Privacy Impact Assessment for the VA IT System called:

Medical Device – Legacy Information Technology Environment (MD-LITE)

VA Office of Information Security (OIS) Specialized Device Cybersecurity Department (SDCD)

Veterans Health Administration (VHA)

eMASS ID # 2278

Date PIA submitted for review:

12/21/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Phillip Cauthers	Phillip.Cauthers@va.gov	503-721-1037
Information System Security Officer (ISSO)	George Quintela	George.Quintela@va.gov	727-412-5872
Information System Owner	Woodie Robinson	Woodie.Robinson@va.gov	202-288-4360
Data/Business/Information Owner[1]	Megan Friel	Megan.Friel@va.gov	202-384-3987
Data/Business/Information Owner	Connor Walsh	Connor.Walsh@va.gov	857-329-2818
Data/Business/Information Owner	Andrew Aiken	Andrew.Aiken2@va.gov	706-414-9641

Abstract

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

Medical Device-Legacy Information Technology Environment (MD-LITE) is a Platform-IT (PIT) system consisting of non-Cerner medical devices, and applicable components, hosted within Veterans Health Administration (VHA) Medical facilities. The MD-LITE PIT is comprised of medical assets spanning 136 Medical facilities. The system environment is comprised of medical devices/systems for diagnosis, treatment, or monitoring of physiological measurements, or for health analytical purposes, and has been subject to and completed the U.S. Food and Drug Administration's (FDA) Premarket Notification-- 510(k) certification—or Premarket Approval (PMA) Process. Examples of medical devices/systems include, but are not limited to, physiological monitoring systems, ventilators, infusion pumps, Computed Tomography (CT) scanners, MUSE™ cardiology information systems, Picture Archiving and Communication Systems (PACS), Clinical Information Systems (CIS), and laboratory analyzers. This includes medical devices/systems that directly connect to a patient, process human and other biologic specimens, create medical images, display electrophysiological waveforms, obtain physiologic measurements, and/or directly perform therapeutic support to the patient. These devices/systems cannot be managed using a Veterans Affairs (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 and Technology (OIT)-management via System Center Configuration

[1] VA DIRECTIVE 6508: System Steward/Data Owners - Work with the POs, Program Managers, Project Managers, ISOs, System Managers, and System Developers to ensure that appropriate privacy protections related to data sensitivity are in place and indicated in their PIA submissions; Serve as point of contact for questions related to system data; Respond to questions from POs, Program Managers, Project Managers, ISOs, System Managers, and System Developers that are related to the PA submission.

Manager (SCCM), BigFix). MD-LITE relies on the Veterans Affairs Enterprise Network (VAEN) Platform to provide the networking backbone for connectivity as well as all support systems that require network transport to function.

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?
Medical Device – Legacy Information Technology Environment (MD-LITE).

The VA program office system owner is the Office of Information Security (OIS) Specialized Device Cybersecurity Department (SDCD) in conjunction with the VHA Healthcare Technology Management (HTM) Program Office.

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

The Enterprise Medical Device Legacy Information Technology Environment (MD-LITE) establishes a baseline of the VA medical devices/systems for diagnosis, treatment, or monitoring of physiological measurements or for health analytical purposes towards achieving VHA's Mission to "Honor America's Veterans by providing exceptional health care that improves their health and well-being".

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

SDCD is responsible for the MD-LITE ATO boundary, and the medical devices are owned by VHA. MD-LITE is 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?

50,000 Estimate derived from Veteran's patient records. Users include Contractors and VA Personnel (Employees and Volunteers).

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

MD-LITE may collect health information on Veterans which will include Social Security Numbers, Name, Address, and Medical Records, as well as other information listed in question 1.1 for the purpose of better serving the Veteran's healthcare.

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

Information will be shared internally with Veterans Health Information Systems and Technology Architecture (VistA) and further information can be found in question 4.1. MD-LITE shares data with VistA and defers to VistA for data handling and retention. Additionally, information will be shared externally with Abbott Laboratories, Inc., Accuray Inc., Phillips Healthtech, CareFusion LLC. and other external entities as listed in section 5.1 of this PIA. MD-LITE resides within the Medical Device Isolation Architecture (MDIA) consisting of continuously monitored protected Virtual Local Area Networks (VLANs) and Access Control Lists (ACLs).

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?

All VHA medical devices are held to Medical Device Protection and Security Program policies and procedures to ensure the Confidentiality, Integrity, and Availability (CIA Triad) of medical system data is preserved. The Medical Device Protection and Security Program is an internal VA program owned by HTM in collaboration with SDCD in establishing a resource community regarding medical device security and procedures needed to help safely and securely maintain medical equipment throughout the equipment lifecycle. MD-LITE operates in 136 Area sites in accordance with approved configuration, administration and maintenance defined in each documented Enterprise Risk Analysis (ERA), which is a residual risk determination for all network-connected medical devices prior to implementation on the VA network. Legacy devices (those without an existing ERA) are being evaluated as their lifecycles permit. Legacy devices still adhere to the same policies, procedures, and security controls as those devices with an ERA. HTM provides onsite Biomedical support to perform the day-to-day activities, maintenance, and management of the MD-LITE medical devices in accordance with the Medical Device Protection and Security Program.

3. Legal Authority and SORN

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

System of Record Notices (SORN) 24VA10A7/85 FR 62406 “Patient Medical Records-VA" https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf. Authority for maintenance of the record: Title 38, United States Code, Sections 501(b) and 304.

SORN 79VA10/85 FR 84114 Veterans Health Information Systems and Technology Architecture (VistA) Records-VA https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf. Authority for maintenance of the system: Title 38, United States Code, Section 7301(a).

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 SORNS do not require amendment to accommodate MD-LITE.

4. System Changes

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

No changes to the business process are expected.

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

No technology changes are expected.

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[2]

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

☐ 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: <<Add Additional Information Collected but Not Listed Above Here (For Example, A Personal Phone Number That Is Used as A Business Number)>>

- *Patient First and Last Name*
- *Patient ID*
- *Addresses*
- *Telephone Numbers*
- *Demographics*
- *Primary Contact*
- *Sex*
- *Height*
- *Weight*
- *Blood Type*
- *Disabilities*
- *Diagnosis*
- *Designated User (DUZ) Number*
- *Username*
- *Provider Orders*
- *Physician/ Nurse Histories*
- *Physicals*
- *Shoe size*
- *Treatment Notes*
- *Treatment Plans*
- *Progress Notes/ Assessments*
- *Laboratory Results*
- *Test Results*
- *Admission/ Discharge Information*
- *Prescribed Medications/Medication Lists*
- *Pharmacy*
- *Prescription information (drug, strength, quantity, dosage form)*
- *Prescription Number*
- *National Drug Code (NDC) number*
- *Health Insurance*

- *Imaging*
- *Computerized Tomography (CT)*
- *Waveforms*
- *Electronic Data Interchange Personnel Identifier (EDIPI)*
- *'Problem lists' of on-going persistent medical needs*
- *Account Numbers*
- *VA Facility Code*
- *Sample ID*
- *Instrument/ System Logs*
- *Remote diagnostics, maintenance, monitoring, and repair*
- *Accession Number*
- *Study Dates/ Times*
- *Specimen Source*

PII Mapping of Components (Servers/Database)

MD-LITE consists of **27** key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by MD-LITE and the reasons for the collection of the PII are in the table below.

