Privacy Impact Assessment for the VA IT System called:

Ensocare Assessing

Veteran’s Health Administration

National office Social Work

eMASS ID: #788

Date PIA submitted for review:

12/4/2024

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)	Youlanda Howard	Youlanda.howard@va.gov	501-257-2084
Information System Owner	Angela Gant-Curtis	Angela. Gant-Curtis	520-342-6903

Abstract

Ensocare is a comprehensive web-based transitional care program that is currently used by VA Medical Centers and post-acute care providers connecting hospital personnel with more than 68,000 providers (HIPPA Covered Entities and Business Associates); matching a patient's clinical needs and quality of life wants with available-bed skilled nursing facilities, assisted living, home health, home care, hospice, DME and long-term care facilities.

Ensocare guides Social Workers, Care Managers, or Discharge Planners through the post-acute case management process and then sends electronic referral information to any selected post-acute providers for referral acceptance. Once alerted, via email, text or pager, or facsimile (future) the post-acute providers log into a Health Insurance Portability and Accountability Act (HIPAA)- secure site to review relevant patient information and inform the hospital of its ability to take a particular patient or to request additional information.

Overview

The overview is the most important section of the Privacy Impact Assessment (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 business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?*
Ensocare allows VA social workers and other VA staff acting as case managers to automate care coordination with referrals and placement requests to non-VA HIPAA Covered Entities and Business Associates. This efficiency supports VA goals to improve access to care and Social Work's 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.

B. *Who is the owner or has control of the IT system or project? If the system has an eMASS entry, ensure this information matches with the eMASS entry.*
Ensocare ATO/ATC (eMASS ID: 788) authorized Vendor managed IaaS is hosted within the VAEC/AWS environment. The solution is available for use VA wide, as an embedded API in Cerner or as a direct to end user solution for legacy VistA/CPRS facilities. Business Ownership – National Office of Social Work

2. Information Collection and Sharing

C. *Indicate the expected number of individuals whose information is stored in the system and include 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. *Current number of live or in flight VAMCs: 30.*

Check if Applicable	Demographic of individuals
☒	Veterans or Dependents
☒	VA Employees
☒	Clinical Trainees
☒	VA Contractors
☒	Members of the Public/Individuals
☐	Volunteers

D. *What is a general description of the information in the IT system and the purpose for collecting this information?*
Information received, stored and transmitted includes Veteran PII and PHI as well as publicly available end user information (PII) can include but is not limited to the following: demographics included in a cover sheet based on ADT message content, clinical documentation such as; allergies, vital signs, current medications, dietary orders, precautions, respiratory status, and current treatment requirements.

E. *What information sharing is conducted by the IT system? A general description of the modules and components, where relevant, and their functions.*
Ensocare receives data from
- IAM related to end users for authentication and authorization
- System(s) of Record including VistA, VDIF and/or Cerner.

Ensocare will transmit PHI/PII data via ECFax to external HIPAA Covered Entities and Business Associates

F. *Are the modules/subsystems only applicable if information is shared?*
Yes, the modules/subsystems are applicable because the system receive, store, or share data with the component/modules/subsystems.

G. *Is the system operated in more than one site to include primary and secondary 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.

- 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 data.

Indeterminate of source of PHI/PII the use of the system is PIV SSO compliant limited to VA credentialed IAM provisioned staff referring the Veteran patient for services and/or placement to HIPAA Covered Entities and Business Associates using multifactor authentication.

3. Legal Authority and System of Record Notices (SORN)

H. What is the citation of the legal authority?

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).

12110A7 -National Patient Database – VA - Title 38 United States Code Section 50

I. What is the SORN?

Patient Medical Records–VA (24VA10A7)

Veterans Health Information Systems and Technology Architecture (VistA) Records-VA (79VA10).

National Patient Databases-VA'' (121VA10)

J. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval.

No

4. System Changes

a. Will the business processes change due to the information collection and sharing?

