Privacy Impact Assessment for the VA IT System called:

Ensocare

National Social Work Services

Veteran’s Health Administration

Date PIA submitted for review:

12/21/2022

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)	Crystal White	Crystal.White5@va.gov	(813)972-2000 x 7007
Information System Owner	Angela Gant-Curtis	Angela.Gant-Curtis@va.gov	540-760-7222

Abstract

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

Ensocare provides VA social workers and other staff acting as Case Managers, care coordination software and technology-enabled services to smoothly manage care transitions, enable remote monitoring in real-time, and connect all caregivers around a unified goal: The Veteran. Ensocare provides the VA services and solutions which will enable patients to move more efficiently and effortlessly through the care continuum. Every step of the patient's non-VA care transition can be coordinated, from hospital discharge to post-acute placement or recovery at home, and all points in between by providing an automated solution. The Ensocare automates previously manual processes, helping hospitals wrest back efficiency in what has historically been an inefficient system. This functionality, working in concert with The Veterans Data Integration and Federation Enterprise Platform (VDIF), VistA/CPRS or Cerner lets case managers use software to instantly communicate with post-acute providers. After reviewing prospective post-acute providers with the patient, right at the bedside, it takes just a few clicks to send the referral to their chosen providers, who can then respond in their own provider/agency-facing version of the application. Instead of standing by a fax machine and waiting or playing phone tag with those agencies. The response of "Yes," "No" or "Maybe" gets sent right away, electronically, bringing the median response rate down to 30 minutes from what was previously hours or even days.

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. The IT system name and the name of the program office that owns the IT system.

Ensocare's business ownership lies within the National Office of Social Work Services.

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

The solution will allow VA social workers and other VA staff acting as case managers to automate care coordination. This automation software and its technology-enabled services will smooth manage care transitions via referrals and placement to non-VA points of care and care providers. This efficiency supports VA Social Works mission to help in resolving challenges to Veteran's health and wellbeing by connecting Veterans with services and programs to meet their emergent needs without lapsed time or having to wait for manual processes using paper and faxed information.

C. Indicate the ownership or control of the IT system or project.

Ensocare ATO/ATC (eMASS ID: 788) authorized managed service hosted within the VAEC/AWS environment. The solution is available for use VA wide, whether a facility has migrated to Cerner or remains on VistA/CPRS.

2. Information Collection and Sharing

D. The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.

The expected number of individuals whose information is stored in the system and is based on adoption rates (e.g., quantity of VA facilities and the size of those facilities) as well as other mitigating factors approximately 1000 per site.

E. A general description of the information in the IT system and the purpose for collecting this information.

Information gathered on a Veteran can include but is not limited to the following: demographics included in a cover sheet based on ADT message content, clinical summary document (dependent on VDIF integration) containing allergies, vital signs, current medications, dietary orders, precautions, respiratory status, and current treatment requirements. In addition, other notes such as history and physical, medication reconciliation, physical therapy , dialysis, wound care, progress notes by MD, Social Work Geriatric and Extended Care Assessment, etc. can be included via Cerner API interface or uploaded from VistA/CPRS for inclusion in the referral clinical packet to be shared with the non-VA point of care or provider.

F. *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
Ensocare receives data from VistA, VDIF and/or Cerner. Ensocare does not share or transmit data to any other system

G. *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.*
Ensocare is available and operated at more than one site. For Ensocare Cerner Acute Case Management embedded API—use and PII is controlled by the source system Cerner. Ensocare as a stand-alone solution with VistA and/or VDIF integration; the EHR provides the conical source of PII. Indeterminate of source of PII the use of the system is limited to referring the Veteran patient for services and/or placement to non-VA providers and agencies

3. Legal Authority and SORN

H. *A citation of the legal authority to operate the IT system.*

24VA10A7 – Patient Medical Records -VA: Title 38, United States Code, Sections 501(b) and 304
79VA10 – Veterans Health Information Systems and Technology Architecture (VISTA) Records - VA Title 38, United States Code, section 7301(a).
121 VA10A7 -National Patient Database – VA - Title 38 United States Code Section 501.