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

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection / Storage of PII	Safeguards
AccuCheck 360 [Internal Database (DB)]	**Yes**	**Yes**	•Demographics • Patient First and Last Name • Social Security Number • Date of Birth • Gender • Race/ Ethnicity • Medical record • Electronic Data Interchange Personnel Identifier (EDIPI)	Provide direct treatment, diagnostics and monitoring of patients	Medical Device Isolation Architecture (MDIA) and Access Control List (ACL) on ports and protocols to limit communication outside of Virtual Local Area Network (VLAN) to protect Access Control, Audit and Accountability, Configuration

			• Designated User (DUZ) Number		Management, and System and Information Integrity
OmniCenter (Internal DB)	**Yes**	**Yes**	• Patient First and Last Name • Social Security Number • Date of Birth • Gender • Medication Lists • EDIPI	Provide direct treatment, diagnostics, and monitoring of patients	MDIA and ACLs on ports and protocols to limit communication outside of VLAN to protect Access Control, Audit and Accountability, Configuration Management, and System and Information Integrity
INFUSION CONTROLLERS (Internal DB)	**Yes**	**Yes**	• Patient First and Last Name • Social Security Number • Date of Birth • Gender • Medication Lists • EDIPI	Provide direct treatment, diagnostics and monitoring of patients	MDIA and ACLs on ports and protocols to limit communication outside of VLAN to protect Access Control, Audit and Accountability, Configuration Management, and System and Information Integrity
MONITORS: PHYSIO: VITAL SIGNS (Internal DB)	**Yes**	**Yes**	• Patient First and Last Name • Social Security Number • Date of Birth • Gender • Medication Lists	Provide direct treatment, diagnostics and monitoring of patients	MDIA and ACLs on ports and protocols to limit communication outside of VLAN to protect Access Control, Audit and Accountability, Configuration Management, and System and Information Integrity
AUTOMATION SYSTEMS: MEDICATION DISPENSING (Internal DB)	**Yes**	**Yes**	• Patient First and Last Name • Social Security Number	Provide direct treatment,	MDIA and ACLs on ports and protocols to limit

			• Date of Birth • Gender • Medication Lists • Pharmacy • Treatment Notes • EDIPI • DUZ	diagnostics and monitoring of patients	communication outside of VLAN to protect Access Control, Audit and Accountability, Configuration Management, and System and Information Integrity
ELECTROCARDIOGRAPHS (Internal DB)	**Yes**	**Yes**	• Patient First and Last Name • Social Security Number • Date of Birth • Gender • Medication Lists	Provide direct treatment, diagnostics and monitoring of patients	MDIA and ACLs on ports and protocols to limit communication outside of VLAN to protect Access Control, Audit and Accountability, Configuration Management, and System and Information Integrity
INFORMATION SYSTEMS: DATA MGMT: CLINICAL PHARM (Internal DB)	**Yes**	**Yes**	• Patient First and Last Name • Social Security Number • Date of Birth • Gender • Medication Lists • Pharmacy • EDIPI • DUZ	Provide direct treatment, diagnostics and monitoring of patients	MDIA and ACLs on ports and protocols to limit communication outside of VLAN to protect Access Control, Audit and Accountability, Configuration Management, and System and Information Integrity
INFORMATION SYSTEMS: PACS: RADIOLOGY (Internal DB)	**Yes**	**Yes**	• Patient First and Last Name • Social Security Number • Date of Birth • Gender • Medication Lists • Imaging	Provide direct treatment, diagnostics and monitoring of patients	MDIA and ACLs on ports and protocols to limit communication outside of VLAN to protect Access Control, Audit and Accountability, Configuration Management, and

					System and Information Integrity
INFORMATION SYSTEMS: DATA MGMT: BEDSIDE (Internal DB)	**Yes**	**Yes**	• Patient First and Last Name • Social Security Number • Date of Birth • Gender • Medication Lists • Next of Kin • Emergency Contact • Primary Contact • DUZ • 'Problem Lists' of on-going persistent medical needs	Provide direct treatment, diagnostics and monitoring of patients	MDIA and ACLs on ports and protocols to limit communication outside of VLAN to protect Access Control, Audit and Accountability, Configuration Management, and System and Information Integrity
ANALYZERS: POC: BLOOD: GLUCOSE (Internal DB)	**Yes**	**Yes**	• Patient First and Last Name • Social Security Number • Date of Birth • Gender • Medication Lists • DUZ	Provide direct treatment, diagnostics and monitoring of patients	MDIA and ACLs on ports and protocols to limit communication outside of VLAN to protect Access Control, Audit and Accountability, Configuration Management, and System and Information Integrity
DATA INTERFACE SYSTEMS: MEDICAL (Internal DB)	**Yes**	**Yes**	• Patient First and Last Name • Social Security Number • Date of Birth • Gender • Medication Lists • EDIPI • DUZ • 'Problem Lists' of on-going persistent medical needs	Provide direct treatment, diagnostics and monitoring of patients	MDIA and ACLs on ports and protocols to limit communication outside of VLAN to protect Access Control, Audit and Accountability, Configuration Management, and System and Information Integrity

INFORMATION SYSTEMS: DATA MGMT: ANESTHESIA (Internal DB)	**Yes**	**Yes**	• Patient First and Last Name • Social Security Number • Date of Birth • Gender • Medication Lists	Provide direct treatment, diagnostics and monitoring of patients	MDIA and ACLs on ports and protocols to limit communication outside of VLAN to protect Access Control, Audit and Accountability, Configuration Management, and System and Information Integrity
SOFTWARE: IMAGE MANAGEMENT (Internal DB)	**Yes**	**Yes**	• Patient First and Last Name • Social Security Number • Date of Birth • Gender • Medication Lists • Imaging	Provide direct treatment, diagnostics and monitoring of patients	MDIA and ACLs on ports and protocols to limit communication outside of VLAN to protect Access Control, Audit and Accountability, Configuration Management, and System and Information Integrity
INFORMATION SYSTEMS: PACS (Internal DB)	**Yes**	**Yes**	• Patient First and Last Name • Social Security Number • Date of Birth • Gender • Medication Lists	Provide direct treatment, diagnostics and monitoring of patients	MDIA and ACLs on ports and protocols to limit communication outside of VLAN to protect Access Control, Audit and Accountability, Configuration Management, and System and Information Integrity
MONITORS: PHYSIO: BEDSIDE (Internal DB)	**Yes**	**Yes**	• Patient First and Last Name • Social Security Number • Date of Birth • Gender • Medication Lists	Provide direct treatment, diagnostics and monitoring of patients	MDIA and ACLs on ports and protocols to limit communication outside of VLAN to protect Access Control, Audit and

			• DUZ • 'Problem Lists' of on-going persistent medical needs		Accountability, Configuration Management, and System and Information Integrity
INFORMATION SYSTEMS: DATA MGMT: CARDIOLOGY (Internal DB)	**Yes**	**Yes**	• Patient First and Last Name • Social Security Number • Date of Birth • Gender • Medication Lists	Provide direct treatment, diagnostics and monitoring of patients	MDIA and ACLs on ports and protocols to limit communication outside of VLAN to protect Access Control, Audit and Accountability, Configuration Management, and System and Information Integrity
CAMERAS: SURVEILLANCE (Internal DB)	**Yes**	**Yes**	• Patient First and Last Name • Social Security Number • Date of Birth • Gender • Medication Lists	Provide direct treatment, diagnostics and monitoring of patients	MDIA and ACLs on ports and protocols to limit communication outside of VLAN to protect Access Control, Audit and Accountability, Configuration Management, and System and Information Integrity
DEFIBRILLATORS (Internal DB)	**Yes**	**Yes**	• Patient First and Last Name • Social Security Number • Date of Birth • Gender • Medication Lists	Provide direct treatment, diagnostics and monitoring of patients	MDIA and ACLs on ports and protocols to limit communication outside of VLAN to protect Access Control, Audit and Accountability, Configuration Management, and System and Information Integrity

INFORMATION SYSTEMS: PACS: CARDIOLOGY (Internal DB)	**Yes**	**Yes**	• Patient First and Last Name • Social Security Number • Date of Birth • Gender • Medication Lists	Provide direct treatment, diagnostics and monitoring of patients	MDIA and ACLs on ports and protocols to limit communication outside of VLAN to protect Access Control, Audit and Accountability, Configuration Management, and System and Information Integrity
DATA INTERFACE UNITS: MEDICAL (Internal DB)	**Yes**	**Yes**	• Patient First and Last Name • Social Security Number • Date of Birth • Gender • Medication Lists • EDIPI • 'Problem Lists' of on-going persistent medical needs	Provide direct treatment, diagnostics and monitoring of patients	MDIA and ACLs on ports and protocols to limit communication outside of VLAN to protect Access Control, Audit and Accountability, Configuration Management, and System and Information Integrity
INFORMATION SYSTEMS: PACS: DENTAL (Internal DB)	**Yes**	**Yes**	• Patient First and Last Name • Social Security Number • Date of Birth • Gender • Medication Lists • Health Insurance • EDIPI	Provide direct treatment, diagnostics and monitoring of patients	MDIA and ACLs on ports and protocols to limit communication outside of VLAN to protect Access Control, Audit and Accountability, Configuration Management, and System and Information Integrity
SCANNING SYSTEMS: ULTRASONIC (Internal DB)	**Yes**	**Yes**	• Patient First and Last Name • Social Security Number • Date of Birth • Gender • Medication Lists	Provide direct treatment, diagnostics and monitoring of patients	MDIA and ACLs on ports and protocols to limit communication outside of VLAN to protect Access Control, Audit and Accountability,

