supervisor or designee requesting access, thus providing the approval for the clinical staff to the VistA/CPRS/EHR and to the medical devices, where the medical device data is transmitted and stored. The local Information System Security Officer (ISSO), and supervisor or designee review the VistA/CPRS/EHR access semi-annually. Where technically feasible for the medical devices, audit logs are maintained on the access to the medical devices. Audit logs are reviewed periodically by the system administrators and business owners.
The assurance of the safeguards for PII are the responsibility of the system administrators, business owners, and users of the medical devices.

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 information below that may be retained. None of the information is retained permanently in the medical devices/systems.

- Name
- SSN
- Date of Birth
- Medical Record Number
- Gender
- Prescription Information
- Medical Information (Diagnostic date)
- Biometric Health Data/Vital Signs

None of the information is retained permanently in the medical devices/systems. Data is entered into VistA/CPRS/Unified EHR as part of the patient record. All patient data (Medical history, vital signs (waveforms, pulse, resp., B/P, O2 sat, temperature) is temporarily saved during patient treatment for reporting purposes. As stated in the Records Control Schedule, RCS 10-1, Chapter Six – Healthcare Records, 6000.2 Electronic Health Record, temporary records can be destroyed after verification of accurate entry of information into EHRS (Electronic Health Record System) Link - https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf

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. If the system is using cloud technology, will it be following the NARA approved retention length and schedule?

The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.
This question is related to privacy control DM-2, Data Retention and Disposal.

All information is temporarily retained for reporting purposes, depending on the medical device/system -this system, MedMOD is not a system of record. As stated in the Records Control Schedule, RCS 10-1, Chapter Six – Healthcare Records, 6000.2 Electronic Health Record, temporary records can be destroyed after verification of accurate entry of information into EHRS (Electronic Health Record System) Link - https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so, please indicate the name of the records retention schedule.

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.
This question is related to privacy control DM-2, Data Retention and Disposal.

As not all data is not retrieved at a personally identifiable level, no records retention schedule is required. All information is temporarily retained for reporting purposes back to the patient's medical record. VA clinical staff document notes in CPRS on the patient treatment, and that record's retention is determined at the local facility. When managing and maintaining VA data and records, healthcare facilities follow the guidelines established in the National Archives and Records Administration (NARA) approved Records Control Schedule, RCS 10-1, Chapter Six – Healthcare Records, 6000.2 Electronic Health Record, temporary records can be destroyed after verification of accurate entry of information into EHRS (Electronic Health Record System) Link - https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf

3.4 What are the procedures for the elimination of SPI?

Explain how records are destroyed or eliminated at the end of the 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

As reports are produced by the medical devices/systems and sent electronically to the patient medical records or manual entry, no hard paper copy would be produced. However, if a hard paper copy was used and scanned, the hard copy would then be shredded per the VA sanitization requirements within VA Directive 6500. The media sanitization requirements as outlined in VA Directive 6500 are followed, and this would mean that the hard drives would be destroyed to meet the VA Directive 6500 requirements. If the hard drives could not be destroyed, then guidance and procedures for appropriate use of the MDPP (Medical Device Protection Program) Clearing Software in device sanitization would be followed. MDPP Clearing Software tool for non-destructive removal of PII and/or ePHI from medical device hard drives, while maximizing the potential trade-in or resale value of the device.
As stated in the Records Control Schedule, RCS 10-1, Chapter Six – Healthcare Records, 6000.2 Electronic Health Record, temporary records can be destroyed after verification of accurate entry of information into EHR link - https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf.

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. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?
This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research

MedMod Zone 6B Int system does not use PII for research, testing or training. Test patient data for the medical devices/systems would be used, if at all, and not actual patient data (PII).

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.

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

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

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

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

Follow the format below:

Privacy Risk:
The risk of maintaining data within medical devices or medical systems. The longer the time frame of information residing within medical devices or medical systems, the more the risk increases.

Mitigation:
Record storage in both the retention and the number of records is reviewed and assessed during the risk analysis of medical devices. MDPP develops guidance and promotes the adoption throughout VA of multiple layers of administrative, technical, and physical safeguards that work together to reduce the attack surface and minimize negative outcomes of medical device compromise without inhibiting performance or the patient's healthcare experience. Some safeguards or compensating controls that are in place are encryption of hard drives, physical security measures to secure medical devices, device sanitization, and awareness and training. None of the information is retained permanently in the medical devices/systems.

