



Privacy Impact Assessment for the VA IT System called:

National TeleCritical Care Program

Specialty Care Program Office (11SPEC)

Veterans Health Administration

Date PIA submitted for review:

July 20, 2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Kamilah Jackson	Kamilah.Jackson@va.gov	513-288-6988
Information System Security Officer	Katherine Vollmer	Katherine.vollmer@va.gov	605-745-200x22258
Information System Owner	Harpreet Sodhi	Harpreet.sodhi@va.gov	301-873-2288

Abstract

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

This PIA is for the National TeleCritical Care Program, previously known as Tele-Intensive Care (TeleICU), utilizes the eCareManager (eCM) software. The eCareManager software is the primary component of TeleCritical Care that allows Intensivists and nurses to monitor patients in remote Intensive Care Units (ICU) (patient care sites). The heart of TeleCritical Care is a central monitoring center, which is located at a Veterans Affairs Medical Center (VAMC) with a concentration of intensivists and experienced critical care nurses. The monitoring center is connected to intensive care unit (ICU) rooms in various associated VAMCs. This program improves access to specialized, enhanced ICU care.

Overview

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

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

The National TeleCritical Care Program, previously known as Tele-Intensive Care (TeleICU) will be under the Telehealth and Scheduling portfolio.

For the National TeleCritical Care Program, the eCareManager (eCM) software is utilized. The eCareManager software is the primary component of TeleCritical Care that allows Intensivists and

nurses to monitor patients in remote ICUs (patient care sites). The heart of TeleCritical Care is a central monitoring center, which is located at a Veterans Affairs Medical Center (VAMC) with a concentration of intensivists and experienced critical care nurses. The monitoring center is connected to ICU rooms in various associated VAMCs. This program improves access to specialized, enhanced ICU care.

The patient information stored is limited to those patients who are monitored in TeleCritical Care enabled rooms at each patient care site. The total number of patients that have information stored is dependent on the number of patients that are admitted to the monitored ICUs. The information is taken from existing health records such as Computerized Patient Record System (CPRS)/ Unified Electronic Health Record (EHR). The information of patient medical history and current medications is manually entered into eCareManager. The VA sends Health Level 7 (HL7) messages to the TeleCritical Care software (eCareManager). eCareManager receives this information from Veterans Health Information System Technology Architecture (VistA) for Admission, Discharge, Transfer (ADT) and Lab information via the Health Level 7 (HL7) messaging. The information used in eCareManager is Name, Social Security Number (SSN), Date of Birth (DOB), medical history, vital signs (waveforms, pulse, respiration, Blood Pressure, oxygen (O2) saturation, temperature).

eCareManager is specialized software that is a remote patient monitoring program in which intensivists support the ICU bedside team using videoconferencing technology and organ system data displays. eCareManager provides continuous physiologic monitoring of each patient with the help of clinical decision support tools and advanced algorithms that provide early warnings. The clinical data such as vital signs, lab, medication, and input/output data is used to:

- Receive patient or population-level information for prioritization,
- Target physiologic areas of patient condition to define a care action plan, and
- have oversight of a large number of patients.

The information is collected for continuity care purposes under the treatment provision of the HIPAA Privacy Rule and manually entered in the CPRS/EHR record where it becomes part of the Veteran health record. All other information is put in eCareManager and is used for reporting purposes; however, this information is not retrieved by a unique identifier. Therefore, a SORN is not required for eCareManager.

The legal authority is HIPAA Privacy Rule Parts 160 and 164. The information is collected for continuity care purposes under the treatment provision of the HIPAA Privacy Rule and placed in the CPRS/EHR record where it becomes part of the Veteran health record. The patient medical record information is found under the SORN of Patient Medical Records - 24VA10A7/85 FR 62406 – VA, dated 10/2/2020.

TeleCritical Care and eCareManager is a medical system and will be covered under the TeleCritical Care system's Authority to Operate (ATO) within eMASS (Enterprise Mission Assurance Support Service), which is the VA's Governance, Risk and Compliance (GRC) tool, and is the authoritative management tool for VA's Assessment and Authorization (A&A) process and Risk Management Framework. It is the responsibility of each TeleCritical Care monitoring facility to include their local TeleCritical Care in their A&A boundary.