					Configuration Management, and System and Information Integrity
NETWORK INFRASTRUCTURE: SERVER PLATFORM: MEDICAL (Internal DB)	**Yes**	**Yes**	• Patient First and Last Name • Social Security Number • Date of Birth • Gender • Medication Lists • EDIPI	Provide direct treatment, diagnostics and monitoring of patients	MDIA and ACLs on ports and protocols to limit communication outside of VLAN to protect Access Control, Audit and Accountability, Configuration Management, and System and Information Integrity
SOFTWARE: PHYSIO MONITORING: VITAL SIGNS (Internal DB)	**Yes**	**Yes**	• Patient First and Last Name • Social Security Number • Date of Birth • Gender • Medication Lists	Provide direct treatment, diagnostics and monitoring of patients	MDIA and ACLs on ports and protocols to limit communication outside of VLAN to protect Access Control, Audit and Accountability, Configuration Management, and System and Information Integrity
CAMERAS: PHOTOGRAPHIC: OPHTHALMIC: FUNDUS (Internal DB)	**Yes**	**Yes**	• Patient First and Last Name • Social Security Number • Date of Birth • Gender • Medication Lists	Provide direct treatment, diagnostics and monitoring of patients	MDIA and ACLs on ports and protocols to limit communication outside of VLAN to protect Access Control, Audit and Accountability, Configuration Management, and System and Information Integrity
INFORMATION SYSTEMS: DATA MGMT:	**Yes**	**Yes**	• Patient First and Last Name • Email	Provide direct treatment,	MDIA and ACLs on ports and protocols to limit

PERIOPERATIVE (Internal DB)			• Fax • Next of Kin • Emergency Contact • Primary Contact • Social Security Number • Date of Birth • Gender • Medication Lists	diagnostics and monitoring of patients	communication outside of VLAN to protect Access Control, Audit and Accountability, Configuration Management, and System and Information Integrity
ANALYZERS: POC: BLOOD: MULTIANALYTE (Internal DB)	**Yes**	**Yes**	• Patient First and Last Name • Social Security Number • Date of Birth • Gender • Medication Lists	Provide direct treatment, diagnostics and monitoring of patients	MDIA and ACLs on ports and protocols to limit communication outside of VLAN to protect Access Control, Audit and Accountability, Configuration Management, and System and Information Integrity

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?

MD-LITE can collect and receive data from VistA/ Computerized Patient Record System (CPRS) via Health Level Seven (HL7) messaging or Digital Imaging and Communications in Medicine (DICOM), or by manual entry from the patient record. A holistic approach is used to gather data from any of the listed DBs in table 1.1, VistA, or directly from the VA patient to allow the healthcare provider to understand the entire situation for proper diagnosis and treatment.

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.

MD-LITE can collect and receive data from VistA/CPRS via HL7 messaging or DICOM, or by manual entry from the patient record to assess the VA patient's health. A holistic approach is used to gather data from any of the listed DBs in table 1.1, VistA, or directly from the VA patient to allow the healthcare provider to understand the entire situation for proper diagnosis and treatment.

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

MD-LITE can collect and receive data from VistA/CPRS via HL7 messaging or DICOM, or by manual entry from the patient record. Information can also be collected directly from the VA patient to create information. VA staff can create diagnosis and treatment plans. There are also medical devices within MD-LITE that can collect, receive, and/or create data, such as imaging machines and Electrocardiograms (EKGs).

1.3 How is the information collected?

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

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

Information is electronically collected via transfer (HL7 messaging transmission) from VistA/CPRS, DICOM, non-DICOM image, as well as by manual entry by the clinical staff into the medical device. Information collected from individuals is collected verbally in interviews and conversations with VA medical and administrative staff, and via electronic and web form submissions. A holistic approach is used to gather data from any of the listed DBs in table 1.1, VistA, or directly from the VA patient to allow the healthcare provider to understand the entire situation for proper diagnosis and treatment. Please review the Area PIAs for facility specific collection methods. https://www.oprm.va.gov/privacy/pia.aspx.

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?

MD-LITE does not collect information in paper form. Information is collected electronically via transfer (HL7 messaging transmission) from VistA/CPRS, DICOM, non-DICOM image, and by manual entry by the clinical staff into the medical device. The use of electronic transmission of data, automated systems, and electronic forms are used to reduce and control the paperwork burden.

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.

MD-LITE 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. Information obtained directly from the individual will be assumed to be accurate. Furthermore, individuals have the right to obtain access to their records and request correction to them when necessary. Please review the individual PIAs for area specific information about information accuracy. https://www.privacy.va.gov/privacy_impact_assessment.asp

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?

MD-LITE 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. There is no known commercial aggregator used.

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

MD-LITE operates under the following system authority:

- SORN 24VA10A7/85 FR 62406 "Patient Medical Records-VA" https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf. Authority for maintenance of the record: Title 38, United States Code, Sections 501(b) and 304.
- SORN 79VA10/85 FR 84114 Veterans Health Information Systems and Technology Architecture (VistA) Records-VA https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf. Title 38, United States Code, Section 7301(a).
- Title 38, United States Code (U.S.C.), Chapter 3, Department of Veterans Affairs.
- Title 38, U.S.C., Chapter 5, Authority and Duties of the Secretary.
- Title 38, U.S.C., Chapter 73, Veterans Health Administration (VHA) – Organization and Functions.
- Privacy Act of 1974 Freedom of Information Act (FOIA) 5 U.S.C. 552.
- Health Insurance Portability and Accountability Act of 1996 (HIPAA).

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: 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 the data collected, there is a risk that, if the data were accessed by an unauthorized individual, accidentally released, or breached, personal and/or emotional harm to the VA patient may result.

Mitigation: 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 Health Level Seven (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 Health Level Seven (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. PII taken directly from VistA/CPRS, DICOM, non-DICOM image, or by manual entry by the clinical staff into the medical device 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 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	Identification Purposes	Identification Purposes
Social Security	Identification Purposes	Identification Purposes
Date of Birth	Identification Purposes	Identification Purposes
Mother's Maiden Name	Identification Purposes	Identification Purposes
Personal Mailing Address	Identification/Equipment delivery purpose	Identification/Equipment delivery purpose
Personal Phone	Communication Purposes	Communication Purposes
Personal Fax Number	Communication Purposes	Communication Purposes
Personal Email	Communication Purposes	Communication Purposes
Emergency Contact Information	Communication Purposes	Communication Purposes
Internet Protocol	Maintenance, Monitoring, Repair	Maintenance, Monitoring, Repair
Medications	Treatment Purposes	Treatment Purposes
Medical Records	Treatment Purposes	Treatment Purposes
Race/Ethnicity	Identification Purposes	Identification Purposes
Tax Identification Number	Identification Purposes	Identification Purposes
Medical Records Number	File Identification Purposes	File Identification Purposes
Gender	Identification Purposes	Identification Purposes
Next of Kin	Communication Purposes	Communication Purposes

The MD-LITE system boundary is comprised of facility level instances. Due to the extensive amount and nature of the information contained at each facility which can determine what information to collect, process, retain, or disseminate, a full understanding of the purpose for each individual data point can be obtained by reviewing the facility-level Privacy Impact Assessment. https://www.oprm.va.gov/privacy/pia.aspx

The records and information may be used for statistical analysis to produce various management, workload tracking and follow-up reports; to track and evaluate the ordering and delivery of equipment, services, and patient care; the planning, distribution, and utilization of resources; the possession and use of equipment or supplies; the performance of vendors,

equipment, and employees; and to provide clinical and administrative support to patient medical care.