☐ Yes
☒ No
if yes, <<ADD ANSWER HERE>>

b. Will the technology changes impact information collection and sharing?

☐ Yes
☒ No

if yes, <<ADD ANSWER HERE>>

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 Information 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
☒ **Full** Social Security Number
☐ **Partial** 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/Sex
☒ Integrated Control Number (ICN)
☐ Military History/Service Connection
☒ Next of Kin
☐ Date of Death
☐ Business Email Address
☐ Electronic Data Interchange Personal Identifier (EDIPI) ☐ Other Data Elements (list below)

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

The following Veteran or Dependent information record information is received/retained:

1.) Sending facility
2.) Visit ID
3.) Primary Language
4.) Patient Class
5.) Patient location (ward/room)
6.) Next of Kin
7.) Admitting/Attending Physician
8.) Insurer
9.) Admit Date
10.) Primary Diagnosis
11.) Allergies
12.) Vital Signs
13.) Diet Order/Restrictions
14.) VistA IEN
15.) Active Problems
16.) Durable Medical Equipment Orders
17.) Mental Behavioral Health Status
18.) Precautions
19.) Respiratory Status
20.) Special Treatments (e.g., chemo, suctioning, vent, etc.)
21.) Transition of level of care
22.) Expected discharge date
23.) Date medically cleared to leave
24.) Health Summaries/Reports
25.) Consult Reports
26.) History & Physical(s)
27.) Full TIU Notes (Prognosis, patient understanding of diagnosis, physical therapy eval, dialysis notes, wound care notes, physical therapy notes PM&R,), Lab, Radiology, Consult Reports, etc.
28.) Medication Reconciliation

The following user (VA Employees, Contractors, Clinical Trainees) information is received and retained:

1) Work email
2) First and Last Name
3) FedIAMSecID.

The following public information is received/retained:

1) Name
2) Phone
3) Business Address
4) Email
5) Username
6) Password

1.2 List 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?
VistA/CPRS – via VA middleware known as VDIF (Veterans Data Integration and Federation Enterprise Platform) REST API, Manual entry/upload by VA staff authenticated and authorized to the system via VA SSOi and IAM Provisioning and Active Directory.

Oracle Cerner via embedded API

IAM SSOi Oauth

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.

Ensocare does not collect PII/PHI from external Sources. Publicly accessible provider data is received and stored from Centers for Medicare and Medicaid Services related quality ratings.

1.2c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?
No, Ensocare does not create information – it serves as a pass through.

1.3 Methods of information collection

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 API electronic transmission from VDIF (VistA/CPRS), Cerner and/or manual entry by authenticated/authorized end users.

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?

Information is not collected on a form.

1.4 Information checks for accuracy, and 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 via VDIF. 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 demographic 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 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?

No commercial aggregator is in use or referenced in contract(s)

1.5 Identify the specific legal authorities, arrangements, and agreements that 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:

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

Principle of Minimization: *The information is directly relevant and necessary to accomplish the specific purposes of the program.*

Principle of Individual Participation: *The program, to the extent possible and practical, collects information directly from the individual.*

Principle of Data Quality and Integrity: *VA policies and procedures must ensure that personally identifiable information is accurate, complete, and current.*
This 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 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	File Identification purposes	Provides required referral information by community providers, agencies and/or services

PII/PHI Data Element	Internal Use	External Use
Date of Birth	File Identification purposes	Provides required referral information by community providers, agencies and/or services
SSN	Not Used	Not Used
Integrated Control Number (ICN)	File Identification purposes	Not Used
VistA IEN	File Identification purposes	Not Used
Patient Class	File Identification purposes	Not Used
Patient Location	File Identification purposes	Provides required referral information by community providers, agencies and/or services
Sending Facility/User	File Identification purposes	Provides required referral information by community providers, agencies and/or services
Visit ID	File Identification purposes	Not Used
Admitting/Attending Physician	Not Used	Provides required referral information by community providers, agencies and/or services
Expected discharge date	Not Used	Provides required referral information by community providers, agencies and/or services
Gender	Not Used	Provides required referral information by community providers, agencies and/or services
Insurer	Not Used	Provides required referral information by community providers, agencies and/or services
Personal Phone Number	Not Used	Provides required referral information by community providers, agencies and/or services
Personal Address	Not Used	Provides required referral information by community providers, agencies and/or services
Primary Language	Not Used	Provides required referral information by community providers, agencies and/or services