This system is located throughout the United States at the following locations and the pending sites listed below. The list of VA medical centers and Department of Defense location, where the TeleCritical Care capability exists are:

Facility Name	Facility Name
Minneapolis, MN	Nellis Air Force Base (DoD)
Omaha, NE	Las Vegas, NV
Fargo, ND	Lebanon, PA
Sioux Falls, SD	Phoenix, AZ
Iowa City, IA	Ann Arbor, MI
Cincinnati, OH	Salisbury, NC
Dayton, OH	Indianapolis, IN
Cleveland, OH	Fayetteville, AR
Des Moines, IA	Columbia, MO
Fort Meade/Black Hills, SD	Boise, ID
Spokane, WA	Cheyenne, WY
Marion, IL	Memphis, TN
Topeka, KS	Shreveport, LA
Leavenworth, KS	Montana HCS (Fort Harrison, MT)
Wichita, KS	Detroit, MI
St. Louis, MO	Huntington, WV
Central Alabama (Montgomery, AL)	Martinsburg, WV
Augusta, GA	Jackson VAMC, MS
Columbia, SC	Southern Arizona HCS (Tucson, AZ)
Birmingham, AL	Baltimore VA Medical Center (Maryland)
Atlanta, GA	Sierra Nevada HCS (Reno)
Wilkes-Barre, PA	Washington DC
Kansas City, MO	Central California (Fresno)
Northern Indiana HCS (Marion, IL)	Richmond, VA
Muskogee, OK	Fayetteville, AR
Togus, ME	Buffalo, NY
Wilmington, DE	Greater Los Angeles HCS (Los Angeles, CA)
Beckley, WV	Eastern Colorado HCS (Denver, CO)
Clarksburg, WV	Albany, NY
Biloxi, MS	Upstate New York - Syracuse
White River Junction, CO	Northport, NY
Mountain Home, TN	New York HHS (Brooklyn, NY)
Grand Junction, CO	Northern California HCS (Sacramento, CA)
	Manhattan, NY

Pending Sites	
Connecticut HCS (West Haven, CT)	Bronx, NY
Amarillo HCS (Amarillo, TX)	Las Vegas (Expansion)
Central Arkansas HCS (Little Rock, AR)	Miami, FL
Central Texas HCS (Temple, TX)	N. Florida/S. Georgia HCS (Gainesville, FL)
San Francisco, CA	N. Florida/S. Georgia HCS (Lake City, FL)
Bay Pines, FL	New Jersey HCS (East Orange, NJ)

Loma Linda, CA	Oklahoma City, OK
New Mexico HCS (Albuquerque NM)	Palo Alto HCS (Palo Alto, CA)
Orlando, FL	Providence, RI
New Orleans, LA	San Juan, PR
Houston, TX	Tampa, FL

With the completion of this PIA, there will not be any changes to business processes.
 With the completion of this PIA, there will be no technology changes.

Section 1. Characterization of the Information

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

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

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

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.

This question is related to privacy control AP-1, Authority To Collect, and AP-2, Purpose Specification.

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

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

- | | | |
|---|--|---|
| <input checked="" type="checkbox"/> Name | <input type="checkbox"/> Emergency Contact | <input type="checkbox"/> Vehicle License Plate |
| <input checked="" type="checkbox"/> Social Security | <input type="checkbox"/> Information (Name, Phone | <input type="checkbox"/> Number |
| Number | <input type="checkbox"/> Number, etc. of a different | <input type="checkbox"/> Internet Protocol (IP) |
| <input checked="" type="checkbox"/> Date of Birth | <input type="checkbox"/> individual) | <input type="checkbox"/> Address Numbers |
| <input type="checkbox"/> Mother's Maiden Name | <input type="checkbox"/> Financial Account | <input checked="" type="checkbox"/> Current Medications |
| <input type="checkbox"/> Personal Mailing | <input type="checkbox"/> Information | <input checked="" type="checkbox"/> Previous Medical |
| Address | <input type="checkbox"/> Health Insurance | Records |
| <input type="checkbox"/> Personal Phone | <input type="checkbox"/> Beneficiary Numbers | <input type="checkbox"/> Race/Ethnicity |
| Number(s) | <input type="checkbox"/> Account numbers | <input type="checkbox"/> Tax Identification |
| <input type="checkbox"/> Personal Fax Number | <input type="checkbox"/> Certificate/License | Number |
| <input type="checkbox"/> Personal Email | numbers | <input type="checkbox"/> Medical Record |
| Address | | Number |