The data may be used for such purposes as assisting in job assignments of employees; the scheduling of patient treatment services, including nursing care, clinic appointments, surgery, diagnostic and therapeutic procedures; the repair and maintenance of equipment and for follow-up activities to determine that the actions were accomplished and to evaluate the results; to plan, schedule, and maintain rosters of patients, employees and others attending or participating in sports, recreational or other events (e.g., National Wheelchair Games, concerts, picnics); for audits, reviews and investigations conducted by staff of the health care facility, the Network Directors Office, VA Central Office, and the VA Office of Inspector General (OIG); for quality assurance audits, reviews, investigations and inspections; for law enforcement investigations; and for personnel management, evaluation and employee ratings, and performance evaluations.

Data element types collected include Personal Information, Healthcare Information for Treatment, VA Staff Information, and System Information. List of these data elements are below:

Personal Information Identifiers

Name, Patient First and Last Name, Patient ID, Social Security Number (SSN), Date of Birth (DoB), Personal Fax Number, Personal Email, Personal Mailing Address, Addresses, Demographics, Race/Ethnicity, Gender, Sex, Next of Kin, Telephone Numbers, Height, Weight, Primary Contact, Emergency Contact, Blood Type, and Shoe size.

Healthcare Information for Treatment

Account Numbers, Medical Records, Medical Record Number, Disabilities, Diagnosis, Treatment Notes, Treatment Plans, Medications, Prescribed Medications, Medication Lists, Pharmacy, Prescription information (drug, strength, quantity, dosage form), Prescription Number, National Drug Code (NDC) number, Health Insurance, Physician/ Nurse Histories, Physicals, Imaging, Computerized Tomography (CT), Waveforms, Provider Orders, Progress Notes/Assessments, Admission/Discharge Information, Laboratory Results, Test Results, 'Problem Lists' of on-going persistent medical needs, Specimen Source, Study Dates/Times, and Electronic Data Interchange Personnel Identifier (EDIPI).

VA Staff Information

Accession Number, Username, and Designated User (DUZ) Number

System Information

Internet Protocol (IP) Address Numbers, Instrument/ System Logs, Remote diagnostics, Maintenance, Monitoring, Repair, VA Facility Code, and Sample ID

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?

MD-LITE 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. Information is sent and received by medical devices/systems in the forms of health information, and then sent back to VistA/CPRS via (HL7) messaging or (DICOM), for clinicians to use in patient monitoring, management, diagnosis, and treatment of Veterans. MD-LITE medical devices can analyze data and provide recommendations. However, the VA Staff will accept or reject any data analysis provided by MD-LITE medical devices based on their judgment.

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.

MD-LITE 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. This information is sent and received by medical devices/systems in the forms of health information, and then sent back to VistA/CPRS via (HL7) messaging or (DICOM), 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. Therefore, yes, MD-LITE can create new records based on the medical device recommendations and those records will be accessible by those VA Staff with the need to know.

2.3 How is the information in the system secured?

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

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

MD-LITE is comprised of medical systems that utilize approved encryption technologies for data in transit in bi-directional traffic flows between medical desktop/laptops, servers, medical system components, and related telecommunication devices both locally (LAN) and remotely (VA WAN), when possible. Communication requirements (i.e., ports, protocols, services) are learned during the ERA process. Medical Devices/Systems are deployed within VLANs, and ACLs configured to explicitly allow the required Ports, protocols, and Services (PPS) for device/system communication. ERA process ensures data at rest encryption technologies are documented for each approved medical system, where applicable. However, the majority of medical devices within MD-LITE do not have the technology in place for encryption of data. Therefore, a Plan of Actions and Milestones (POAM) will document the planned recommendations.

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

MD-LITE requires each Area to document deviations from approved processes and uses of medical systems. Please refer to the facility-level Privacy Impact Assessment for the handling of SSNs during the collecting, processing, or retaining of SSNs locally.
https://www.oprm.va.gov/privacy/pia.aspx

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

MD-LITE requires each Area to comply with all OMB Memorandum M-06.15 mandates in accordance with the Privacy controls deemed applicable to medical systems by MD-LITE Information System Owner and approved by VA Senor Authorizing Official. Please refer to the facility-level Privacy Impact Assessment for the PII/PHI safeguards in place at the local facility. https://www.oprm.va.gov/privacy/pia.aspx.

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?

MD-LITE requires each Area to document how access to PII is determined. 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. MD-LITE is restricted to personnel with VA Privacy and Information Security Awareness and Rules of Behavior, and Privacy and HIPAA training, certified annually via the Training Management System (TMS). The access control procedures are with the supervisor or designee requesting access, thus providing the approval for the clinical staff to the VistA/CPRS 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 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. Please refer to the facility-level Privacy Impact Assessment for local guidance on PII access. https://www.oprm.va.gov/privacy/pia.aspx.

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

MD-LITE requires each Area to document all criteria, procedures, controls, and responsibilities relevant to access to PII. Please refer to the facility-level Privacy Impact Assessment for local guidance on PII criteria, procedures, controls, and responsibilities. https://www.oprm.va.gov/privacy/pia.aspx.

2.4c Does access require manager approval?

MD-LITE requires each Area to document where access requires manager approval. Please refer to the facility-level Privacy Impact Assessment for local guidance on whether access requires manager approval. https://www.oprm.va.gov/privacy/pia.aspx.

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

MD-LITE requires each Area to document how access to PII is monitored, tracked, and recorded. Please refer to the facility-level Privacy Impact Assessment for local guidance for

information regarding whether the access to PII is being monitored, tracked, and recorded. https://www.oprm.va.gov/privacy/pia.aspx.

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

MD-LITE requires that all VA Staff, or those otherwise with access to any PII or PHI stored, collected, or accessed by MD-LITE systems, are trained and aware that all VA personnel are responsible for assuring PII is safeguarded. Please refer to the facility-level Privacy Impact Assessment for local guidance for information regarding the responsibility assuring safeguards for PII. https://www.oprm.va.gov/privacy/pia.aspx.

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*

Personal Information Identifiers

Name, Patient First and Last Name, Patient ID, SSN, DoB, Personal Fax Number, Personal Email, Personal Mailing Address, Addresses, Demographics, Race/Ethnicity, Gender, Sex, Next of Kin, Telephone Numbers, Height, Weight, Primary Contact, Emergency Contact, Blood Type, and Shoe size.

Healthcare Information for Treatment

Account Numbers, Medical Records, Medical Record Number, Disabilities, Diagnosis, Treatment Notes, Treatment Plans, Medications, Prescribed Medications, Medication Lists, Pharmacy, Prescription information (drug, strength, quantity, dosage form), Prescription Number, NDC number, Health Insurance, Physician/ Nurse Histories, Physicals, Imaging, CT, Waveforms, Provider Orders, Progress Notes/Assessments, Admission/Discharge Information, Laboratory Results, Test Results, 'Problem Lists' of on-going persistent medical needs, Specimen Source, Study Dates/Times, and EDIPI.

VA Staff Information

Accession Number, Username, and DUZ Number.

System Information

IP Address Numbers, Instrument/ System Logs, Remote diagnostics, Maintenance, Monitoring, Repair, VA Facility Code, and Sample ID.

3.2 How long is information retained?

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

All information is temporarily retained for reporting purposes, depending on the medical device/system. As stated in the Records Control Schedule, RCS 10-1, Chapter Six – Healthcare Records, 6000.2 Electronic Health Record (EHR), https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf

MD-LITE retains medical information in accordance with RCS 10-1, Part Three, Chapter Six-Healthcare Records, Item 6000.2a(2), Interim Electronic Source Information, which states "Temporary electronic source or output information can be deleted after migration to another electronic medium or when no longer needed for administrative or clinical operations." Once information from MD-LITE has been migrated to the Patient Medical Records it is retained there for a total of 75 years after the last episode of care. (Department of Veterans Affairs Record Control Schedule (RCS)10-1, Part Three, Chapter Six-Healthcare Records, Item 6000.1a and 6000.1d).

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?

MD-LITE Medical systems with system of records, the records are stored within the approved disposition authority. All information is temporarily retained for reporting purposes back to the patient's medical record. 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 Link - https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf.

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

Patient medical information is retained by MD-LITE under VA Records Control Schedule, item 6000.2a(2) with disposition authority N1-15-02-3 item 2.

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.

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. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

MD-LITE 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. (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: There is a risk that information maintained by or within an Area implementation of a medical systems could be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released, breached, or exploited for reasons other than what is described in the privacy documentation associated with the information.