Information gathered on the Veteran can include but is not limited to the following: demographic cover sheet based on ADT message content, clinical summary document (dependent on VDIF integration) containing allergies, vital signs, current medications, dietary orders, precautions, respiratory status, and current treatment requirements. In addition, other notes such as history and physical, medication reconciliation, physical therapy , dialysis, wound care, progress notes by MD, Social Work Geriatric and Extended Care Assessment, etc. can be included via Cerner API interface or uploaded from VistA/CPRS for inclusion in the referral clinical packet to be shared with the non-VA point of care or provider. Information gathered on the Veteran can include but is not limited to the following: demographic cover sheet based on ADT message content, clinical summary document (dependent on VDIF integration) containing allergies, vital signs, current medications, dietary orders, precautions, respiratory status, and current treatment requirements. In addition, other notes such as history and physical, medication reconciliation, physical therapy , dialysis, wound care, progress notes by MD, Social Work Geriatric and Extended Care Assessment, etc. can be included via Cerner API interface or uploaded from VistA/CPRS for inclusion in the referral clinical packet to be shared with the non-VA point of care or provider.

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?*
NA

D. System Changes

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

NA

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

NA

Section 1. Characterization of the Information

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

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

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

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

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

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

☒ Name
☒ Social Security Number
☒ Date of Birth
☐ Mother's Maiden Name
☒ Personal Mailing Address
☒ Personal Phone Number(s)
☐ Personal Fax Number
☒ Personal Email Address
☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
☐ Financial Information
☐ Health Insurance Beneficiary Numbers Account numbers
☐ Certificate/License numbers*
☐ 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)

There is a MRN Medical Record Number field which may use the ICN in compliance with Federal Identity, Credential, and Access Management (FICAM). In some cases where direct VistA PIMS ADT subscription provides demographics the SSN may be transmitted but is not processed or stored in any data field(s). In addition, the following medical record information is retained in TIFF or PDF format:

1) Sending facility
2) Primary Language
3) Patient Class
4) Admitting/Attending Physician
5) Insurer
6) Primary Diagnosis
7) Allergies
8) Patient Demographics (face sheet)
9) Patient Unit/Ward and Room location
10) Visit ID
11) Admission Date
12) Transition of level of care
13) Estimated discharge date
14) Date medically cleared to leave
15) Health Summaries/Reports
16) Consult Reports
17) Full TIU Notes, Lab, Radiology, Consult Reports, Health Summaries, etc.

PII Mapping of Components (Servers/Database)

Ensocare consists of 1 server/database. This db has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Ensocare 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 the server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

Internal Database Connections

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
Ensocare	Yes	Yes	•First/Last Name •Sending facility •ICN/MRN •Visit ID	First/Last Name, Sending Facility, Visit ID gender, dob	ICN/MRN used instead of patient social

			•DoB •Gender •Address (street, city, state, zip/postal code) •Phone number(s) •Primary Language •Patient Class •Patient Location (Ward/Room) •Admitting/Attending Physician •Next of Kin •Insurer •Admit Date •Primary Diagnosis •Allergies •Vital Signs •Diet Restrictions •Durable Medical Equipment Orders •Mental/Behavioral Health Status •Precautions •Respiratory status •Special Treatments (e.g., chemo, suctioning, vent, etc.)	and location to create patient context within the system First/Last name, gender and remaining data elements provide discharge planners and case managers patients administrative information so that the information is available to the staff at the post-acute care facility that is reviewing the Veteran patient for acceptance as part of the referral packet as part of the referral packet	Security number

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 demographic and medical record information is provided by one or more sources including:

- Vista/CPRS
- VDIF
- Cerner
- Manual entry by VA Social Workers or other staff acting as Case Managers

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.

NA—no PII is collected from external sources

1.2c If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

NA

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?

PII is collected via electronic transmission e.g., HL7 or API from VistA, VDIF and/or Cerner; in addition, and VA staff

1.3b 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.

NA

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.

The information stored in Ensocare is electronically transmitted from VA Electronic Health Record(s) and/or Health Information Exchange (e.g., Cerner, VistA and/or VDIF) or manually entered/uploaded by role-based access authorized VA staff acting as case managers from Cerner or

VistA/CPRS. Processes are implemented that ensure quality during PII collection or creation, by ensuring individuals are prompted to review provided PII information. Much of the information provided by veterans or other members of the public, such as address and phone number, next of kin and emergency contact information, and similar information are assumed to be accurate because it is provided directly by the individual. Additionally, information entered an individual's medical record by a doctor or other medical staff is also assumed to be accurate and is not verified

1.4b 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.