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***
VHA VistA VAEC-AWS (VA Enterprise Cloud – Amazon Web Service) -- various VAMC (VA Medical Centers and their CBOC's (Community Based Outpatient Clinic)	Treatment and diagnosis of patients	Patient first and Last Name, Social Security Number (SSN), Date of Birth (DOB), Current medications	Manual and Health Level 7 (HL7) transfer

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

Follow the format below:

Privacy Risk: Data sharing is necessary for medical care of persons eligible for care at VHA facilities. There is risk data could be shared with inappropriate organizations or institutions which has the potential for a catastrophic impact on privacy.

Mitigation: Potential harm is mitigated by various levels of security in place on MedMOD Zone 6B Int system. The system uses full disk encryption to protect data at rest. Transport Layer Security (TLS) encryption for MedMOD Zone 6B Int protects Data in Transit Secure File Transfer Protocol (SFTP) is used when transferring call lists. The process, and all encryption, complies with Federal Information Processing Standards (FIPS) 140-2. Access to MedMOD Zone 6B Int is restricted to personnel with VA Privacy and Information Security Awareness and Rules of Behavior training and Privacy and HIPAA training, certified annually.

Users access device technologies within MedMOD Zone 6B Int with VA provided PIV card, providing Multi-Factor Authentication by requiring PIV card authentication. MedMOD Zone 6B Int system administrator(s) access requires elevated privileges authenticated by an eToken. Finally, MedMOD Zone 6B Int system only contains, accesses, and processes the minimum necessary data to complete required processing, to minimize PHI / PII at any given time.

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*	*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*	*List the method of transmission and the measures in place to secure data*

	with the specified program office or IT system		***sharing (can be more than one)***	
Cerner Corporation	Treatment and diagnosis of patients	Patient First and Last Name, SSN, DOB, Medical record number, Gender, Medical Information (diagnostic date), Biometric health data/vital signs	SORN - 24VA10A7/85 FR 62406 - Patient Medical Records-VA; National ISA/ MOU – Cerner VA ISA/MOU – ID: E-2168 and MEDCOI ID: 687	Group Encrypted Transport VPN -IPSec tunnel utilizing Joint Security Architecture (JSA) across MedCOI
DOD Defense Health Agency (DHA)	Treatment and diagnosis of patients	Patient First and Last Name, SSN, DOB, Medical record number, Gender, Medical Information (diagnostic date), Biometric health data/vital signs	SORN - 24VA10A7/85 FR 62406 - Patient Medical Records-VA; Interagency Agreement DOD DHA VA National MEDCOI ISA – ID 733	Group Encrypted Transport VPN -IPSec tunnel utilizing Joint Security Architecture (JSA) across MedCOI
ScriptPro	Treatment and diagnosis of patients	Prescription data with Social Security Number, and DOB	SORN - 24VA10A7/85 FR 62406 - Patient Medical Records-VA; Script Pro ISA/MOU ID: E-80	Encrypted S2S (site-to-site) VPN
Nuance Communications, Inc. (Microsoft Comp	Treatment and diagnosis of patients	Patient First and Last Name, Social Security Number, Date of Birth, Gender, and medical condition and/or diagnosis	SORN - 24VA10A7/85 FR 62406 - Patient Medical Records-VA; Nuance Communications ISA/MOU ID: E-774	Encrypted S2S (site-to-site) VPN
Carestream Health	Maintenance and support of medical device	No PHI/PII	Carestream Health ISA/MOU ID: E-723	Carestream remote Support over TCP/UDP (transmission

				control protocol/user datagram protocol) ports 53 and 443
Omnicell Technologies	Maintenance and support of medical device	No PHI/PII	Omnicell Technologies ISA/MOU ID: E-776	Encrypted S2S (site-to-site) VPN
Abbott	Maintenance and support of medical device	No PHI/PII	Abbott ISA/MOU ID: E-704	Encrypted S2S (site-to-site) VPN
Philips Intellibridge (IBE) and Xper Information Management	Treatment and diagnosis of patients	Patient First and Last Name, SSN, DOB, Medical record number, Gender, Medical Information (diagnostic date), Biometric health data/vital signs	SORN - 24VA10A7/85 FR 62406 - Patient Medical Records-VA; Philips Healthcare ISA/MOU ID: E-789	Encrypted S2S (site-to-site) VPN
Siemens Healthineers AG	Treatment and diagnosis of patients	Patient first and last name, test results, medical record number, patient identifier, and accession number	SORN - 24VA10A7/85 FR 62406 - Patient Medical Records-VA; Siemens Healthcare ISA/MOU ID: E-812	Encrypted S2S (site-to-site) VPN
Omnicell Connect RX (vSuite IDM)	Maintenance and support of medical device	No PHI/PII	Omnicell Technologies ISA/MOU ID: E-776 and ID: E-777	Encrypted S2S (site-to-site) VPN
GE Healthcare	Treatment and diagnosis of patients	Patient First and Last Name, DOB, Medical Record Number, Patient images, waveforms, Gender	SORN - 24VA10A7/85 FR 62406 - Patient Medical Records-VA; GE Healthcare-ISA/MOU ID: E-742	Encrypted S2S (site-to-site) VPN
EndoSoft	Treatment and diagnosis of patients	Patient First and Last Name, Date of Birth, Medical Record Number, Gender	SORN - 24VA10A7/85 FR 62406 -	Encrypted S2S (site-to-site) VPN