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. Please refer to sections 3.1 through 3.5 of this PIA as well as the facility-level Privacy Impact Assessment for applicable retention schedule and length. https://www.oprm.va.gov/privacy/pia.aspx.

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***
Veterans Health Information Systems and Technology Architecture (VistA)	Provide direct treatment, diagnostics and monitoring of patients	Name, Patient First and Last Name, Patient ID, Social Security Number, Date of Birth, Personal Fax Number, Personal Email, Personal Mailing Address, Addresses, Demographics, Race/Ethnicity, Gender, Sex, Blood Type, Next of Kin, Telephone Numbers, Height, Weight, Primary Contact, Emergency Contact, Account Numbers, Medications, Medical Records, Medical Record Number, Disabilities, Diagnosis, Treatment	CPRS via HL7 messaging

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*
		Notes, Treatment Plans, Test Results, Prescribed Medications/Medication Lists, Pharmacy, Health Insurance, Physician/ Nurse Histories, Physicals, Imaging, Computerized Tomography, Waveforms, Provider Orders, Progress Notes/Assessments, Admission/Discharge Information, Laboratory Results, 'Problem Lists' of on-going persistent medical needs, Specimen Source, Study Dates/Times, Accession Number, Username, Designated User Number, Electronic Data Interchange Personnel Identifier, Internet Protocol Address Numbers, Instrument/ System Logs, Remote diagnostics, Maintenance, Monitoring, Repair, VA Facility Code, Sample ID	

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

Follow the format below:

Privacy Risk: 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: Safeguards are implemented to ensure data is not inappropriately shared or accessed including employee security and privacy training and awareness and required reporting of suspicious activity. Additionally, use of role-based access control mechanisms, need-to-know determinations, secure passwords, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption of data-at-rest and in-transit, and monitoring of access authorization are all measures that are utilized within the facilities. Access to sensitive information and the systems where the information is stored is controlled by the VA using a "least privilege/need to know" policy. Access must be requested and only the access required by VA persons or processes acting on behalf of VA persons is to be requested or granted.

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	***List the purpose of informatio n being***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)wit h the Program or IT system***	***List the legal authority, binding***	***List the method of transmissio n and the***

shared/received with	***shared / received / transmitted with the specified program office or IT system***		***agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***measures in place to secure data***
Abbott Laboratories Inc.	Provide direct treatment, diagnostics and monitoring of patients	Internet Protocol (IP) Address Numbers, Instrument/ System Logs, Remote diagnostics, maintenance, monitoring, and repair	National MOU/ISA E-698	Site to Site (S2S) Virtual Private Network (VPN)
Abbott Laboratories Inc.	Provide direct treatment, diagnostics and monitoring of patients	IP Address Numbers, Instrument/ System Logs, Remote diagnostics, maintenance, monitoring, and repair	National MOU/ISA E-1874	Secure File Transfer Protocol (sFTP)
Abbott Rapid Diagnostics Informatics, Inc.	Provide direct treatment, diagnostics and monitoring of patients	IP Address Numbers, Instrument/ System Logs, Remote diagnostics, maintenance, monitoring, and repair	National MOU/ISA E-704	S2S VPN
Accuray Inc.	Provide direct treatment, diagnostics and monitoring of patients	Name, CT images, Treatment Plans, System logs	National MOU/ISA E-701	Secure Socket Layer (SSL)/ Transport Layer Security (TLS)
Philips Healthcare, a division of Philips North America LLC	Provide direct treatment, diagnostics and monitoring of patients	Name, Patient ID, Social Security Number (SSNs), Date of Birth (DOB), Height, Weight, Patient images, Remote diagnostics, maintenance, monitoring, and repair	National MOU/ISA E-789	S2S VPN
CareFusion, LLC (a Becton	Provide direct treatment,	Test results, Accession Number, Patient Name, DOB, SSN, Medical Record Number, Gender, Age,	National MOU/ISA E-715	SSL/ TLS

Dickson subsidiary)	diagnostics and monitoring of patients	Marital Status, Phone Numbers, Blood Type, Address, Patient ID, Admissions, Discharge, Pharmacy		
ScriptPro LLC & ScriptPro USA	Provide direct treatment, diagnostics and monitoring of patients	VA Facility Code, receiving facility address, assigning facility ID, ordering facility address, Patient ID, Name, SSN, Date of Birth	National MOU/ISA E-809	S2S VPN
OmniCell, Inc.	Provide direct treatment, diagnostics and monitoring of patients	Names, Address, Date of Birth, Admission date, Discharge date, telephone numbers, SSN, MRN, Account numbers	National MOU/ISA E-776	S2S VPN
Siemens Healthcare Diagnostics Inc / Siemens Medical Solutions Inc	Provide direct treatment, diagnostics and monitoring of patients	IP Address Numbers, Instrument/ System Logs, Remote diagnostics, maintenance, monitoring, and repair	National MOU/ISA E-812	S2S VPN
GE Healthcare	Provide direct treatment, diagnostics and monitoring of patients	Patient Name, Date of Birth (DOB), MRN, Images, Waveforms, Gender, System Maintenance, System Monitoring, and System Repair	National MOU/ISA E-742	S2S VPN
Varian Medical Systems Inc.	Provide direct treatment, diagnostics and monitoring of patients	IP Address Numbers, Instrument/ System Logs, Remote diagnostics, maintenance, monitoring, and repair	National MOU/ISA E-830	S2S VPN
Canon Medical Systems USA Inc	Provide direct treatment, diagnostics and monitoring of patients	IP Address Numbers, Instrument/ System Logs, Remote diagnostics, maintenance, monitoring, and repair	National MOU/ISA E-824	S2S VPN
CliniComp, Intl.	Provide direct treatment, diagnostics	Physician/nurse histories and physicals, Progress notes, Assessments, Treatment Plans, Admission data, Laboratory	National MOU/ISA E-728	S2S VPN

	and monitoring of patients	results, Medications, Treatments, Discharge, Patient Demographics		
Draeger Inc	Provide direct treatment, diagnostics and monitoring of patients	Medical Record Number	National MOU/ISA E-736	S2S VPN
Nuance Communications Inc	Provide direct treatment, diagnostics and monitoring of patients	Name, Address, Gender, Age, Date of Birth, Account Numbers, Diagnosis, Treatment	National MOU/ISA E-774	S2S VPN
Sysmex America, Inc	Provide direct treatment, diagnostics and monitoring of patients	Patient ID, Test Results	National MOU/ISA E- 818	S2S VPN
Agfa Healthcare Corporation and Agfa US Corp	Provide direct treatment, diagnostics and monitoring of patients	Imaging	National MOU/ISA E-703	S2S VPN
Roche Diagnostics	Provide direct treatment, diagnostics and monitoring of patients	Sample ID, Patient ID, Test Results	National MOU/ISA E-804	S2S VPN
Bayer HealthCare LLC	Provide direct treatment, diagnostics and monitoring of patients	Accession Number, Study Dates/Times, DOB, Gender, Height, Weight, MRN, SSN	National MOU/ISA E-713	S2S VPN
Quest Diagnostics	Provide direct treatment, diagnostics and	Patient Name, DOB, Sex, Patient ID, Accession number, VA Facility Code, Account number, Provider Orders, Specimen source	National MOU/ISA E-797	S2S VPN

	monitoring of patients			
Beckman Coulter Inc	Provide direct treatment, diagnostics and monitoring of patients	IP Address Numbers, Instrument/ System Logs, Remote diagnostics, maintenance, monitoring, and repair, Sample IDs, VA Facility Names	National MOU/ISA E-714	S2S VPN
Change Healthcare Technologies LLC	Provide direct treatment, diagnostics and monitoring of patients	Radiology imaging	National MOU/ISA E-2192	S2S VPN
Parata Systems	Provide direct treatment, diagnostics and monitoring of patients	System security, updates, robot monitoring and remote support	National MOU/ISA E-5225	SSL/ TLS
Carestream Health, Inc.	Provide direct treatment, diagnostics and monitoring of patients	IP Address Numbers, Instrument/ System Logs, Remote diagnostics, maintenance, monitoring, and repair	National MOU/ISA E-723	S2S VPN
Lifepoint	Provide direct treatment, diagnostics and monitoring of patients	Imaging, Test Results	National MOU/ISA E-2331	S2S VPN
AirStrip Technologies, Inc.	Provide direct treatment, diagnostics and monitoring of patients	IP Address Numbers, Instrument/ System Logs, Remote diagnostics, maintenance, monitoring, and repair	National MOU/ISA E-1589	S2S VPN
iRhythm Technologies, Inc.	Provide direct treatment, diagnostics and	Patient ID, Test Results, Diagnosis	National MOU/ISA E-2302	sFTP

