Privacy Impact Assessment for the VA IT System called:

Emergency Department Integration System (EDIS)

Veterans Health Administration (VHA)

Clinical Services (VHA-11)

eMASS #1248

Date PIA submitted for review:

July 22, 2024

System Contacts:

System Contacts

Title	Name	E-mail	Phone Number
Privacy Officer	Phillip Cauthers	Phillip.Cauthers@va.gov	503-721-1037
Information System Security Officer (ISSO)	Eric Bailey	Eric.Bailey3@va.gov	732-639-3959
Information System Owner	Tony Sines	Tony.Sines@va.gov	316-249-8510

Abstract

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

The Emergency Department Integration System (EDIS) is a VHA-wide application used to track and manage the delivery of care to patients in the Emergency Care System (ECS). This critical IT solution directly supports the major initiative of Enhance the Veteran Experience and Access to Healthcare (EVEAH). The application improves emergency department care by introducing the systematic collection, display and reporting on patient status information. It is able to integrate with Appointment Management and Patient Care Encounter within Veterans Health Information Systems and Technology Architecture/Computerized Patient Record System (VistA/CPRS).

Overview

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

1. *General Description*

   A. *What is the IT system name and the name of the program office that owns the IT system?*
   Emergency Department Integration System (EDIS) is sponsored by VHA Front Office - Clinical Services (VAH-11).

   B. *What is the business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?*
   EDIS is part of VHA's Major Initiative (MI) #7, New Models of Healthcare, which is designed to improve access to primary and specialty care, enhance the efficiency of the healthcare team, and boost patient satisfaction. The mission/business process of EDIS is to provide Health Care to Veterans by:

   - Provide Emergency Health Care Treatment
   - Perform Track Patient Bed and Room Assignment
   - Capacity Management
   - Monitor Clinical Tasks
   - Develop Patient Summary Record of Care
   - Capture Patient Care Encounter Information
   - Manage Clinician Communications

   C. *Who is the owner or control of the IT system or project?*
   Veterans Health Administration (VHA) – VA Owned and Operated

2. *Information Collection and Sharing*

   A. *What is the expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual?*
   EDIS does not store any information and only processes information from the source systems VistA.

   The expected number of individuals that will have their information processed through EDIS is over 250,000. The affected individuals are Veterans and/or their dependents requiring care from the VA.

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

The Emergency Department Integration System (EDIS) is an extension to the Veterans Health Information System and Technology Architecture (VistA) for tracking and managing the delivery of care to patients in an Emergency Department (ED); it is a class III to class I software conversion. The system tracks ED patients during incidents of care, displays the current state of care delivery, and reports data extracts on the delivery of care. EDIS displays all information for active patients assigned to the ED, on the "white board" on any computer which has access to the EDIS server using a web browser or on a "large screen" display within the ED. This replaces the traditional manual white board found in most Emergency Departments. EDIS system provides a multi-provider, multi-patient, workflow-driven tool for tracking patients while they're assigned to the ED.

The system can be configured to specifics of different Veterans Health Administration (VHA) Emergency Departments. The following are some of the features of EDIS:

- Captures, monitors, and provides reports on the flow of patients through the ED.
- Requires standardized role-based workflow.
- Supplies PC-based and optional big screen displays configured specifically to each individual ED.
- Provides bi-directional information flow with some VistA applications.
- Creates Patient Care Encounter (PCE) visits and passes diagnosis information.
- Communicates with Scheduling package.
- Displays associated lab and Imaging order status.
- Patient registration in VistA appears in EDIS.

EDIS is a web-based application that connects to the VistA systems deployed on the each of the Veterans Integrated Services Networks (VISNs). The system uses VistALink to access the VistA Patient file, against which it will perform patient lookup. Selecting a patient from the lookup list will add the patient to the ED Log file, which will serve as the key source of information for EDIS tracking and reporting. Users also have the ability to add patients who are not in their facilities' local VistA systems. Users launch EDIS on their workstations by pointing a standard web browser to the EDIS main web server Uniform Resource Locator (URL). Facilities run the EDIS display board (usually a large plasma or liquid crystal display) by pointing the display machine's browser to a display-board URL. EDIS display boards run in kiosk mode, a method of operation designed for Internet kiosks and other settings where limiting end-user interactions with applications is advisable. Kiosk mode locks down the user interface to protect applications from accidental or deliberate misuse.

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

Emergency Department Integration System has interconnections with the following applications and information systems that are listed below:

System Name	Data Direction & Data Type	Type of Connection
Veterans Health Administration (VHA-10) Veterans Health Information System and Technology Architecture (VistA)	Bidirectional VistA serves as the main source of the information for EDIS to provide actual data for emergency department. The following data elements are shared: Name, Social Security Number, Date of Birth, Personal Mailing Address, Personal Phone Number, Emergency Contact Information, Medications, Unique Identifying Number – Data File Number (DFN) and Patient Health Information (includes patient status, diagnosis, complaint, vitals, active mediations/issues, and associated labs and imaging order status).	Internal

EDIS is a web-based application that connects to the VistA systems deployed on the each of the Veterans Integrated Services Networks (VISNs). The system uses VistALink to access the VistA Patient file, against which it will perform patient lookup. Selecting a patient from the lookup list will add the patient to the ED Log file, which will serve as the key source of information for EDIS tracking and reporting. Users also have the ability to add patients who are not in their facilities' local VistA systems. Users launch EDIS on their workstations by pointing a standard web browser to the EDIS main web server Uniform Resource Locator (URL). Facilities run the EDIS display board (usually a large plasma or liquid crystal display) by pointing the display machine's browser to a display-board URL. EDIS display boards run in kiosk mode, a method of operation designed for Internet kiosks and other settings where limiting end-user interactions with applications is advisable. Kiosk mode locks down the user interface to protect applications from accidental or deliberate misuse.

