Privacy Impact Assessment for the VA IT System called:

TeleCritical Care Program

Veterans Health Administration

Specialty Care Program Office (11SPEC)- TeleCritical Care Program

eMass ID# 2209

Date PIA submitted for review:

Sept 21, 2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Nancy Katz-Johnson	Nancy.Katz-Johnson@va.gov	203-535-7280
Information System Security Officer (ISSO)	Stuart Chase	Stuart.Chase@va.gov	410-340-2018
Information System Owner	Steven Green	steven.green@va.gov	510-630-9099

Abstract

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

This PIA is for the TeleCritical Care Program (TCC), previously known as National TeleCritical Care Program, that utilizes the eCare Manager (eCM) software. The eCare Manager 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 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:

1 *General Description*

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

TeleCritical Care Program, previously known as National TeleCritical Care Program, is under the Specialty Care 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?*

For the TeleCritical Care Program, the eCare Manager (eCM) software is utilized. The eCare Manager 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 rooms in various associated VAMCs. This program improves access to specialized, enhanced ICU care.

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

TeleCritical Care and eCare Manager 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.

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?*

eCare Manager is specialized software that is a remote patient monitoring program in which intensivists support the ICU bedside team using videoconferencing technology and unified patient data display. eCare Manager provides continuous physiologic monitoring of each patient with the help of clinical decision support tools and advanced algorithms that provide early warnings. This system is used to assist with treatment of approximately 55,000 patients per year. 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.

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

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.

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

Information sharing conducted by the IT system is eCare Manager 1 and 2 in the North TIC gateway and Database 1 and 2 in North and South TIC gateways.

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

The patient information stored is limited to those patients who are monitored in TeleCritical Care enabled rooms at each patient care site across the nation. 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 eCare Manager. The VA sends Health Level 7 (HL7) messages to the TeleCritical Care software (eCare Manager). eCare Manager 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 eCare Manager is Name, Social Security Number (SSN), Date of Birth (DOB), medical history, vital signs (waveforms, pulse, respiration, Blood Pressure, oxygen (O2) saturation, temperature).

3. Legal Authority and SORN

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

SORN of Patient Medical Records - 24VA10A7/85 FR 62406 – VA, dated 10/2/2020.

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 patient medical record information is found under the SORN of Patient Medical Records - 24VA10A7/85 FR 62406 – VA, dated 10/2/2020. All other information is put in eCare Manager and is used for reporting purposes; however, this information is not retrieved by a unique identifier. Therefore, a SORN is not required for eCare Manager.

4. System Changes

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

With the completion of this PIA, there will not be any changes to business processes.

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

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://vaww.va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

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

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

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

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

Other PII/PHI data elements: Vital signs (waveforms, pulse, resp., blood pressure, O2 sat, temperature), lab results, and flowsheet data from the bedside CIS system. 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.

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

PII Mapping of Components (Servers/Database)

TeleCritical Care consists of six key components (servers/databases/instances/applications/software/application programming interfaces (API). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by TeleCritical Care 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

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 eCare Manager 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 (Business Associate Agreement) and background investigation done on vendor for remote access; Employee/contractor security and privacy training; encrypted transmission and encryption at rest
Gateway North TeleCritical Care eCare Manager	yes	yes	PII/PHI - Name, social security number, date of birth (DOB), current medications, and medical history, vital	Patient Care	BAA and background investigation done on vendor for

Environment – SQL database for eCM			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.		remote access; Employee/contractor security and privacy training; encrypted database (at rest)
Gateway North TeleCritical Care eCare Manager 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 transmission and encryption at rest
Gateway South TeleCritical Care eCare Manager 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	Patient Care	BAA (Business Associate Agreement) and background investigation done on vendor for remote access;

			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.		Employee/contractor security and privacy training; encrypted transmission and encryption at rest
Gateway South TeleCritical Care eCare Manager 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 South TeleCritical Care eCare Manager 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	Patient Care	BAA and background investigation done on vendor for remote access; Employee/contractor security and privacy training; encrypted database (at rest)

			termination, Audio/Visual is disconnected and not retained or saved.		

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?

The TeleCritical Care software (eCare Manager) collects information from VistA for Admission, Discharge, Transfer (ADT) and Lab information via Health Level 7 (HL7) messaging.

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.

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 eCare Manager 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.

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

The data obtained via eCare Manager could potentially be used for reporting purposes as they relate to morbidity and mortality of ICU patients.

1.3 How is the information collected?

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

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

Information is collected via electronic transfer (HL7 messaging transmitted to eCare Manager) 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.

1.3b 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?

TeleCritical Care does not collect information on a form, so is not subject to the Paperwork Reduction Act.

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.

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.

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?

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 eCare Manager and is used for reporting purposes. However, this information is not retrieved by a unique identifier, therefore a SORN is not required for eCare Manager. 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. (*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: 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 that, this collected, process, or (PHI). Due to the highly sensitive nature of this data, there is a risk 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 that will be used in support of the program's business purpose.

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

PII/PHI Data Element	Internal Use	External Use
Name	Used as an identifier	Not shared
SSN	Used as an identifier.	Not shared
Date of Birth	Used as an identifier.	Not shared
Current Medications	Used in treatment of patient	Not shared
Patient Medical History	Used in decision of treatment	Not shared
Patient audio/visual	Used in treatment	Not shared
Patient trends	Used in treatment	Not shared
Lab results	Used in treatment	Not shared
Vital Signs	Used in treatment	Not shared
Flowsheet Data	Used in treatment	Not shared

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?

eCare Manager and CPRS/EHR are the primary tools utilized with TeleCritical Care. The data obtained via eCare Manager could potentially be used for reporting purposes as they relate to morbidity and mortality of ICU patients.