			Patient Medical Records-VA; UTECH Products-ISA/MOU ID: E-827	

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.

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> There is risk of unintended exposure of patient data to organizations that do not have a need to know or legal authority to access VA data.

<u>Mitigation:</u> Potential harm of unintended exposure of patient data is mitigated by various levels of security in place on MedMOD Zone 6B Int system. The system uses an encrypted VPN between the VA WAN router in the Cerner Federal Enclave and WAN router in VAMC. The cryptographic technology is the GET VPN. GET VPN is designed specifically for the MPLS network where Cisco implements the IPSec Tunnel Mode with Address Preservation (RFC 5374 and RFC 4301). IP Address Preservation enables encrypted packets carry the original source and destination IP addresses in the outer IP header rather than replacing them with tunnel endpoint addresses. (FIPS 140-2 certification #: 2176). In addition, access to medical devices is on a need-to-know basis and limited to clinical staff, Biomedical staff, and others with a legitimate need-to-know. MedMOD Zone 6B Int is restricted to personnel with VA Privacy and Information Security Awareness training and Rules of Behavior, and Privacy and HIPAA training, certified annually.

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 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?

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. If notice was provided in the Federal Register, provide the citation.

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

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 question is 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.

Notice of Privacy Practice (NOPP) are discussed at the individual VistA/CPRS/Unified EHR sites and documented in their respective PIAs. NOPP's are available and mailed to each enrolled veteran. The patient medical records are covered under the SORN of 24VA10A7/85 FR 62406 - Patient Medical Records-VA https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf .

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

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

Yes, patients have the opportunity and right to decline to provide information, and also have the right to decline treatment. However, if the correct patient cannot be verified to be accurate, then treatment may be denied, rescheduled or cancelled by the clinical staff.

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

Patients have the right to decline treatment. Patients do not have the right to consent to particular use of the information if they seek treatment. Information is required for clinical use and success in patient care.

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.

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: Before providing information to the VA, an individual may not receive appropriate notice that their information is being collected, maintained, processed, or disseminated by VA. A risk that Veterans will not know that medical devices/systems exist or that if the medical devices collect, maintain and or disseminate PII/PHI.

Mitigation: The risk is mitigated by providing a Notice of Privacy Practice (NOPP). Risk is also mitigated by making the SORN and the current Privacy Impact Assessment (PIA) available for online review. The information collected is from the System of Records Notice 24VA10A7/85 FR 62406 - Patient Medical Records-VA at the local facility's CPRS/VistA/Unified EHR. This PIA will be posted online for the public to view. Patients and families are educated on the process of medical devices/systems when they are being treated for care. All information collected comes from VistA/CPRS/Unified EHR via HL7 messaging, or by manual entry of the information. NOPP are discussed at the individual VistA/CPRS/Unified EHR sites and documented in their respective PIAs.

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?

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.

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).

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.
This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

Data is entered or communicated to the VistA/CPRS/Unified EHR and the VistA/CPRS/Unified EHR is governed by VA policies and procedures for patient access to that data. VHA Release of Information (ROI) offices at facilities are present to assist Veterans with obtaining access to their health records and other records containing personal information. VHA established the MyHealthVet (MHV) program to provide Veterans remote access to their health records. The Veteran must enroll in MHV to obtain access to all the available features. In addition, Directive 1605.01 Privacy and Release of Information establishes procedures for Veterans to have their records amended when appropriate. Patients do not have access to the information in the medical devices as it is for clinical use only.

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.

If information is incorrect in their patient medical record, then they would contact the VA facility where they are receiving care and request an amendment.

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 NOPP, which every patient receives when they enroll for care, discusses the process for requesting an amendment to their records. VHA staff distributes a Release of Information (ROI) procedure at facilities to assist Veterans with obtaining access to their health records and other records containing personal information. In addition, Directive 1605.01 Privacy and ROI establishes procedures for Veterans to have their records amended when appropriate.

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.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.