	monitoring of patients			
MIM Software Inc.	Provide direct treatment, diagnostics and monitoring of patients	IP Address Numbers, Instrument/ System Logs, Remote diagnostics, maintenance, monitoring, and repair	National MOU/ISA E-769	S2S VPN
bioMérieux	Provide direct treatment, diagnostics and monitoring of patients	IP Address Numbers, Instrument/ System Logs, Remote diagnostics, maintenance, monitoring, and repair	National MOU/ISA E-716	S2S VPN
Spectrum Dynamics Medical Inc.	Provide direct treatment, diagnostics and monitoring of patients	IP Address Numbers, Instrument/ System Logs, Remote diagnostics, maintenance, monitoring, and repair	National MOU/ISA E-5233	S2S VPN
Spectrum Medical Inc	Provide direct treatment, diagnostics and monitoring of patients	IP Address Numbers, Instrument/ System Logs, Remote diagnostics, maintenance, monitoring, and repair	National MOU/ISA E-2179	S2S VPN
Spacelabs Healthcare	Provide direct treatment, diagnostics and monitoring of patients	IP Address Numbers, Instrument/ System Logs, Remote diagnostics, maintenance, monitoring, and repair	National MOU/ISA E-1570	SSL/TLS
Medicom Technologies Inc	Provide direct treatment, diagnostics and monitoring of patients	Imaging	National MOU/ISA E-2247	S2S VPN
Picis Clinical Solutions, Inc.	Provide direct treatment, diagnostics and	IP Address Numbers, Instrument/ System Logs, Remote diagnostics, maintenance, monitoring, and repair	National MOU/ISA E-791	S2S VPN

	monitoring of patients			
Asteres Inc.	Provide direct treatment, diagnostics and monitoring of patients	Patient name, DOB, Address, Phone numbers, Prescription information	National MOU/ISA E-711	S2S VPN
UTECH Products Inc.	Provide direct treatment, diagnostics and monitoring of patients	IP Address Numbers, Instrument/ System Logs, Remote diagnostics, maintenance, monitoring, and repair	National MOU/ISA E-827	S2S VPN
Elekta, Inc.	Provide direct treatment, diagnostics and monitoring of patients	IP Address Numbers, Instrument/ System Logs, Remote diagnostics, maintenance, monitoring, and repair	National MOU/ISA E-738	S2S VPN
Apollo Enterprise Imaging Corp (formerly Apollo PACS Inc.)	Provide direct treatment, diagnostics and monitoring of patients	Imaging	National MOU/ISA E-708	S2S VPN
Sorna Corporation	Provide direct treatment, diagnostics and monitoring of patients	IP Address Numbers, Instrument/ System Logs, Remote diagnostics, maintenance, monitoring, and repair, Patient Name, Patient ID, SSN, DOB	National MOU/ISA E-815	S2S VPN
Ortho Clinical Diagnostics, Inc.	Provide direct treatment, diagnostics and monitoring of patients	IP Address Numbers, Instrument/ System Logs, Remote diagnostics, maintenance, monitoring, and repair	National MOU/ISA E-782	S2S VPN
PedAlign Holdings, Inc.	Provide direct treatment, diagnostics and	Patient name, Weight, Shoe size, Imaging	National MOU/ISA E-786	S2S VPN

	monitoring of patients			
GSL Solutions, Inc.	Provide direct treatment, diagnostics and monitoring of patients	Patient ID, Name, DOB, Gender, Address, Prescription information (drug, strength, quantity, dosage form), National Drug Code (NDC) number, Pharmacy, Prescription number	National MOU/ISA E-749	S2S VPN
Intelerad Medical Systems Inc.	Provide direct treatment, diagnostics and monitoring of patients	IP Address Numbers, Instrument/ System Logs, Remote diagnostics, maintenance, monitoring, and repair, MRN, Patient Name, DOB	National MOU/ISA E-759	S2S VPN
Radiometer America, Inc.	Provide direct treatment, diagnostics and monitoring of patients	IP Address Numbers, Instrument/ System Logs, Remote diagnostics, maintenance, monitoring, and repair	National MOU/ISA E-798	S2S VPN
HillRom (Welch-Allyn)	Provide direct treatment, diagnostics and monitoring of patients	IP Address Numbers, Instrument/ System Logs, Remote diagnostics, maintenance, monitoring, and repair	National MOU/ISA E-835	S2S VPN
Hill-Rom Company, Inc.	Provide direct treatment, diagnostics and monitoring of patients	IP Address Numbers, Instrument/ System Logs, Remote diagnostics, maintenance, monitoring, and repair	National MOU/ISA E-752	S2S VPN
Barco Inc.	Provide direct treatment, diagnostics and monitoring of patients	IP Address Numbers, Instrument/ System Logs, Remote diagnostics, maintenance, monitoring, and repair	National MOU/ISA E-712	S2S VPN
Merge, an IBM Company	Provide direct treatment, diagnostics and	IP Address Numbers, Instrument/ System Logs, Remote diagnostics, maintenance, monitoring, and repair, Imaging, Waveform data, Treatment Plans	National MOU/ISA E-767	S2S VPN

	monitoring of patients			
Diagnostica Stago Inc.	Provide direct treatment, diagnostics and monitoring of patients	IP Address Numbers, Instrument/ System Logs, Remote diagnostics, maintenance, monitoring, and repair	National MOU/ISA E-2326	SSL/TLS
Intuitive Surgical, Inc.	Provide direct treatment, diagnostics and monitoring of patients	First and Last Names, Email addresses	National MOU/ISA E-760	SSL/TLS
ARxIUM, Inc.	Provide direct treatment, diagnostics and monitoring of patients	Name, SSN, DOB, Prescription, Pharmacy	National MOU/ISA E-710	S2S VPN
Immucor Inc.	Provide direct treatment, diagnostics and monitoring of patients	IP Address Numbers, Instrument/ System Logs, Remote diagnostics, maintenance, monitoring, and repair	National MOU/ISA E-1665	SSL/TLS
Riverain Technologies	Provide direct treatment, diagnostics and monitoring of patients	IP Address Numbers, Instrument/ System Logs, Remote diagnostics, maintenance, monitoring, and repair	National MOU/ISA E-2089	S2S VPN
Sun Nuclear Corporation	Provide direct treatment, diagnostics and monitoring of patients	IP Address Numbers, Instrument/ System Logs, Remote diagnostics, maintenance, monitoring, and repair, Treatment Plans	National MOU/ISA E-1535	S2S VPN
RGI Informatics, LLC	Provide direct treatment, diagnostics and	IP Address Numbers, Instrument/ System Logs, Remote diagnostics, maintenance, monitoring, and repair	National MOU/ISA E-802	S2S VPN

	monitoring of patients			
Hitachi Medical Systems America, Inc	Provide direct treatment, diagnostics and monitoring of patients	IP Address Numbers, Instrument/ System Logs, Remote diagnostics, maintenance, monitoring, and repair	National MOU/ISA E-753	SSL/TLS
Biocartis US Inc.	Provide direct treatment, diagnostics and monitoring of patients	IP Address Numbers, application updates and Patches, anonymized information to include exam type, dosage used, and machine type.	National MOU/ISA E-2320	SSL/TLS
PHS Technologies Group, LLC	Provide direct treatment, diagnostics and monitoring of patients	IP Address Numbers, application updates and Patches, anonymized information to include exam type, dosage used, and machine type.	National MOU/ISA E-783	SSL/TLS
eVideon Inc. (Optimal Solutions, Inc.)	Provide direct treatment, diagnostics and monitoring of patients	IP Address, movies and patient education videos, image files, software updates and patches	National MOU/ISA E-780	S2S VPN
InVita Healthcare Technologies (Champion Healthcare/Terso)	Provide direct treatment, diagnostics and monitoring of patients	IP Address, patient identifier (first initial and last 4 of SSN), DOB, procedure and implant/device information, RFID Tag Numbers	National MOU/ISA E-727	S2S VPN
Vital Images, Inc	Provide direct treatment, diagnostics and monitoring of patients	IP Address Numbers, de-identified images and datasets, software updates	National MOU/ISA E-834	S2S VPN
College of American Pathologists	Provide direct treatment, diagnostics and	IP Address Number, laboratory LIS test codes with their associated PT observations values, test qualifier values, units of measure, associated PT observation dates and time, lab demographic	National MOU/ISA E-2293	S2S VPN