NA

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

Title 38, United States Code, section 7301(a).
Title 38 United States Code Section 501.
Title 38, United States Code, Sections 501(b) and 304.
Veterans Health Administration – Organization and Functions, Title 38, U.S.C., Chapter 73, § 7301(a)
Health Insurance Portability and Accountability Act of 1996 (HIPAA)
Privacy Act of 1974
24VA10A7 – Patient Medical Records -VA: Title 38, United States Code, Sections 501(b) and 304
79VA10 – Veterans Health Information Systems and Technology Architecture (VISTA) Records ; Title 38, United States Code, section 7301(a), 121 VA10A7 – National Patient Database - VA.

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

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

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

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

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 system collects, processes, and retains PII and PHI on Veterans and on Members of the Public. If this information was breached or accidentally disclosed to inappropriate parties or the public, it could result in personal and financial harm to the individuals impacted and adverse negative effect to the VA.

Mitigation: Data collected, processed, and retained will be protected in accordance with VA Handbook 6500 and FIPS 140-2 encryption and data in-transit protection standards. All systems and individuals with access to the system will be approved, authorized, and authenticated before access is granted. VA annual privacy and security training compliance will be enforced for all VA employees, contractors, and vendors

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.

The National Office of Social Work Services has assumed the role of business owner for Ensocare Automated Discharge Planning. The solution will allow VA social workers and other VA staff acting as case managers to automate care coordination with non-VA providers and agencies improving throughput and access to care. This automation software and its technology-enabled services will manage care transitions via referrals and placement to non-VA points of care and care providers. This efficiency supports VA Social Works mission to help in resolving challenges to Veteran's health and wellbeing by connecting Veterans with services and programs to meet their emergent needs without lapsed time or having to wait for manual processes using paper and faxed information.VA staff users requirements as defined in the VA WC20200708 Automated Patient Discharge Interface Requirements Traceability Matrix (RTM) include the ability to provide patient demographic and clinical information as outlined in section 1.1 on demand, dynamically so the receiving facility has complete demographic, administrative, and clinical information for the patient being referred for acceptance. .

The following PII data elements are received from VistA, VDIF and/or Cerner and used to create patient context within the system enabling users to find the patient and populate referral packets for community providers, agencies and/or services:

- Admission Date
- Date of Birth
- Integrated Control Number (ICN)—required by FICAM
- MRN
- Name
- Patient Class
- Patient Location (Ward/Room)
- Sending facility
- Visit ID

The Social Security Number is transmitted to Ensocare when interfaced to VistA by default—this data element is not used for any business purpose.

The following administrative/demographic data elements are received from VistA, VDIF and/or Cerner providing required referral information by community providers, agencies and/or services :

- Admitting/Attending Physician
- Date medically cleared to leave
- Estimated discharge date
- Gender
- Insurer
- Next of Kin
- Patient Demographics (face sheet   )
- Personal Mailing Address
- Personal Phone Number(s)
- Primary Language

The following PHI data elements are received from VistA, VDIF and/or Cerner providing required information to determine clinical appropriateness for acceptance of a referral by community providers, agencies and/or services:

- Allergies
- Consult Reports
- Diet Restrictions
- Durable Medical Equipment Orders
- Full TIU Notes, Lab, Radiology, Consult Reports, Health Summaries, etc.
- Health Summaries/Reports
- Medical Records
- Medications
- Mental/Behavioral Health Status

- Precautions
- Primary Diagnosis
- Respiratory status
- Special Treatments (e.g., chemo, suctioning, vent, etc.)
- Transition of level of care
- Vital Signs

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.

While Ensocare is not the system of record, we inherit data from VA system(s) of record. Ensocare analysis of data received is limited to the internal application logical rules to validate data values as correct in format and value (e.g. DOB cannot be in the future). During implementation resources manually validate and verify the data transmitted in respective interface(s)—HL7, API, and/or SSOi

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.

NA

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?