PII/PHI Data Element	Internal Use	External Use
Active Problems	Not Used	Provides required information to determine clinical appropriateness for acceptance of a referral by community providers, agencies and/or services
Primary Diagnosis	Not Used	Provides required information to determine clinical appropriateness for acceptance of a referral by community providers, agencies and/or services
Allergies	Not Used	Provides required information to determine clinical appropriateness for acceptance of a referral by community providers, agencies and/or services
Consult Reports	Not Used	Provides required information to determine clinical appropriateness for acceptance of a referral by community providers, agencies and/or services
Diet Orders/Restrictions	Not Used	Provides required information to determine clinical appropriateness for acceptance of a referral by community providers, agencies and/or services
Durable Medical Equipment Orders	Not Used	Provides required information to determine clinical appropriateness for acceptance of a referral by community providers, agencies and/or services
Full TIU Notes (Prognosis, patient understanding of diagnosis, date medically cleared to leave, physical therapy eval, dialysis notes, wound care notes, physical therapy notes PM&R, Medicine and rehabilitation, most recent notes by MD (SW GEC) Social work Geriatric Extended Care Assessment)	Not Used	Provides required information to determine clinical appropriateness for acceptance of a referral by community providers, agencies and/or services

PII/PHI Data Element	Internal Use	External Use
Lab Orders/Results	Not Used	Provides required information to determine clinical appropriateness for acceptance of a referral by community providers, agencies and/or services
Radiology Orders/Results	Not Used	Provides required information to determine clinical appropriateness for acceptance of a referral by community providers, agencies and/or services
Vital Signs	Not Used	Provides required information to determine clinical appropriateness for acceptance of a referral by community providers, agencies and/or services
Medications	Not Used	Provides required information to determine clinical appropriateness for acceptance of a referral by community providers, agencies and/or services
Mental/Behavioral Health Status	Not Used	Provides required information to determine clinical appropriateness for acceptance of a referral by community providers, agencies and/or services
Precautions	Not Used	Provides required information to determine clinical appropriateness for acceptance of a referral by community providers, agencies and/or services
Respiratory Status	Not Used	Provides required information to determine clinical appropriateness for acceptance of a referral by community providers, agencies and/or services
Special Treatments	Not Used	Provides required information to determine clinical appropriateness for acceptance of a referral by community

PII/PHI Data Element	Internal Use	External Use
		providers, agencies and/or services
Transition of Level of Care	Not Used	Provides required information to determine clinical appropriateness for acceptance of a referral by community providers, agencies and/or services

2.2 Describe the types of tools 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.

Ensocare does not create or make new data available regarding an individual.

2.3 How the information in the system is 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 and/or HTTPS/TLS ≥1.2 FIPS Certificate4523 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? (refer to PTA question 3.8).

Ensocare historically leveraged VA PIMS ADT messaging which by default send SSN in PID segments 3 and/or 19. If/when Ensocare receives an 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 Server Approved 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 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u>

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:

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

<u>Principle of Use Limitation:</u> 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 Personal Identity Verification (PIV) compliant solution using VA Identity Access Management (IAM) Single Sign On Integeration 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 Non-mail Enabled Account (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 systems on a bi-annual basis. In addition, for VDIF integrated sites—VDIF clinical summary access is authorized via Lightweight Directory Access Protocol (LDAP) interface to validate user access to clinical documentation.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented? How are the documented, i.e. Policy, SOP, other. And where is this documentation located?

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 as identified in eMASS?