- Gender
- Integration Control Number (ICN)
- Military History/Service Connection

- Next of Kin
- Other Unique Identifying Information (list below)

Other Unique Identifying Information -

Patient Trends reporting also includes patient morbidity/mortality from the health checks of the patients which could include heart rate, oxygen levels, blood pressure, etc. Audio/Visual of the patient by a remote provider is used. At session termination, Audio/Visual is disconnected and not retained or saved.

PII Mapping of Components

TeleCritical Care consists of six (6) key components (databases). TeleCritical Care consists of one key component. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by TeleCritical Care and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

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

PII Mapped to Components

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/Storage of PII	Safeguards
Gateway North TeleCritical Care eCareManager Environment – Web Database for eCM	yes	yes	PII/PHI - Name, social security number, date of birth (DOB), current medications, and Medical history, vital signs (waveforms, pulse, resp., blood pressure, O2 sat, temperature), and flowsheet data from the bedside clinical information system (CIS). Audio/Visual of the patient by a remote provider is	Patient Care	BAA (Business Associate Agreement) and background investigation done on vendor for remote access; Employee/contractor security and privacy training; encrypted transmission and encryption at rest

			used. At session termination, Audio/Visual is disconnected and not retained or saved.		
Gateway North TeleCritical Care eCareManager Environment – SQL database for eCM	yes	yes	PII/PHI - Name, social security number, date of birth (DOB), current medications, and Medical history, vital signs (waveforms, pulse, resp., blood pressure, O2 sat, temperature), and flowsheet data from the bedside clinical information system (CIS). Audio/Visual of the patient by a remote provider is used. At session termination, Audio/Visual is disconnected and not retained or saved.	Patient Care	BAA and background investigation done on vendor for remote access; Employee/contractor security and privacy training; encrypted database (at rest)
Gateway North TeleCritical Care eCareManager Environment – Second SQL database for eCM	yes	yes	PII/PHI - Name, social security number, date of birth (DOB), current medications, and Medical history, vital signs (waveforms, pulse, resp., blood pressure, O2 sat, temperature), and flowsheet data from the bedside clinical information system (CIS). Audio/Visual of the patient by a remote provider is used. At session termination,	Patient Care	BAA and background investigation done on vendor for remote access; Employee/contractor security and privacy training; encrypted database (at rest)

			Audio/Visual is disconnected and not retained or saved.		
Gateway South TeleCritical Care eCareManager Environment – Web Database for eCM	yes	yes	PII/PHI - Name, social security number, date of birth (DOB), current medications, and Medical history, vital signs (waveforms, pulse, resp., blood pressure, O2 sat, temperature), and flowsheet data from the bedside clinical information system (CIS). Audio/Visual of the patient by a remote provider is used. At session termination, Audio/Visual is disconnected and not retained or saved.	Patient Care	BAA and background investigation done on vendor for remote access; Employee/contractor security and privacy training; encrypted transmission
Gateway South TeleCritical Care eCareManager Environment – SQL database for eCM	yes	yes	PII/PHI - Name, social security number, date of birth (DOB), current medications, and Medical history, vital signs (waveforms, pulse, resp., blood pressure, O2 sat, temperature), and flowsheet data from the bedside clinical information system (CIS). Audio/Visual of the patient by a remote provider is used. At session termination, Audio/Visual is disconnected and	Patient Care	BAA and background investigation done on vendor for remote access; Employee/contractor security and privacy training; encrypted database (at rest)