Ensocare uses SSL to protect data in transit and TDE AES-256 at rest

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

Ensocare may leverage VA PIMS ADT messaging which may by default send SSN in PID segments 3 and/or 19. If/when Ensocare receives a SSN it is stored in our MIRTH DB for no more than 30 days as a row of the original HL7 message. Ensocare does not transmit, pass through or display the SSN as part of our VAEC/AWS instance of the application Encryption:At rest: TDE AES-256In transit: SSLAccess Control: Access to the MIRTH DB requires Active PIV and NMEA/OAuth Account to RDP from VA desktop to VAEC/AWS Ensocare Report ServerApproved ePAS and assignment for the following group membership(s):VA\cldunixp_userprofiles VA\cldwins_vaec_aws_ens_dba_stage VA\cldwins_vaec_aws_ens_dba_prod OPS: VA\cldwins_vaec_aws_ens_admin_dba_prod VA\cldwins_vaec_aws_ens_admin_dba_stage

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

VA Privacy Service in conjunction with the Senior Agency Official for Privacy (SAOP), the Privacy Compliance Assurance Office, and the Office of Enterprise Risk Management (ERM) are responsible for monitoring and auditing privacy controls continuously. The Privacy Compliance Assurance Office provides privacy compliance assessment tools for monitoring compliance.

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?

Ensocare is a PIV compliant solution using VA IAM SSOi OAuth for system authentication and AD role assignment for privileged access and IAM PROV interface for application authorization. Ensocare follows VA/VAEC policy and procedures for privileged system and standard user access. Privileged users are granted access to Ensocare after approval by supervisor and the VA elevated privileges process including VAEC Workflow Manager and ePAS request approval, creation of NMEA accounts and user assignment standard AD groups. Access to Ensocare is granted according to role-based access controls in compliance with minimum necessary permissions and/or access to perform job functions. Standard application users are provisioned in IAM PROV as either ENS_EndUser or ENS_REPORTVUSER by facility identified approvers for system access. Ensocare will review access to the the systems on a bi-annual basis. In addition, for VDIF integrated sites—VDIF will add an LDAP interface to validate user access to clinical documentation

Yes

2.4c Does access require manager approval?

Yes

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

Yes

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

The organization develops a comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures. VA Privacy Service in conjunction with the Information Technology Workforce Development (ITWD) are responsible for developing a training and awareness strategy verifying that personnel understand privacy roles and responsibilities, privacy policy, and privacy 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*

The following information is retained a in a TIFF file…. And MRN number is used instead of patient's social security number

1) Patient Demographics (face sheet)
   a. First/Last Name
   b. Sending facility
   c. ICN/MRN
   d. Visit ID
   e. DoB
   f. Gender
   g. Address (street, city, state, zip/postal code)
   h. Phone number(s)
   i. Primary Language
   j. Patient Class
   k. Patient Location (Ward/Room)
   l. Admitting/Attending Physician
   m. Next of Kin
   n. •Insurer
   o. •Admit Date
2) Patient Unit/Ward and Room location
3) Visit ID
4) Admission Date
5) Transition of level of care
6) Estimated discharge date

7) Date medically cleared to leave
8) Health Summaries/Reports
9) Consult Reports
10) Other TIU/Progress Notes
    a. History & Physical
    b. Medication Reconciliation
    c. Physical Therapy Eval
    d. Dialysis notes (if applicable)
    e. Wound care notes (if applicable)
    f. Most recent physical therapy notes (PM&R) Physical Medicine and Rehabilitation
    g. Most recent progress notes by MD
    h. (SW GEC) Social Work Geriatric Extended Care Assessment

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.*

The information is retained in Ensocare until the action is completed and the Veteran is placed in a facility.

Information covered by 24VA10A7: In accordance with the records disposition authority approved by the Archivist of the United States, paper records and information stored on electronic storage media are maintained for seventy-five (75) years after the last episode of patient care and then destroyed/or deleted. VHA Records Control Schedule (RCS 10–1), Chapter 66000.1d (N1–15–91–6, Item 1d) and 6000.2b (N1–15–02–3, Item 3).
Information Covered by 79VA10: RCS 10–1, Item 2000.2 Information Technology Operations and Maintenance Records destroy 3 years after agreement, control measures, procedures, project, activity, or when transaction is obsolete, completed, terminated or superseded, but longer retention is authorized if required for business use (DAA–GRS–2013–0005– 0004, item 020). RCS10–1, Item 2100.3 2100.3, System Access Records destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use (DAA–GRS–2013–0006– 0004, item 31).
Information covered by 121VA10A7: The records are disposed of in accordance with General Records Schedule 20, item 4. Item 4 provides for deletion of data files when the agency determines that the files are no longer needed for administrative, legal, audit, or other operational purposes.