The organization leverages the VA' existing 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*

1.) Name
2.) Date of Birth
3.) SSN
4.) Integrated Control Number

5.) IEN
6.) Patient Class
7.) Patient Location
8.) Sending Facility/User
9.) Visit ID
10.) Admitting/Attending Physician
11.) Expected discharge date
12.) Gender
13.) Insurer
14.) Personal Phone Number
15.) Personal Address
16.) Primary Language
17.) Active Problems
18.) Diagnosis
19.) Allergies
20.) Consult Reports
21.) Diet Orders/Restrictions
22.) Durable Medical Equipment Orders
23.) Full TIU Notes (Prognosis, patient understanding of diagnosis, date medically cleared to leave, physical therapy eval, dialysis notes, wound care notes, physical therapy notes PM&R, Medicine and rehabilitation, most recent notes by MD (SW GEC) Social work Geriatric Extended Care Assessment)
24.) Lab Orders/Results
25.) Radiology Orders/Results
26.) Vital Signs
27.) Medications
28.) Mental/Behavioral Health Status
29.) Precautions
30.) Respitory Status
31.) Special Treatments
32.) Transition of Level of Care

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 https://www.archives.gov/records-mgmt/grs? 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 / 85 FR 62406: Patient Medical Records-VA 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 The retention schedule 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. Please work with the system 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). by 24VA10A7 / 85 FR 62406: Patient Medical Records-VA: 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) as defined in VA Handbook 6500.1

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 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System Privacy Officer (PO) 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: *The project retains only the information necessary for its purpose, additionally, the PII is retained only for as long as necessary and relevant to fulfill the specified purposes.*

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

Follow the format below:

Privacy Risk: There is a low risk that the system will retain information for longer than necessary which can put the records at greater risk of being breached.

Mitigation: To mitigate the risk, the system adheres to the retention schedule listed in RCS 101, where records are destroyed after 5 years. The destruction procedures are outlined in 3. 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.

PII Mapping of Components

4.1a Ensocare Assessing consists of **4** 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 Ensocare Assessing 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 3.9a in the PTA should be used to answer this question.

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	**Does this system collect PII? (Yes/No)**	**Does this system store PII? (Yes/No)**	**Type of PII (SSN, DOB, etc.)**	**Reason for Collection/ Storage of PII**	**Safeguards**
MIRTH	Yes	Yes	Name, Date of Birth, Personal Mailing Address, Personal Phone Number(s), Medications, Medical Records, Medical Record Number, Gender, Integrated Control Number (ICN), Sending facility, Primary Language, Patient Class, Admitting/Attending Physician, Insurer, Diagnosis, Allergies, Patient Demographics (face sheet), Patient Unit/Ward and Room location, Visit ID, Admission Date, Health Summaries/Reports, Consult Reports, (Lab, Radiology, Consult Reports, etc.), Full TIU notes (Prognosis, patient understanding of diagnosis, date medically cleared to leave, physical therapy eval, dialysis notes, wound care notes, physical therapy notes PM&R, Medicine and	Ingestion of required data for referral management	SSL and/or HTTPS/TLS ≥1.2 FIPS Certificate4523 to protect data in transit and TDE AES-256 at rest

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
			rehabilitation, most recent notes by MD (SW GEC) Social work Geriatric Extended Care Assessment)		
Mongo DB	Yes	Yes	Name, Date of Birth, Personal Mailing Address, Personal Phone Number(s), Medications, Medical Records, Medical Record Number, Gender, Integrated Control Number (ICN), Sending facility, Primary Language, Patient Class, Admitting/Attending Physician, Insurer, Diagnosis, Allergies, Patient Demographics (face sheet), Patient Unit/Ward and Room location, Visit ID, Admission Date, Transition of level of care, Estimated discharge date, Date medically cleared to leave, Health Summaries/Reports, Consult Reports, (Full	Document Caching for Cerner workflows	SSL and/or HTTPS/TLS ≥1.2 FIPS Certificate4523 to protect data in transit and TDE AES-256 at rest