	monitoring of patients	information, lab instrument identifier, CAP test mapping codes, CAP kit identifiers, associated CAP numbers, CAP specimen identifiers, driver set-up codes		
Varian Medical Systems, Inc	Provide direct treatment, diagnostics and monitoring of patients	IP Address Numbers, FSOP infrastructure system patches and upgrades	National MOU/ISA E-2195	S2S VPN
Biotronik	Provide direct treatment, diagnostics and monitoring of patients	Personally Identifiable Information (PII), Health Information, Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), Patient Identifiers, and Unique Identifier.	Local MOU/ISA E-2208	SSL/TLS
St. Mary's Hospital	Provide direct treatment, diagnostics and monitoring of patients	Personally Identifiable Information (PII), Health Information, Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), Patient Identifiers, and Unique Identifier.	Local MOU-ISA E-2203	S2S VPN
University of Nebraska Medical Center	Provide direct treatment, diagnostics and monitoring of patients	Personally Identifiable Information (PII), Health Information, Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), Patient Identifiers, and Unique Identifier.	Air-Gapped MOU E-1021	S2S VPN
University of Washington PACS	Provide direct treatment, diagnostics and monitoring of patients	Personally Identifiable Information (PII), Health Information, Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), Patient Identifiers, and Unique Identifier.	Local MOU-ISA E-205	S2S VPN

Hermes Medical Solutions	Provide direct treatment, diagnostics and monitoring of patients	Personally Identifiable Information (PII), Health Information, Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), Patient Identifiers, and Unique Identifier.	Local MOU-ISA E-186	S2S VPN
University of Iowa Hospital Clinics	Provide direct treatment, diagnostics and monitoring of patients	Personally Identifiable Information (PII), Health Information, Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), Patient Identifiers, and Unique Identifier.	Local MOU-ISA E-973	S2S VPN
Bitscopic, Inc.	Provide direct treatment, diagnostics and monitoring of patients	Personally Identifiable Information (PII), Health Information, Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), Patient Identifiers, and Unique Identifier.	Local MOU-ISA E-2112	S2S VPN
Bloodworks Northwest	Provide direct treatment, diagnostics and monitoring of patients	Personally Identifiable Information (PII), Health Information, Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), Patient Identifiers, and Unique Identifier.	Local MOU-ISA E-1986	S2S VPN
Black Hills Orthopedic & Spine (BHOSC)	Provide direct treatment, diagnostics and monitoring of patients	Personally Identifiable Information (PII), Health Information, Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), Patient Identifiers, and Unique Identifier.	Local MOU-ISA E-1670	S2S VPN
Black Hills Surgical Hospital	Provide direct treatment, diagnostics and monitoring of patients	Personally Identifiable Information (PII), Health Information, Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected	Local MOU-ISA E-854	S2S VPN

		Health Information (PHI), Patient Identifiers, and Unique Identifier.		
Rapid City Regional Health	Provide direct treatment, diagnostics and monitoring of patients	Personally Identifiable Information (PII), Health Information, Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), Patient Identifiers, and Unique Identifier.	Local MOU-ISA E-695	S2S VPN
Oregon Health & Science University, Radiology Imaging Center	Provide direct treatment, diagnostics and monitoring of patients	Personally Identifiable Information (PII), Health Information, Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), Patient Identifiers, and Unique Identifier.	Local MOU-ISA E-58	S2S VPN
Cascade Medical Imaging, LLC (CMI)	Provide direct treatment, diagnostics and monitoring of patients	Personally Identifiable Information (PII), Health Information, Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), Patient Identifiers, and Unique Identifier.	Local MOU-ISA E-45	S2S VPN
Vaultara [VA System	Provide direct treatment, diagnostics and monitoring of patients	Personally Identifiable Information (PII), Health Information, Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), Patient Identifiers, and Unique Identifier.	Local MOU-ISA E-2120	SSL/TLS
Boston Scientific	Provide direct treatment, diagnostics and monitoring of patients	Personally Identifiable Information (PII), Health Information, Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), Patient Identifiers, and Unique Identifier.	Local MOU-ISA E-1904	S2S VPN
Medtronic	Provide direct treatment, diagnostics and	Personally Identifiable Information (PII), Health Information, Individually Identifiable Information (III), Individually Identifiable Health	Local MOU-ISA E-2164	S2S VPN

	monitoring of patients	Information (IIHI), Protected Health Information (PHI), Patient Identifiers, and Unique Identifier.		
Caregility	Provide direct treatment, diagnostics and monitoring of patients	Personally Identifiable Information (PII), Health Information, Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), Patient Identifiers, and Unique Identifier.	Local MOU-ISA E-2182	S2S VPN
Abbott Laboratories Inc	Provide direct treatment, diagnostics and monitoring of patients	Personally Identifiable Information (PII), Health Information, Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), Patient Identifiers, and Unique Identifier.	Local MOU-ISA E-2165	AS2
iSchemaView	Provide direct treatment, diagnostics and monitoring of patients	Personally Identifiable Information (PII), Health Information, Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), Patient Identifiers, and Unique Identifier.	Local MOU-ISA E-2357	SSL/TLS
Fujifilm Healthcare Americas Corporation	Provide direct treatment, diagnostics and monitoring of patients	Personally Identifiable Information (PII), Health Information, Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), Patient Identifiers, and Unique Identifier.	Local MOU-ISA E-5202	S2S VPN
Thermo Fisher Scientific	Provide direct treatment, diagnostics and monitoring of patients	Personally Identifiable Information (PII), Health Information, Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), Patient Identifiers, and Unique Identifier.	Local MOU-ISA E-2335	SSL/TLS
Boston Medical Center	Provide direct treatment, diagnostics	Personally Identifiable Information (PII), Health Information, Individually Identifiable Information (III),	Air-Gapped MOU LAN Ext.	LAN Ext.

	and monitoring of patients	Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), Patient Identifiers, and Unique Identifier.	E-2162	
GenMark Diagnostics	Provide direct treatment, diagnostics and monitoring of patients	Personally Identifiable Information (PII), Health Information, Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), Patient Identifiers, and Unique Identifier.	Local MOU-ISA E-2333	S2S VPN
Kore Wireless	Provide direct treatment, diagnostics and monitoring of patients	Personally Identifiable Information (PII), Health Information, Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), Patient Identifiers, and Unique Identifier.	Local MOU-ISA E-553	S2S VPN
Softek Illuminate	Provide direct treatment, diagnostics and monitoring of patients	Personally Identifiable Information (PII), Health Information, Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), Patient Identifiers, and Unique Identifier.	Local MOU-ISA E-2297	S2S VPN
Colorado West Healthcare System DBA Community Hospital	Provide direct treatment, diagnostics and monitoring of patients	Personally Identifiable Information (PII), Health Information, Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), Patient Identifiers, and Unique Identifier.	Local MOU-ISA E-955	S2S VPN
Nutanix	Provide direct treatment, diagnostics and monitoring of patients	Personally Identifiable Information (PII), Health Information, Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), Patient Identifiers, and Unique Identifier.	Local MOU-ISA E-1657	SSL/TLS
Subtle Medical – Aidoc	Provide direct	Personally Identifiable Information (PII), Health	Local MOU-ISA	SSL/TLS

	treatment, diagnostics and monitoring of patients	Information, Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), Patient Identifiers, and Unique Identifier.	E-2082	
SonaCare Medical, LLC	Provide direct treatment, diagnostics and monitoring of patients	Personally Identifiable Information (PII), Health Information, Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), Patient Identifiers, and Unique Identifier.	Local MOU-ISA E-2135	SSL/TLS
iSchemaView	Provide direct treatment, diagnostics and monitoring of patients	Personally Identifiable Information (PII), Health Information, Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), Patient Identifiers, and Unique Identifier.	Local MOU-ISA E-2100	S2S VPN
Atirix Medical Systems	Provide direct treatment, diagnostics and monitoring of patients	Personally Identifiable Information (PII), Health Information, Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), Patient Identifiers, and Unique Identifier.	Local MOU-ISA E-2071	SSL/TLS
Document Storage Systems, Inc. (DSS) (CyberREN Dialysis)	Provide direct treatment, diagnostics and monitoring of patients	Personally Identifiable Information (PII), Health Information, Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), Patient Identifiers, and Unique Identifier.	Local MOU-ISA E-1773	S2S VPN

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: 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.