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?

Medical Records Folder File or CHR (Consolidated Health Record) contains all professional and administrative material necessary to document the episodes of medical care and benefits provided to individuals by the VA health care system. The medical records folder will be retained in the VA health care facility until 3 years after last episode of care, and then converted to an inactive medical record. Once designated an inactive medical record, it will be moved to a VA records storage facility. Patient medical records are retained for a total of 75 years after the last episode of care. (Department of Veterans Affairs Record Control Schedule (RCS)-10, Chapter Six Health Care Records, Item No. III-6-1 (January 2019).

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

Medical Records Folder File or CHR (Consolidated Health Record) contains all professional and administrative material necessary to document the episodes of medical care and benefits provided to individuals by the VA health care system. The medical records folder will be retained in the VA health care facility until 3 years after last episode of care, and then converted to an inactive medical record. Once designated an inactive medical record, it will be moved to a VA records storage facility. Patient medical records are retained for a total of 75 years after the last episode of care. (Department of Veterans Affairs Record Control Schedule (RCS)-10, Chapter Six Health Care Records, Item No. III-6-1 (January 2019).

79VA10 RCS 10–1, Item 2000.2 Information Technology Operations and Maintenance Records destroy 3 years after agreement, control measures, procedures, project, activity, or when transaction is obsolete, completed, terminated or superseded, but longer retention is authorized if required for business use (DAA–GRS–2013–0005– 0004, item 020). RCS10–1, Item 2100.3 2100.3, System Access Records destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use (DAA–GRS–2013–0006– 0004, item 31).

24VA10A7: In accordance with the records disposition authority approved by the Archivist of the United States, paper records and information stored on electronic storage media are maintained for seventy-five (75) years after the last episode of patient care and then destroyed/or deleted. VHA Records Control Schedule (RCS 10–1), Chapter 6, 6000.1d (N1–15–91–6, Item 1d) and 6000.2b (N1–15–02–3, Item 3).

3.4 What are the procedures for the elimination or transfer of SPI?

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

SPI is disposed of, destroyed, erased, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and uses organization-defined techniques or methods to ensure secure deletion or destruction of PII (including originals, copies, and archived records).

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.

If PII must be used, organizations take measures to minimize any associated risks and to authorize the use of and limit the amount of PII for these purposes. The Senior Agency Official for Privacy (SAOP) is responsible for developing and documenting policies and procedures within the privacy plan to minimize personally identifiable information (PII) within a test, development, training, research, or preproduction environment. VA research investigators use PII for VA Institutional Review Board (IRB) approved research. Organizations consult with the SAOP/CPO and legal counsel to ensure that the use of PII in testing, training, and research is compatible with the original purpose for which it was collected.

3.6 <u>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:

<u>Principle of Minimization:</u> 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?

<u>Principle of Data Quality and Integrity:</u> 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: Only information necessary to obtain the appropriate facility for the Veteran. A MRN is used in place of Veteran's social security number, and information entered is only available in the Ensocare system until the Veteran is accepted and placed in a facility

Mitigation: In addition to collecting and retaining only information necessary for fulfilling the VA mission, the disposition of data housed is based on standards developed by the National Archives Records Administration (NARA). This ensures that data is held for only as long as necessary, in this case until the Veteran is accepted and transferred to a facility.