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	**Does this system collect PII? (Yes/No)**	**Does this system store PII? (Yes/No)**	**Type of PII (SSN, DOB, etc.)**	**Reason for Collection/ Storage of PII**	**Safeguards**
			TIU Notes (Prognosis, patient understanding of diagnosis, date medically cleared to leave, physical therapy eval, dialysis notes, wound care notes, physical therapy notes PM&R, Medicine and rehabilitation, most recent notes by MD (SW GEC) Social work Geriatric Extended Care Assessment), Lab, Radiology, Consult Reports, etc.)		
Transition DB	Yes	Yes	Name, Date of Birth, Personal Mailing Address, Personal Phone Number(s), Medications, Medical Records, Medical Record Number, Gender, Integrated Control Number (ICN), Sending facility, Primary Language, Patient Class, Admitting/Attending Physician, Insurer, Diagnosis, Allergies, Patient Demographics	Referral case creation and management	SSL and/or HTTPS/TLS ≥1.2 FIPS Certificate4523 to protect data in transit and TDE AES-256 at rest

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
			(face sheet), Patient Unit/Ward and Room location, Visit ID, Admission Date, Transition of level of care, Estimated discharge date, Date medically cleared to leave, Health Summaries/Reports, Consult Reports, (Full TIU Notes (Prognosis, patient understanding of diagnosis, date medically cleared to leave, physical therapy eval, dialysis notes, wound care notes, physical therapy notes PM&R, Medicine and rehabilitation, most recent notes by MD (SW GEC) Social work Geriatric Extended Care Assessment), Lab, Radiology, Consult Reports, etc.)		
ADT DB	Yes	Yes	Name, Date of Birth, Personal Mailing Address, Personal Phone Number(s), Medications, Medical Records, Medical		SSL and/or HTTPS/TLS ≥1.2 FIPS Certificate4523 to protect data in transit and

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
			Record Number, Gender, Integrated Control Number (ICN), Sending facility, Primary Language, Patient Class, Admitting/Attending Physician, Insurer, Admitting Diagnosis, Patient Unit/Ward and Room location, Visit ID, Admission Date,		TDE AES-256 at rest

4.1b List internal organizations information is shared/received/transmitted, the information shared/received/transmitted, and the purpose, and how the information is transmitted.

NOTE: Question 3.9b (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

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
National SW: VDIF	Referral Management	Name, Date of Birth, Personal Mailing Address, Personal Phone Number(s), Medications, Medical Records, Medical Record Number, Gender, Integrated Control Number (ICN), Sending facility, Primary Language, Patient Class, Admitting/Attending Physician, Insurer, Diagnosis, Allergies, Patient Demographics (face sheet), Patient Unit/Ward and Room location, Visit ID, Admission Date, Transition of level of care	HTTPS TLS 1.2 or greater.1.2 REST API
National SW: Cerner	Referral Management	• 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 • Admit Date • Expected discharge date • Health Summaries/TIU Notes: • Diagnosis • Allergies • Vital Signs • Diet Orders/Restrictions • DME Orders • Mental/Behavioral Health Status • Precautions • Respiratory status • Special Treatments (e.g., chemo,	HTTPS TLS 1.2 or greater.1.2 REST API

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
		suctioning, vent, etc.) • entered including: • Transition level of care • Prognosis • Patient knows/understanding • of diagnosis • Date medically cleared to leave • Lab orders/results, • Radiology orders/results • Consult Reports, • Other administrative and clinical data can be manually	
ECFax	Referral Management	• User Oauth bearer token • X-Correlation-ID • Transaction ID• 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 • Admit Date • Expected discharge date • Health Summaries/TIU Notes: • Diagnosis • Allergies • Vital Signs • Diet Orders/Restrictions • DME Orders • Mental/Behavioral Health Status • Precautions • Respiratory status • Special Treatments (e.g., chemo, suctioning, vent, etc.) • entered including: • Transition level of care • Prognosis • Patient knows/understanding • of diagnosis • Date medically cleared to leave • Lab orders/results, • Radiology	HTTPS (TLS >1.2) JSON based64 payload

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
		orders/results • Consult Reports,	

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the VA network 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 in this section.).