			not retained or saved.		
Gateway South TeleCritical Care eCareManager Environment– Second SQL database for eCM	yes	yes	PII/PHI - Name, social security number, date of birth (DOB), current medications, and Medical history, vital signs (waveforms, pulse, resp., blood pressure, O2 sat, temperature), and flowsheet data from the bedside clinical information system (CIS). Audio/Visual of the patient by a remote provider is used. At session termination, Audio/Visual is disconnected and not retained or saved.	Patient Care	BAA and background investigation done on vendor for remote access; Employee/contractor security and privacy training; encrypted database (at rest)

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

List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

Describe why information from sources other than the individual is required. For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question 1.3 indicate why the system is using this source of data.

If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

The TeleCritical Care software (eCareManager) collects information from VistA for Admission, Discharge, Transfer (ADT) and Lab information via Health Level 7 (HL7) messaging. It obtains vital sign data from facility vital signs servers via a HL7 message. There is currently manual entry of patient medical history and current medications into eCareManager from CPRS/EHR. The Clinical

Information System (CIS) in the ICU also populates input and output data, intravenous (IV) infusions, vital signs, and medications.

This information is also collated to create “smart alarms” and alerts to direct the practitioners to patients with vital signs or labs that require further review and possible intervention.

1.3 How is the information collected?

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

If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form’s OMB control number and the agency form number.

This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

Information is collected via electronic transfer (HL7 messaging transmitted to eCareManager) and manual entry. Information also comes from a two-way audio/visual connection to each patient ICU room. The TeleCritical Care staff or the corresponding ICU facility can initiate audio/visual when needed, or when medical information detects intervention from the TeleCritical Care staff.

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

Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

All application interfaces were tested to ensure accuracy. This was done by reviewing data passed from test account to test account, production account to test account and production account to production account.

Mapping worksheets were used as a guide to confirm each data element and its accuracy was verified for each element interfaced into the system. Manual entry validation is dependent on review by clinicians during each shift.

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

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

This question is related to privacy control AP-1, Authority to Collect

The legal authority is the HIPAA Privacy Rule 45 CFR Part 160 and Part 164. The information is collected for continuity care purposes under the treatment provision of the HIPAA Privacy Rule and placed in the CPRS/EHR record where it becomes part of the Veteran health record. All other information is put in eCareManager and is used for reporting purposes. However, this information is not retrieved by a unique identifier, therefore a SORN is not required for eCareManager. The patient medical records are covered under the SORN 24VA10A7/85 FR 62406 - Patient Medical Records - VA, dated 10/02/2020, Link to Printed Version: <https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf>

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.

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

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

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

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

Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?

This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

Privacy Risk: The Tele-Intensive Care Units collects both Personally Identifiable Information (PII) and a variety of other Sensitive Personal Information (SPI), such as Protected Health Information

(PHI). Due to the highly sensitive nature of this data, there is a risk that, this collected, process, or retained data is not accurate, not complete, nor current.

Mitigation:

The TeleCritical Care software provides an extra layer of patient care to veterans in our ICU's, and this is directly in line with the VA's mission to provide high quality healthcare to our veterans. Information collected is used by the software to provide inputs to algorithms that trigger "smart alerts/alarms" that function as an early detection and decision support system. This information is collected via the applications interfaces to patient waveforms, vital signs, and through direct entry from clinical personnel. Patients provide little of the information collected directly, as most is already within VA information systems or is by observation of the patients. Personal Identifiable Information (PII) is taken directly from VistA and is verified by local facility staff instead of by the remote TeleCritical Care staff.

Section 2. Uses of the Information

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

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

Identify and list each use (both internal and external to VA) of the information collected or maintained.

This question is related to privacy control AP-2, Purpose Specification.

Name: Used as an identifier

SSN: Used as an identifier

DOB: Used as an identifier

Current Medications: used in treatment of patient

Patient Medical History: used in decision of treatment of patient

Audio/Visual of the patient: Used by a remote provider. At session termination, Audio/Visual is disconnected and not retained or saved.