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***
VistA and/or VDIF	The data elements are used to create patient context within the system enabling users to find the patient and populate referral packets and determine clinical appropriateness for acceptance of a referral by community providers, agencies and/or services	• First/Last Name • Sending facility • ID/MRN = ICN • SSN • Visit ID • DoB • Gender • Address (street, city, state, • zip/postal code) • Phone number(s) • Primary Language • Patient Class • Patient Location (Ward/Room) • Admitting/Attending Physician • Next of Kin • Insurer • Admit Date • Primary Diagnosis • Allergies • Vital Signs • Diet Restrictions • Durable Medical Equipment • Orders • Mental/Behavioral Health • Status • Precautions • Respitory status • Special Treatments (e.g., • chemo, suctioning, vent, etc.) • Other administrative and • clinical data can be manually • entered including: • Transition level of care	Secure connection using secure socket layer (SSL) with certificates HTTPS HL7

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***
		• Prognosis • Patient knows/understanding • of diagnosis • Expected discharge date • Date medically cleared to • leave • Full TIU Notes, Lab, • Radiology, Consult Reports, • Health Summaries, etc	

4.2 <u>PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure</u>

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

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

Follow the format below:

<u>Privacy Risk</u>: The internal sharing of data is necessary for individuals to receive VHA benefits, however, there is a risk that the data could be shared with an inappropriate VA organization or institution which could result in a breach of privacy and disclosure of PII/PHI to unintended parties or recipients.

<u>Mitigation</u>: Safeguards implemented to ensure data is not sent to the wrong VA organization are employee security and privacy training and awareness and required reporting of suspicious activity. Use of secure passwords, access for need-to-know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized within the facilities. Access to sensitive information and the systems where the information is stored is controlled by the VA using a “least privilege/need to know” policy. Access must be requested and only the access required by VA persons or processes acting on behalf of VA persons is to be requested or granted.

Section 5. External Sharing/Receiving and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to VA, which includes Federal, State, and local governments, and the private sector.

5.1 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

Is the sharing of information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.

NOTE: Question 3.10 on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any Federal, State, or local government agency or private sector organization with which information is shared.

For each interface with a system outside VA, state what specific data elements (PII/PHI) are shared with each specific partner.

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.
This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***

Cerner	The purpose for sharing the information is to arrange for accommodations at a facility outside in the community.	First/Last Name •Sending facility •ID/MRN = ICN •SSN •Visit ID •DoB •Gender •Address (street, city, state, zip/postal code) •Phone number(s) •Primary Language •Patient Class •Patient Location (Ward/Room) •Admitting/Attending Physician •Next of Kin •Insurer •Admit Date •Primary Diagnosis •Allergies •Vital Signs •Diet Restrictions •Durable Medical Equipment Orders •Mental/Behavioral Health Status •Precautions •Respitory status •Special Treatments (e.g., chemo, suctioning, vent, etc.) Other administrative and clinical data can be manually entered including: •Transition level of care •Prognosis •Patient knows/understanding of diagnosis •Expected discharge date •Date medically cleared to leave Full TIU Notes, Lab, Radiology, Consult Reports, Health Summaries, et	HTTPS	ICD—per ISSO, no MOU ISA required as AO is same for both systems

•

5.2 <u>PRIVACY IMPACT ASSESSMENT: External sharing and disclosure</u>

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

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

Follow the format below:

Privacy Risk: : The system collects, processes, and retains PII and PHI on Veterans and on Members of the Public. If this information was breached or accidentally disclosed to inappropriate parties or the public, it could result in personal and financial harm to the individuals impacted and adverse negative effect to the VA.

Mitigation: Data collected, processed, and retained will be protected in accordance with VA Handbook 6500 and FIPS 140-2 encryption and data in-transit protection standards. All systems and individuals with access to the system will be approved, authorized, and authenticated before access is granted. VA annual privacy and security training compliance will be enforced for all VA employees, contractors, and vendors Section 6. Appendix C

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 Notice of Privacy Practice (NOPP) is a document which explains the collection and use of protected information to individuals applying for VHA benefits. Major changes are mailed out every three years to all VHA beneficiaries.
The Department of Veterans Affairs provides additional notice of this system by publishing the System of Record Notices (SORNs): This Privacy Impact Assessment (PIA) also serves as notice of the Enterprise VistA System. As required by the eGovernment Act of 2002, Pub.L. 107–347

§208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means."

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

https://vaww.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

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

The notice is mailed to all beneficiaries and can be accessed on line https://vaww.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946. A copy of the notice is available at every VHA medical center. Notice is also provided in the applicable SORN and in this PIA.

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.