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

Follow the format below:

Privacy Risk: 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.

Mitigation: 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 List the external organizations (outside VA) that information shared/received. and information shared/received, and the purpose, and how the information transmitted and what measures are taken to ensure it is secure.

The sharing of information outside the agency must be compatible with the original collection. The sharing must be covered by an appropriate routine use in a SORN. If not covered, 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 IT System or External Program Office information is shared/received with	***List the purpose of information being shared / received / transmitted***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)***	***List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
VDIF	Referral Management	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	EPIC Agreement	HTTPS TLS 1.2 or greater.1.2 REST API

		• Admit Date • Expected discharge date • Health Summaries/TIU Notes: • Diagnosis • Allergies • Vital Signs • Diet Orders/Restrictions • DME Orders • Mental/Behavioral Health Status • Precautions • Respiratory status • Special Treatments (e.g., chemo, suctioning, vent, etc.) • entered including: • Transition level of care • Prognosis • Patient knows/understanding • of diagnosis • Date medically cleared to leave • Lab orders/results, • Radiology orders/results • Consult Reports, • Other administrative and clinical data can be manually		
Cerner	Referral Management	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	ICD—per ISSO, no MOU ISA required as AO is same for both systems	HTTPS TLS 1.2 or greater.1.2 REST API

		•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		
ECFax	Referral Management	• Admit Date • 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	ICD and MOU ISA	HTTPS (REST API)

		• Expected discharge date • Date medically cleared to • leave • Full TIU Notes, Lab, • Radiology, Consult Reports, • Health Summaries, etc		

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.

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:

<u>Privacy Risk:</u> The system collects, processes, and retains PII and PHI on Veterans and publicly available PII on members of HIPAA covered entities and VA Business Associates. 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.

<u>Mitigation:</u> 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

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 The notice provided to the individual before collection of the information. Please provide a copy and/or screen shot of a web notice of the notice as an Appendix-A 6.1 on the last page of the document. (A notice may include a posted privacy policy, a Privacy Act notice on forms, notice given to individuals by the sources system, or a system of records notice published in the Federal Register.) If notice was not provided, explain why.

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 Provide the Privacy Notice provided to the public by this system or any source systems. Include a copy of the notice in Appendix A of the PIA, the Federal Register citation, or Privacy Statement from collection of information such as forms or surveys.

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

6.1b If notice was not provided, explain why.

Notice was provided and can be found here:
https://vaww.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

6.1c Provide how the notice provided at the time of collection meets the purpose of use for this system.

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

This 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 provided in the SORN

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.

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.

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 Privacy Officer (PO) 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: This is referring to sufficient notice provided to the individual.

Principle of Use Limitation: The information used only for the purpose for which notice was provided either directly to the individual or through a public notice. The procedures in place must 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 receive notice that their information is being collected, maintained, processed, or disseminated by the Veterans' Health Administration and the local facilities prior to providing the information to the VHA.

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 at least every 3 years and periodic monitoring is performed to check that all employees are aware of the requirement to provide guidance to Veterans and that the signed acknowledgment form, when applicable, is scanned into electronic records, The NOPP is also available at all VHA medical centers from the facility Privacy Officer.
The System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) are also available for review online, as discussed in question 6.1.

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 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 [VA Public Access Link-Home (efoia-host.com)](https://efoia-host.com) 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)?

The system is not exempt.

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

The system is covered by the Privacy Act

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

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed? If the correction procedures are the same as those given in question 7.1, state as much. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Individuals are required to provide a written request to amend or correct their records to the appropriate Privacy Officer or System Manager as outlined in the Privacy Act SOR. Every Privacy Act SOR contains information on Contesting Record Procedure which informs the individual who to contact for redress. The VHA Notice of Privacy Practices also informs individuals how to file an amendment request with VHA.