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

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

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

If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

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

eCareManager and CPRS/EHR are the primary tools utilized with TeleCritical Care. The data obtained via eCareManager could potentially be used for reporting purposes as they relate to morbidity and mortality of ICU patients. There will be summary of de-identified data and will not be placed in the patients' records. CPRS/EHR notes are manually entered by TeleCritical Care staff in the appropriate patient records. All patient monitoring data is deleted from eCareManager after patient is discharged from ICU, approximately 36 hours after discharge.

2.3 How is the information in the system secured?

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

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

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

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

The measures in place to protect data in transit and are rest are full disk encryption to protect data at rest. Transport Layer Security (TLS) encryption between the system to protect Data in Transit. The process, and all encryption, complies with Federal Information Processing Standards (FIPS) 140-2.

Additional protections are that SSNs are only available to TeleCritical Care providers. Communication connections between servers, and between workstations and eCM application server are encrypted with TLS (Transport Layer Security) 1.2. The Network Application (Netapp) Volume Encryption (data at rest) is encrypted and meets FIPS 140-2 Level 2 compliant.

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 VHA Privacy and HIPAA Focused Training.

All information used within the TeleCritical Care monitoring sites are within secure, locked units without visitors or other veterans. TeleCritical Care Staff work within this locked area of the VA Medical Center and do not leave the room during their shift, generally (bathroom and kitchen are included in the suite). 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, along with the VHA Privacy and HIPAA Focused Training.

The privacy of patient information must be preserved, and the information must not be accessible to, or discussed with, any unauthorized persons, nor is the information to be discussed in public areas. Every employee with access to patient health records in any medium is responsible for the proper use, disclosure, and handling of the patient health records (see VHA Directive 1605.01 Privacy and Release of Information, VHA Directive 1605 VHA Privacy Program and VA Directive 6500, Information Security Program). They are also accountable for safeguarding patient confidentiality and privacy, and failure to do so results in administrative action, up to and including, termination or other legal adverse action.

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

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. 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.

All clinical staff in the TeleCritical Care are trained in the use of eCareManager and applicable privacy implications. All VHA personnel including employees, volunteers, and students must be trained, at least annually, on privacy policies to include the requirements of Federal privacy and information laws, regulations, and VHA policy.

New personnel must be trained within 30 days of employment. Staff training, and competencies are tracked and recorded. Management approves of TeleCritical Care staff for both access and training. At a minimum, instruction must be provided within 6 months of significant change in Federal law, regulation, this policy, and/or facility or office procedures.

Section 3. Retention of Information

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

3.1 What information is retained?

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

None of the information is retained in eCareManager. Data is entered into CPRS/EHR as part of the patient record. All patient data (Medical history, vital signs (waveforms, pulse, resp., B/P, O2 sat, temperature), and flowsheet data from the bedside CIS system is temporarily saved during patient treatment for reporting purposes only on our reports server which is in a secure data center within the VA firewall. All reports use aggregate patient data and individual patient data is not produced in reports. As stated in the Records Control Schedule, RCS 10-1, Chapter Six – Healthcare Records, 6000.2 Electronic Health Record, temporary records can be destroyed after verification of accurate entry of information into EHRS (Electronic Health Record System) Link - <https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf>

3.2 How long is information retained?

In some cases VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. If the system is using cloud technology, will it be following the NARA approved retention length and schedule?

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

All information is temporarily retained for approximately thirty-six (36) hours after discharge for reporting purposes only at a summary level—this is not a system of record. As stated in the Records Control Schedule, RCS 10-1, Chapter Six – Healthcare Records, 6000.2 Electronic Health Record, temporary records can be destroyed after verification of accurate entry of information into EHRS (Electronic Health Record System) Link - <https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf>

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

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner. This question is related to privacy control DM-2, Data Retention and Disposal.