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.

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.

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?

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.

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

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.

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

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.

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?

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.

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

Staff training, and competencies are tracked and recorded.

2.4c Does access require manager approval?

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.

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

Yes

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

Management monitors, tracks, and records TeleCritical staff for both access and training

Section 3. Retention of Information

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

3.1 What information is retained?

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

- Name
- Social Security Number
- Date of Birth

- Medications
- Medical Records
- Other Data Elements (listed below)

Other PII/PHI data elements: Vital signs (waveforms, pulse, resp., blood pressure, O2 sat, temperature), lab results, and flowsheet data from the bedside CIS system. 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.

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.*

Information is retained indefinitely.

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?

As the data is not retrieved at a personally identifiable level, no records retention schedule is required. All information is retained in the SQL Database inaccessible through the application.

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

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

PII is only used for testing for eCare Manager application at this time

<u>3.6 PRIVACY IMPACT ASSESSMENT: Retention of information</u>

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: 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

Identify and list the name of the VA program office, system name, or category of individuals within VA with which information is shared (sent or received)	**Specifically list the Data Elements Shared (sent or received)**	**Method of Transmission**
Veterans Information Systems and Technology Architecture (VistA)	Name, SSN, DOB, current medications, and lab results.	TCP, bi-directional
Clinical Information Systems (CIS)	Name, SSN, DOB, current medications, and lab results.	TCP, bi-directional
Summit Data Platform	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.	TCP, outbound
Data Access Services (DAS) Single Point of Entry (SPoE)	Name, SSN, DOB, current medications, and lab results.	TCP, bi-directional

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: Unintended exposure of patient PII to unauthorized programs

Mitigation: All data transmitted electronically are encrypted, if they contain PHI, all manual entries 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

Identify and list the name of the VA program office, system name, or category of individuals outside of the VA with which information is shared (sent or received)	**Specifically list the Data Elements Shared (sent or received)**	**Type of Connection**	**Agreement Type (Can be more than one)**
Philips Remote Service	No PHI/PII transmitted	VPN	MOU#: E-789
DigiCert Remote Service	No PHI/PII transmitted	HTTP/HTTPS	OIT NextGen Solution Certification Server

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: All data transmitted electronically is 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). 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 6.1 on the last page of the document. Also provide notice given to individuals by the source system (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

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

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

The VHA Notice of Privacy Practice (NOPP) https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946 explains the collection and use of protected health information to individuals receiving health care from VA. The NOPP is mailed every three years or when there is a major change to all enrolled Veterans. Non-Veterans receiving care are provided the notice at the time of their encounter.

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

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.

Notice is also provided in the Federal Register with the publication of the SORN:

Patients and families are educated on the process of TeleCritical Care (Tele-ICU) when they are admitted to the unit.

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

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

6.1c 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.

Notice was provided in accordance with 6.1a above.

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.

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

This question is directed at whether an individual may provide consent for specific uses, or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent.

Information is used, accessed and disclosed in accordance with the Privacy Act, 5 USC 552a, Title 38 USC 5701, Confidential Nature of Claims, Title USC 7332 and the HIPAA Privacy Rule 45 CFR. Individuals are provided with a copy of the Notice of Privacy Practices that indicates when information will be used without their consent and when they will be asked to provide consent. Information is used, accessed and disclosed in accordance with the Privacy Act, 5 USC 552a, Title 38 USC 5701, Confidential Nature of Claims, Title USC 7332 and the HIPAA Privacy Rule 45 CFR. Individuals or their legal representative may consent to the use or disclosure of information via a written request submitted to their facility Privacy Officer. Individuals also have the right to request a restriction to the use of their information. The written request must state what information and/or to whom the information is restricted and must include their signature and date of the request. The request is then forwarded to facility Privacy Officer for review and processing. Individuals may also request to Opt-Out of the facility directory during an inpatient admission. If the individual chooses to opt-out, information is not disclosed from the facility directory unless otherwise required by law. 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.

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: 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 and patient monitoring systems 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?

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.***

Patients do not have access to the information in the medical devices/systems (eCare Manager) 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.

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)?

TeleCritical Care is not exempt from the Privacy Act. 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 MyHealtheVet (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.

7.1c 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?

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 MyHealtheVet (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. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

The 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 (eCare Manager) 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.*** *(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 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?

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 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 eCare Manager program.

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?
eCare Manager 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.

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.

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 Version Date: October 1, 2021 Page 27 of 33 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?

8.4a If Yes, provide:

1. *The Security Plan Status:* Complete
2. *The System Security Plan Status Date:* 07/24/2024
3. *The Authorization Status:* 2-Year ATO
4. *The Authorization Date:* 09/30/2024
5. *The Authorization Termination Date:* 09/30/2026
6. *The Risk Review Completion Date:* 04/05/2024
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* HIGH

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

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)*

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). (*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.*

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**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

NANCY KATZ-JOHNSON

Digitally signed by NANCY KATZ-JOHNSON
Date: 2024.10.25 10:28:02 -04'00'

Privacy Officer, Nancy Katz-Johnson

STUART CHASE

Digitally signed by STUART CHASE
Date: 2024.10.25 08:58:40 -04'00'

Information System Security Officer, Stuart Chase

STEVEN GREEN

Digitally signed by STEVEN GREEN
Date: 2024.10.28 16:14:10 -07'00'

Information System Owner, Steven Green

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).

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)

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 1605.04