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

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

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

Formal redress is provided.

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 Privacy Officer (PO) to complete all Privacy Risk questions in this section).*

Consider the following FIPPs below to assist in providing a response:
<u>Principle of Individual Participation:</u> The individual must be provided with the ability to find out whether a project maintains a record relating to them.

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

<u>Principle of Individual Participation:</u> The mechanism by which an individual is able to prevent information about them obtained for one purpose from being used for other purposes without their 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 received by a Veteran.

<u>Mitigation:</u> the risk of incorrect information in an individual's records is mitigated by authenticating information, when possible, Additionally, staff verifies information in medical records and corrects information identified as incorrect during each patient's medical appointments.
The NOPP discusses the process for requesting an amendment to one's records.

The] Release of Information (ROI) office is available to assist Veterans with obtaining access to their health records and other records containing personal information.
The Veterans' Health Administration (VHA) established MyHealtheVet program to provide Veterans remote access to their medical records. The Veteran must enroll and have access to the premium account to obtain access to all the available features. In addition, VHA Directive 1605.01 Privacy and Release of Information 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. (Work with your ISSO to complete this section).

8.1 The procedures in place to determine which users may access the system, must be 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 CyberArk Accounts.

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 using multi-factor authentication.
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.

8.2a. Will VA contractors have access to the system and the PII?

Yes, ABOUT Staff are classified as contractors. ABOUT Is a subcontractor to covered business associates. Further, Ensocare is classified as an IaaS 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 and/or CyberArk Vault.

8.2b. What involvement will contractors have with the design and maintenance of the system?

Ensocare Assessing is a commercial off the shelf Vendor Managed IaaS solution – fully designed and managed by vendor contractor.

8.2c. Does the contractor have a signed confidentiality agreement? Yes, pass through from prime contractors

8.2d. Does the contractor have an implemented Business Associate Agreement for applicable PHI? Yes, pass through from prime contractor(s)

8.2e. Does the contractor have a signed non-Disclosure Agreement in place? Yes pass through from prime contractor. Contracts are reviewed and renewed annually by VA Contracting Officer(s) and their representative(s) and Prime Contractor(s).

Privacy Roles and Responsibilities are established defining privileged user account(s) (PAUs) and standard user account(s) (SUAs). PAUs require approved ePAS request(s) and SUAs role provisioning is managed at the facility level based on site standard operating procedures.

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.*

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 The Authorization and Accreditation (A&A) completed for the system.

8.4a If Yes, provide:

1. *The Security Plan Status:* Completed/Current

2. *The System Security Plan Status Date:* 06-Feb-2024
3. *The Authorization Status:* Authorized
4. *The Authorization Date:* 02-May-2024
5. *The Authorization Termination Date:* 02-May-2025
6. *The Risk Review Completion Date:* 29-March-2024
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.***

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. ***(Refer to question 1.8 of the PTA)***

As a VAEC/AWS vendor managed IaaS – the CSP is within the VA's network. The data is owned by the VA

9.2 Does the contract with the Hosting 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 3.3.1 of the PTA)* *This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

<<ADD ANSWER 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.

No ancillary data is collected.

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.

All contracts comply with eMASS/ATO SoP.

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).

RPA is not in use with this system.

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: 2025.01.13 13:33:52 -05'00'

Privacy Officer, Nancy Katz-Johnson

YOULANDA HOWARD

Digitally signed by YOULANDA HOWARD
Date: 2025.01.13 10:27:23 -06'00'

Information System Security Officer, Youlanda Howard

ANGELA GANT-CURTIS

Digitally signed by ANGELA GANT-CURTIS
Date: 2025.01.13 13:24:56 -06'00'

Information System Owner, Angela Gant-Curtis

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).

HELPFUL LINKS:

Records Control Schedule 10-1 (va.gov)

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 Directive 1605.04
IB 10-163p (va.gov)