As the data is not retrieved at a personally identifiable level, no records retention schedule is required. All information is temporarily retained for reporting purposes only at a summary level. TeleCritical Care staff document notes in CPRS/EHR on the patient treatment, and that record's retention is determined at the local facility. As stated in the Records Control Schedule, RCS 10-1, Chapter Six – Healthcare Records, 6000.2 Electronic Health Record, temporary records can be destroyed after verification of accurate entry of information into EHRS (Electronic Health Record System) Link - <https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf>

3.4 What are the procedures for the elimination of SPI?

Explain how records are destroyed or eliminated at the end of the retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc? This question is related to privacy control DM-2, Data Retention and Disposal

As reports are produced at an aggregate level, SPI information is not produced and therefore not required to be eliminated. 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. As stated in the Records Control Schedule, RCS 10-1, Chapter Six – Healthcare Records, 6000.2 Electronic Health Record, temporary records can be destroyed after verification of accurate entry of information into EHRS (Electronic Health Record System) Link - <https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf>

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

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

No research, testing or training with use of PII for this eCareManager application is done at this time.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks.

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

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

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

Principle of Data Quality and Integrity: Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?

This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:

Privacy Risk: The risk to maintain data within TeleCritical Care is the longer time frame information is kept, the greater the risk that information possibly will be compromised or breached.

Mitigation: All patient data is saved for aggregate reporting purposes only (not accessible at individual level) on a reports server which is in a secure data center within the VA firewall. The server is protected with the following measures:

- Located behind VA firewall
- In a locked and secure server room
- Business Associate Agreement (BAA) and background investigation done on vendor for remote access

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
TeleCritical Care- eCareManager Philips eCareManager - Gateway North	This is a remote patient monitoring program in which intensivists support the ICU bedside team using videoconferencing technology and organ system data displays.	Patient Trends include the first and last name, DOB, SSN for the reporting of patient morbidity/mortality from the health checks of the patients which could include heart rate, oxygen levels, blood pressure, etc.	Electronic Reporting -- HL7 messaging
TeleCritical Care- eCareManager Philips eCareManager - Gateway South	This is a remote patient monitoring program in which intensivists support the ICU bedside team using videoconferencing technology and organ system data displays.	Patient Trends include the first and last name, DOB, SSN for the reporting of patient morbidity/mortality from the health checks of the patients which could include heart rate, oxygen levels, blood pressure, etc.	Electronic Reporting -- HL7 messaging
VistA – varies at each facility connecting to TeleCritical Care	The information is collected for continuity care purposes / patient treatment	Name, SSN, DOB, and current medications, Medical History of Admission, Discharge, Transfer (ADT) and Lab information	Manual and HL7 transfer

<i>List the Program Office or IT System information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</i>	<i>Describe the method of transmittal</i>
Clinical Information Systems (CIS) varies at each facility connecting to TeleCritical Care	The information is collected for continuity care purposes / patient treatment	Name, SSN, DOB, and current medications	Manual and HL7 transfer

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: Unintended exposure of patient PII to unauthorized programs

Mitigation: All reports transmitted electronically are encrypted, if they contain PHI, all paper reports are handled according to privacy training and responsibilities in maintaining confidentiality.

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

<i>List External Program Office or IT System information is shared/received with</i>	<i>List the purpose of information being shared / received / transmitted with the specified program office or IT system</i>	<i>List the specific PII/PHI data elements that are processed (shared / received/transmitted) with the Program or IT system</i>	<i>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</i>	<i>List the method of transmission and the measures in place to secure data</i>
Philips eCareManager	For reporting purposes	Benchmarking data (summary of de- identified monitoring data	BAA and Contract with vendor (Philips)	Encrypted hard drive

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum Of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.

Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.

This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

Privacy Risk: 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:

All reports transmitted electronically are encrypted. In addition, access to medical devices is on a need-to-know basis and limited to clinical staff, Biomedical staff, and others with a legitimate need-to-know. Access control policies and procedures follow the VA User Provisioning process. Audit Logs are maintained and reviewed. TeleCritical Care access is restricted to personnel with VA Privacy and Information Security Awareness training and Rules of Behavior, and the VHA Privacy and HIPAA training, certified annually.