Mitigation: Safeguards are implemented to ensure data is not inappropriately shared or accessed include employee security and privacy training and awareness and required reporting of suspicious activity. Additionally, use of role-based access control mechanisms, need-to-know determinations, secure passwords, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption of data-at-rest and in-transit, and monitoring of access authorization are all measures that are utilized within the facilities. Access to sensitive information and the systems where the information is stored is controlled by the VA using a "least privilege/need to know" policy. Access must be requested and only the access required by VA persons or processes acting on behalf of VA persons is to be requested or granted. All external connections to medical systems are required to comply with VA's External Connection Compliance requirements, including adjudication of MOU/ISA and S2S VPN connections between Zone implementations to MD-LITE, Enterprise Platforms or connections and contracted Vendor support.

Section 6. Notice

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

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

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

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

The initial method of notification is verbally in person during individual interviews and patient processing, in writing via HIPAA disclosure forms and Privacy Act statement on forms and applications completed by the individual. The VHA Notice of Privacy Practice (NOPP) is a document which explains the collection and use of protected health information to individuals interacting with VA. The NOPP is mailed every three years or when there is a major change to all enrolled Veterans. https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946.

Additionally, the Department of Veterans Affairs also provides notice by publishing the following VA SORN in the Federal Register and online. The patient medical records are covered under the SORN 24VA10A7/85 FR 62406 - Patient Medical Records-VA https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf. Other information in this system is covered under SORN 79VA10 - Veterans Health Information Systems and Technology Architecture (VistA) Records-VA https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf.

This PIA also serves as notice for MD-LITE. 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."

Please refer to the facility-level Privacy Impact Assessment for additional notice information. https://www.oprm.va.gov/privacy/pia.aspx

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

Notice is provided as described in 6.1a above. Please also refer to the facility-level Privacy Impact Assessment for additional notice information.
https://www.oprm.va.gov/privacy/pia.aspx

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

The VHA NOPP is a document which explains the collection and use of protected health information to individuals receiving health care from VA. The NOPP is mailed every three years or when there is a major change to all enrolled Veterans. Non-Veterans receiving care are provided the notice at the time of their encounter.

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

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

Please refer to the facility-level Privacy Impact Assessment for additional notice information. https://www.oprm.va.gov/privacy/pia.aspx

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.

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.

Yes, individuals must submit in writing to their facility Privacy Officer. The request must state what information and/or to whom the information is restricted and must include their signature and date of the request. The request is then forwarded to facility Privacy Officer for review and processing.

Individuals can request further limitations on other disclosures. A veteran, legal guardian or court appointed Power of Attorney can submit a request to the facility Privacy Officer to obtain information.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

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

Privacy Risk: 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: This risk is mitigated by the common practice of providing the NOPP when Veterans are enrolled for health care. s. Employees and contractors are required to review, sign and abide by the National Rules of Behavior on a yearly basis as required by VA Handbook 6500 as well as complete annual mandatory Information Security and Privacy Awareness training. Additional mitigation is provided by making the SORN and PIA available for review online, as discussed in question 6.1 and the Overview section of this PIA.

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.***

An individual wanting notification or access, including contesting the record, should mail or deliver a request to the office identified in the SORN. If an individual does not know the "office concerned," the request may be addressed to the Post Office of any VA field station VHA facility where the person is receiving care or the Department of Veterans Affairs Central Office, 810 Vermont Avenue, NW, Washington, DC 20420. The receiving office must promptly forward

the mail request received to the office of jurisdiction clearly identifying it as "Privacy Act Request" and notify the requester of the referral.
When requesting access to one's own records, patients are asked to complete VA Form 10-5345a: Individuals' Request for a Copy of their own health information, which can be obtained from the medical center where they receive treatment or online at https://www.va.gov/find-forms/about-form-10-5345a/.

Additionally, veterans and their dependents can gain access to their Electronic Health Record (EHR) by enrolling in the myHealtheVet (MHV)program, VA's online personal health record. More
information about myHealtheVet is available at Home - My HealtheVet - My HealtheVet (va.gov)

Please also refer to SORN 79VA10 which states "Individuals seeking information regarding access to and contesting of records in this system may write, call or visit the VA facility location where they are or were employed or made contact."

7.1b If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR)?

The information in this system is not exempt from the Privacy Act.

7.1c If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information?

The information in the system does fall under Privacy Act 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.

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

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

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

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, VHA Directive 1605.01 Privacy and ROI establishes procedures for Veterans to request their records to be amended. Also refer to the facility-level Privacy Impact Assessment for additional guidance.
https://www.oprm.va.gov/privacy/pia.aspx

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.

Formal redress is provided. Please see response to 7.3 which refers to NOPP, VHA Directive 1605.01 and the facility-level PIAs.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?
This question is related to privacy control IP-3, Redress.

Follow the format below:

Privacy Risk: There is a risk that 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 an ROI process at the VA facilities to assist Veterans with obtaining access to their health records and other records containing personal information. In addition, VHA 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.

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?

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 via TMS. Each facility is responsible for the creation and maintenance of system accesses. Please refer to the facility-level Privacy Impact Assessment for additional access procedures, such as account creation, modification, elevated privileges, etc. https://www.oprm.va.gov/privacy/pia.aspx.

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?

MD-LITE does not share information with other agencies.

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

Please refer to the facility-level Privacy Impact Assessment for role-based access procedures. https://www.oprm.va.gov/privacy/pia.aspx

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, select medical device vendors could have remote access to their specific devices, for which there is a national VPN agreement and/or business agreement with the vendor. Contractual, agreed upon privacy training and confidentiality is required from the vendor. A Business Associate Agreement (BAA) and/or an Interconnection System Agreement/Memorandum of Understanding (ISA/MOU) exists between the VA and the medical device vendor. If PII/PHI may be shared, transmitted, or received the data elements are captured in the MOU.
Yes, contractors who are the vendor or manufacturer of the medical device are involved with the design, configuration, and maintenance of their medical device/system.
If applicable, a confidentiality agreement, BAA or NDA is developed for contractors who work on the system. 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 via TMS.

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 the VA network must complete the initial and annual VA Privacy and Information Security Awareness and Rules of Behavior training via the TMS site. In addition, all employees who have access to PHI must also complete the TMS Privacy and HIPAA training. Finally, new on-site 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? Yes

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 07/05/2023
3. *The Authorization Status:* Authorization to Operate (ATO)
4. *The Authorization Date:* 10/17/2023
5. *The Authorization Termination Date: 04*/17/2024
6. *The Risk Review Completion Date:* 10/17/2023
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.

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

Not applicable

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)*

No cloud technology is utilized.

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.

Not applicable as no cloud technology is utilized.

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.

Not applicable as no cloud technology is utilized.

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.

Not applicable as no cloud technology is utilized.

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).

MD-LITE does not utilize RPA

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.

Phillip Cauthers 255139

Digitally signed by Phillip Cauthers 255139
Date: 2024.01.04 08:12:28 -08'00'

Privacy Officer, Phillip Cauthers

GEORGE QUINTELA

Digitally signed by GEORGE QUINTELA
Date: 2024.01.04 07:35:02 -05'00'

Information Systems Security Officer, George Quintela

WOODIE ROBINSON

Digitally signed by WOODIE ROBINSON
Date: 2024.01.11 19:39:52 -05'00'

Information Systems Owner, Woodie Robinson

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).

VHA Notice of Privacy Practice (NOPP):
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946.

SORN 24VA10A7 “Patient Medical Records-VA", https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf.

SORN 79VA10 “Veterans Health Information Systems and Technology Architecture (VistA) Records-VA", https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.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