The Veterans' Health Administration (VHA) as well as the individual facilities request only information necessary to administer benefits to veterans and other potential beneficiaries. While an individual may choose not to provide information to the VHA, this will prevent them from obtaining the benefits necessary to them.

Employees and VA contractors are also required to provide the requested information to maintain employment or their contract with the VA.

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.

VHA permits individuals to agree to the collection and to the consent to the use of

their personally identifiable information (PII) through the use of 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. If the individual does not want their information collected or used, then they do not sign the consent form.
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 (NOPP) and conversations with VHA employees. VA Forms are reviewed by VHACO periodically to ensure compliance with 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 have a right to deny the use of their health information and/or IIHI and for the purpose of research.
Individuals can request further limitations on other disclosures. A veteran, guardian or court appointed Power of Attorney can submit a request to the facility Privacy Officer to obtain information. The facility can approve or deny these requests. However, if the request to provide information is accepted the facility must conform to the restrictions

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: There is a risk that an individual may not understand why their information is being collected or maintained about them.

Mitigation: This risk is mitigated by the common practice of providing the NOPP when Veterans apply for benefits. Additionally, new NOPPs are mailed to beneficiaries when there is a change in regulation. Employees and contractors are required to review, sign and abide by the National Rules of Behavior on a yearly basis as required by VA Handbook 6500 as well as complete annual mandatory Information Security and Privacy Awareness training. Additional mitigation is provided by making the System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) available for review online

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.***

There are several ways a veteran or other beneficiary may access information about them. The Department of Veterans' Affairs has created the MyHealtheVet program to allow online access to their medical records. More information on this program and how to sign up to participate can be found online at HTTPs://www.myhealth.va.gov/index.html. Veterans and other individuals may also request copies of their medical records and other records containing personal data from the medical facility's Release of Information (ROI) office

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).

NA

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.

NA

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.*

The procedure for correcting inaccurate or erroneous information begins with a Veteran requesting the records in question from Release of Information (ROI). The Veteran then crosses out the information they feel is inaccurate or erroneous from the records and writing in what the Veteran believes to be accurate. 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. Employees should contact their immediate supervisor and Human Resources to correct inaccurate or erroneous information. Contractors should contact Contract Officer Representative to correct inaccurate or erroneous information upon request.

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 can also be obtained by contacting the facility ROI office.

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.

NA

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

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

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

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

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

Follow the format below:

<u>Privacy Risk:</u> There is a risk that a Veteran does not know how to obtain access to their records or how to request corrections to their records and that the health record could contain inaccurate information and subsequently effect the care the Veterans receive

<u>Mitigation:</u> The Notice of Privacy Practice (NOPP), which every patient receives when they enroll, discusses the process for requesting an amendment to one's records. The VHA staffs Release of Information (ROI) offices at facilities to assist Veterans with obtaining access to their health l records and other records containing personal information. The Veterans' Health Administration (VHA) established My HealtheVet program to provide Veterans remote access to their health records. The Veteran must enroll to obtain access to all the available features. In addition, Privacy and Release of Information Directive 1605.01 establishes procedures for Veterans to have their records amended where appropriate.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system, and are they documented?

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.

Access to the system by VA staff and contractors follow standard VA Handbook 6500 requirements including standard HIPAA/Privacy and role-based training(s), signed rules of behavior, fingerprinting, background check based on position risk categorization. Authentication Authorization via IAM integrations for SSOi and PROV respectively. PROV role-based access is assigned by facility specific application-level administrators ‘approvers’. System Administrators are authorized using ePAS managed AD accounts requiring NMEA and eTokens.

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?

HIPAA covered entities and VA Business Associates.

VA employee i.e., Social worker, Nurse Case Managers are SSOi authenticated/PROV authorized users of Ensocare having completed both the HIPAA and Information Security training enter information for Ensocare Users of to view and accept the Veteran for transfer to their facility or provision of service.

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.

Read only of VA provided information

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.

ABOUT Staff are classified as contractors. ABOUT Is a subcontractor to covered business associates. Further, Ensocare is classified as a managed service and as with VA employees’ access to the system by VA staff and contractors follow standard VA Handbook 6500 requirements including standard HIPAA/Privacy and role-based training(s), signed rules of behavior, fingerprinting, background check based on position risk categorization. Authentication Authorization via IAM integrations for SSOi and PROV respectively. PROV role-based access is assigned by facility specific application-level administrators ‘approvers’. System Administrators are authorized using ePAS managed AD accounts requiring NMEA and eTokens.