Safeguards implemented to ensure data is not shared with unapproved or incorrect organizations are employee security and privacy training and awareness and required reporting of suspicious activity. Business Associate Agreement (BAA) and background investigation are done on vendors/contractors who have VA network access or remote access. VA Memorandum of Understanding/Interconnection Security Agreement (MOU/ISA) agreements are in place with medical device vendors. In addition, safeguards implemented to ensure data is not shared with unapproved or incorrect organizations are disabling unused ports and restricting access in providing isolation thru firewall Access Control Lists (ACL).

VA encrypted hard drive with de-identified data sent to the vendor quarterly in compliance with agreement between VA and the vendor. Reports are obtained, and data is scrubbed from systems.

Section 6. Notice

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

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

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

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

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

This question is related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

Patients and families are educated on the process of TeleCritical Care (Tele-ICU) when they are admitted to the unit. All information collected comes from VistA/CPRS/EHR via HL7 messaging rather than from patients or their families. The VA sends HL7 messages to eCareManager. NOPP (Notice of Privacy Practice) are discussed at the individual VistA/CPRS/EHR sites and documented in their respective PIAs.

The patient medical records are covered under the SORN 24VA10A7/85 FR 62406 - Patient Medical Records - VA, dated 10/02/2020, Link to Printed Version: <https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf>

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

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

If a patient is admitted to a Tele-ICU enabled room, information is automatically collected. This is part of their consent to be treated. Patients have the right to decline having the TeleCritical Care staff activate the camera to perform an audiovisual exam and also have the right to decline the TeleCritical Care assisting in managing their care.

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

This question is directed at whether an individual may provide consent for specific uses or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use?

This question is related to privacy control IP-1, Consent

. Information is required for TeleCritical Care use and success in patient care. Patients have the right to decline having the TeleCritical Care staff activate the camera to perform an audiovisual exam and also have the right to decline the TeleCritical Care assisting in managing their care.

VHA permits individuals to agree to the collection of their personally identifiable information (PII) using paper and electronic forms that include Privacy Act Statements outlining why the information is being collected, how it will be used and what Privacy Act system of records the information will be stored. In addition, information is collected verbally from individuals. These individuals are made aware of why data is collected through the VHA Notice of Privacy Practices and conversations with VHA employees. VA Forms are reviewed by (VHACO)Veterans Health Administration Central Office periodically to ensure compliance with

Version Date: October 1, 2021

Page 21 of 33

various requirements including that Privacy Act Statements are on forms collecting personal information from Veterans or individuals. VHA uses PII and PHI only as legally permitted including obtaining authorizations were required. Where legally required VHA obtains signed, written authorizations from individuals prior to releasing, disclosing or sharing PII and PHI. Individuals have a right to restrict the disclosure and use of their health information.

Individuals who want to restrict the use of their information should submit a written request to the facility Privacy Officer where they are receiving their care.

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.

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: Risk that Veterans and other members of public will not know that TeleCritical Care exists or that if it collects, maintains and or disseminates PII.

Mitigation: The information collected is from the SORN 24VA10A7/85 FR 62406 - Patient Medical Records - VA, at the local facility's CPRS/VistA/EHR record. This PIA will be posted online for the public to view. Patients and families are educated on the process of TeleCritical Care when they are admitted to the unit. All information collected comes from VistA/CPRS/EHR via HL7 messaging. NOPP (Notice of Privacy Practice) are discussed at the individual VistA/CPRS/EHR sites and documented in their respective PIAs.

Section 7. Access, Redress, and Correction

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

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

Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may

also include additional access provisions. For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at <http://www.foia.va.gov/> to obtain information about FOIA points of contact and information about agency FOIA processes.

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

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

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

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

7.2 What are the procedures for correcting inaccurate or erroneous information?

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed. If the correction procedures are the same as those given in question 7.1, state as much.

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

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

The procedure for correcting inaccurate or erroneous information begins with a Veteran requesting the records in question from Release of Information (ROI). The request for amendment and correction is sent to the facility Privacy Office for processing. The documents are then forwarded to the practitioner who entered the data by the facility Privacy Officer. The practitioner either grants or denies the request. The Veteran is notified of the decision via letter by the facility Privacy Officer.