The veteran would utilize the procedures in the NOPP, which every patient receives when they enroll for care. The users would not have direct access to the medical devices/systems information to allow for corrections, and any information would be within the VistA/CPRS/Unified EHR. VHA staff distributes a Release of Information (ROI) process at facilities to assist Veterans with obtaining access to their health records and other records containing personal information. In addition, Directive 1605.01 Privacy and ROI establishes procedures for Veterans to have their records amended when appropriate.

Inaccurate information is corrected by VA site personnel with access to the appropriate biomedical device.

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.

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 a Veteran may not know how to obtain access to their records or how to request corrections to their records.

Mitigation: The NOPP, which every patient receives when they enroll for care, discusses the process for requesting an amendment to their records. VHA staff distributes a Release of Information (ROI)process at the VA facilities to assist Veterans with obtaining access to their health records and other records containing personal information. In addition, Directive 1605.01 Privacy and ROI establishes procedures for Veterans to have their records amended when appropriate. VHA established the MHV program to provide Veterans remote access to their health records. The Veteran must enroll in MHV to obtain access to all the available features. In addition, Directive 1605.01 Privacy and Release of Information establishes procedures for Veterans to have their records amended when 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?

Describe the process by which an individual receives access to the system.

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?

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.

This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.

The medical devices/workstations have a login that the user must have credentials. This is limited to "need to know" for clinical personnel and Biomedical staff. All staff with access to patient information in the performance of their duties need to know their responsibilities in maintaining the confidentiality of VA sensitive information, especially patient information, by completing the annual VA Privacy and Information Security Awareness and Rules of Behavior training, and Privacy and HIPAA Training.

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, various medical device vendors could have remote access to the system, for which there is a national VPN agreement as well as a business agreement with the vendor. Contractual, agreed upon privacy training and confidentiality is required from the vendor. A Business Associate Agreement (BAA) and an Interconnection System Agreement/Memorandum of Understanding (ISA/MOU) exists between the VA and the medical device vendor.

Yes, contractors who are the vendor or manufacturer of the medical device have involvement with the design, configuration, and maintenance of their medical device/system. No NDA is needed if they represent the medical device vendor/manufacturer.

VA controls access to the system at the hosting infrastructure level and ensures Rules of Behavior are in place and signed before granting access to the VA network. Contractors may obtain VA network accounts if the contractors complete appropriate background investigations and have received security clearance in accordance with VA Standard Policies and Procedures needed to perform their tasks; and complete VA Privacy and Information Security Awareness and Rules of Behavior training, and Privacy and HIPAA training, and are re-certified annually.

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 VA employees/contractors who have access to VA computers must complete the onboarding and annual mandatory privacy and information security training. In addition, all employees who have access to PHI must complete the VHA mandated Privacy and HIPAA Focused training. Finally, all new employees receive face-to-face training by the facility Privacy Officer and Information Security Officer during new employee orientation. The Privacy and Information Security Officer also perform subject specific trainings on an as needed basis.

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

If Yes, provide:

1. *The Security Plan Status,* **Approved**
2. *The Security Plan Status Date,* **June 29, 2022**
3. *The Authorization Status,* **Authorized**
4. *The Authorization Date,* **March 10, 2022**
5. *The Authorization Termination Date,* **March 10, 2023**
6. *The Risk Review Completion Date,* **February 28, 2022**

7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH).* **Moderate**

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

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).

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.

This system does not use any cloud technologies.

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)

This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

This system does not use any cloud technologies.

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.

This system does not use any cloud technologies.

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

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met?

This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

This system does not use any cloud technologies.

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).

This system does not use any cloud 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 provided in this Privacy Impact Assessment is true and accurate.

JULIE C. DRAKE 969177

Digitally signed by JULIE C. DRAKE 969177
Date: 2022.07.25 07:22:41 -06'00'

Privacy Officer, Julie Drake

Katherine Vollmer

Digitally signed by Katherine L. Vollmer 209764
Date: 2022.07.23 09:49:30 -06'00'

Information Systems Security Officer, Katherine Vollmer

Trimaine McFadden 117662

Digitally signed by Trimaine McFadden 117662
Date: 2022.07.24 16:15:22 -04'00'

Information System Owner, Trimaine McFadden

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).

System of Records Notice
1. VA SORN 24VA10A7/85 FR 62406 - Patient Medical Records-VA Patient Medical Records–VA. a. Effective Date: 10/02/2020
b. Link to Printed Version: 2020-21426.pdf (govinfo.gov)

2. VHA Handbook 1605.4 *Notice of Privacy Practices*, October 7, 2015 (https://vaww.va.gov/vhapublications/ViewPublication.asp?pub_ID=3147)