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.

Standard TMS HIPAA/Privacy training is required of all VA and contractor users. Privileged users require specific role-based trainings based on role classifications.

Applicable Roles	**TMS Course and Title**
Required for IT personnel ONLY	3197 Information Security Role-Based Training for IT Specialist
Required for EVERYONE (IT personnel included). Additionally, for any roles selected in the MyVA EPAS that DOES NOT clearly map to a specific Role-Based training below, this training will serve as the 'catch all' role-based training (i.e., Applications, etc.)	3867205 Training for Elevated Privileges for System Access
Any reference to Software Developers in either the role or in the role justification of the 'Granted' section.	1016925 Information Security Role-Based Training for Software Developers
Any reference to the following in the role or in the role justification of the 'Granted' section: • System Administrator • Group • Privileges to a Laptop or Workstation • VistA Imaging • VistA Management • Database Manager (must also have 1357084)	1357076 Information Security Role-Based Training for System Administrators
Any reference to Data Manager in either the role or in the role justification of the 'Granted' section.	1357084 Information Security Role-Based Training for Data Managers
Any reference to Network Administrator in either the role or in the role justification of the 'Granted' section.	1357083 Information Security Role-Based Training for Network Administrators

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

8.4a If yes, provide:

1. *The Security Plan Status:* Yes
2. *The System Security Plan Status Date:* 6/16/2022
3. *The Authorization Status:* Authorized
4. *The Authorization Date:* 6/16/2022
5. *The Authorization Termination Date:* 6/16/2023
6. *The Risk Review Completion Date:* 3/17/2022
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH Moderate*

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

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

10/30/2019

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)*

Ensocare provides VA social workers and other providers, care coordination software and technology-enabled services to smoothly manage care transitions, enable remote monitoring in real-time and connect all caregivers around a unified goal: The Veteran. Ensocare provides the VA services and solutions which will enable patients to move more efficiently and effortlessly through the care continuum. Every step of the patient's transitioning care can be coordinated, from hospital discharge to post-acute placement or recovery at home, and all points in between by providing an automated solution The Ensocare solution addresses those manual processes, helping hospitals wrest back efficiency in what has historically been an inefficient system. This functionality, working in concert with VDIF, VistA/CPRS or Cerner lets case managers use software to instantly communicate with post-acute providers. After reviewing prospective post-acute providers with the patient, right at the bedside, it takes just a few clicks to send the referral to their chosen providers, who can then respond in their own PAC-facing version of the app. Instead of standing by a fax machine and waiting, or playing phone tag with

those PACs, the response of "Yes," "No" or "Maybe" gets sent right away, electronically,
Privacy Threshold Analysis
Template Version Date: October 1, 2021
Page 5 of 16
bringing the median response rate down to 30 minutes from what was previously hours or even days. Automated pass through of information from current point of care to needed point of care.

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.*

Please provide response here

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.

Please provide response here

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.

Please provide response here

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).

Please provide response here

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 they provided in this Privacy Impact Assessment is true and accurate.

NANCY KATZ-JOHNSON

Digitally signed by NANCY KATZ-JOHNSON
Date: 2023.01.31 13:08:20 -05'00'

Privacy Officer,

CRYSTAL L. WHITE 134339

Digitally signed by CRYSTAL L. WHITE 134339
Date: 2023.01.24 10:06:18 -05'00'

Information System Security Officer,

Angela Gant-Curtis 105447

Digitally signed by Angela Gant-Curtis 105447
Date: 2023.01.23 11:12:59 -06'00'

Information System Owner,

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).

https://vaww.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

PIV Complian SSOi via OAuth presents standard VA privacy notice.

HELPFUL LINKS:

Record Control Schedules:

https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

General Records Schedule 1.1: Financial Management and Reporting Records (FSC):

https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

National Archives (Federal Records Management):

https://www.archives.gov/records-mgmt/grs

VHA Publications:

https://www.va.gov/vhapublications/publications.cfm?Pub=2

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