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

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

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

Right to Request Amendment of Health Information.

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

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

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

The users would not have direct access to the medical devices/systems information to allow for corrections, and any information would be within the VistA/CPRS/Unified EHR. In addition, VHA Directive 1605.01, Privacy and Release of Information, establishes procedures for Veterans to have their records amended when appropriate.

7.4 If no formal redress is provided, what alternatives are available to the individual?

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems.

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

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

The Veteran would utilize the procedures in the NOPP, which every patient receives when they enroll for care. The users would not have direct access to the medical devices/systems (eCareManager) information to allow for corrections, and any information would be within the VistA/CPRS/Unified EHR. In addition, VHA Directive 1605.01, Privacy and Release of Information, establishes procedures for Veterans to have their records amended when appropriate.

Inaccurate information is corrected by VA site personnel with access to the appropriate the VistA/CPRS/Unified EHR.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that a Veteran may not know how to obtain access to their records or how to request corrections to their records.

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

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

Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

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

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

The medical devices/workstations require a login with VA credentials. Once logged into the workstation, there is another level of credentialing that must be verified prior to accessing the eCareManager program. eCareManager is a role-based access software so personnel are assigned roles based on their job functions and they are limited to the "need to know" of any information in the system as determined by role 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 the VHA Privacy and HIPAA Focused Training.

8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII.

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

Yes, contractors could have remote access to the system, for which there is a national VPN agreement as well as a business agreement with vendor. Contractual, agreed upon privacy

training and confidentiality is required from the vendor. A Business Associate Agreement (BAA) and an Interconnection System Agreement/Memorandum of Understanding (ISA/MOU) exists between the VA and the contractor.

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 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 the VHA Privacy and HIPAA training, and are re-certified annually.

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

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

All VA employees/contractors who have access to VA computers must complete the onboarding and annual mandatory VA Privacy and Information Security Awareness Training and Rules of Behavior, TMS (Talent Management System) course #10176. In addition, all employees who have access to PHI must complete the required VHA Privacy and HIPAA Focused training, TMS Course #10203. Finally, all new employees receive face-to-face training by the facility Privacy Officer and Information System Security Officer during new employee orientation. The Privacy and Information System Security Officer also perform subject specific trainings on an as needed basis.

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

If Yes, provide:

- 1. The Security Plan Status,*
- 2. The Security Plan Status Date,*
- 3. The Authorization Status,*
- 4. The Authorization Date,*
- 5. The Authorization Termination Date,*
- 6. The Risk Review Completion Date,*
- 7. The FIPS 199 classification of the system (LOW/MODERATE/HIGH).*

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

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

This system will be applying for a P-ATO (Provisional Authority To Operate) as soon as possible. The system security plan will be developed within eMASS (Enterprise Mission Assurance Support Service) The FIPS 199 classification will be determined during the security categorization but expected to be at least moderate. An expected **Initial Operating Capability (IOC) date** is 2/1/2023.

Section 9 – Technology Usage

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

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

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS).

This question is related to privacy control UL-1, Information Sharing with Third Parties.

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1.

This system does not use any cloud technologies.

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract)

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

This system does not use any cloud technologies.

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

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

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

This system does not use any cloud technologies.

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

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

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

This system does not use any cloud technologies.

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

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

This system does not use any RPA technologies.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

ID	Privacy Controls
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.

Privacy Officer, Kamilah Jackson

Information Systems Security Officer, Katherine Vollmer

Information System Owner, Harpreet Sodhi

APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy, a Privacy Act notice on forms).

System of Records Notice

1. VA SORN 24VA10A7/85 FR 62406 - Patient Medical Records–VA.

a. Effective Date: 10/02/2020

b. Link to Printed Version: <https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf>

2. VHA Handbook 1605.4 *Notice of Privacy Practices*, October 7, 2015

(https://vaww.va.gov/vhapublications/ViewPublication.asp?pub_ID=3147)