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

EDIS is hosted at VA Enterprise Cloud (VAEC) Microsoft Azure Government (MAG) US East and South regions as Infrastructure as a Service (IaaS) and leverages VAEC General Support Services (GSS). This boundary incorporates all utilized resources, services, and security measures consistent throughout the regions.

3. Legal Authority and SORN

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

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

B. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?

The system uses cloud technology and the SORN covers cloud usage/storage. The SORN will not require any amendments.

4. *System Changes*

A. *Will the completion of this PIA will result in circumstances that require changes to business processes?*
No, the completion of this PIA will not result in any circumstances that would require changes to business processes.

B. *Will the completion of this PIA could potentially result in technology changes?*
No, the completion of this PIA will not result in technology changes.

Section 1. Characterization of the Information

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

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

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

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

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

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

- ☒ Name
- ☒ Social Security Number
- ☒ Date of Birth
- ☐ Mother's Maiden Name
- ☒ Personal Mailing Address
- ☒ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☐ Personal Email Address
- ☒ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☐ Financial Information
- ☐ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers[1]
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers

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

☒ Medications
☐ Medical Records
☐ Race/Ethnicity
☐ Tax Identification Number
☐ Medical Record Number
☐ Gender
☐ Integrated Control Number (ICN)
☐ Military History/Service Connection
☐ Next of Kin
☒ Other Data Elements (list below)

Other PII/PHI data elements: Unique Identifying Number (includes Data File Number (DFN), Patient health Information: Patient Status, Diagnosis, Complaint, Vitals, Active Medications/Issues, and Associated Lab and Imaging Order Status).

PII Mapping of Components (Servers/Database)

Emergency Department Integration System (EDIS) consists of **three (3)** 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 **EDIS** 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.

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
EDIS Java Application	Yes	No	Name, Date of Birth, Social security, Phone Number, Emergency contact information, Personal Contact Information, Medications,	Track care of patients	Role-based Permissions in Vista, IAM
EDIS Kiosk	Yes	No	Last Name	Track care of patients	Physical secured room
EDIS VistA	Yes	Yes	Patient Name, Phone Number and Unique Identifying Number	Link EDIS file entries to the Patient file entries, Unknown why phone number is collected	Access and verify codes required to connect to Vista, Role based permissions within Vista.

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 data is collected by EDIS is received electronically from VistA/CPRS and/or Patient Care Encounter (PCE), manually by healthcare personnel and lastly some information created during the ED visit to provide care for the Veteran.

As a clinical application for VHA Emergency Departments (ED), EDIS provides critical information about patients' physical whereabouts, the status of their laboratory and imaging tests, their acuities, their staffing assignments, their time in the emergency department, and more. This information is input manually by healthcare personnel. Some information is obtained from the Patients' VistA Medical record and some information is created during the ED visit and are posted back to the Patient's VistA record.

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.
Veterans receive health care services from multiple VA locations during the course of their lifetime. In order to provide optimal health care, VA healthcare personnel need to be able to access relevant information pertaining to the individual. The Sensitive Personal Information (SPI) processed by EDIS is a collection of data organized in a format that supports the delivery of care, regardless of the patient's location. EDIS provides common access to consistent, comprehensive, and reliable patient information across continuity of care and across the VA.

EDIS uses the data it collects to identify and track ED patients during incidents of care. EDIS system provides a multi-provider, multi-patient, workflow-driven tool for tracking patients while they're assigned to the ED.

1.2c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?
There are reports created within the application that are used for Emergency room metrics.

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?

The data is collected by EDIS is received electronically from VistA/CPRS and/or Patient Care Encounter (PCE), manually by healthcare personnel and lastly some information created during the ED visit.

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?
Not Applicable.

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

These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.
All information is checked for accuracy and verified by the original source (VistA/CPRS, PCE, or healthcare personnel). EDIS does not verify as it only transmits PII/PHI and does not store or collect.

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?
EDIS does not verify as it only transmits PII/PHI and does not store or collect.

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

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

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk:
EDIS collects Personally Identifiable Information (PII)/Personal Health Information (PHI) in VHA Emergency Departments when assessing the individual's care. The information collected is used to identify the individual for treatment for access to health care and track and manage the delivery of care, improving clinical outcomes. The information is collected from the source system VistA and is needed to identify the parties involved in an incident, identify potential issues and concerns, and offer any assistance to the affected individuals so that they may find the help they need to get through their crisis. If this information were breached or accidentally released to inappropriate parties or the public, it could result in personal and/or emotional harm to the individuals whose information is contained in the system.

Mitigation:
VA is careful to only collect the information necessary to identify the parties involved and assist in the care of patients. By only collecting the minimum necessary information, VA is able to better protect the Veterans information. EDIS receives the information via a secured internal VA Intranet and no external exposure results from this connection. Once collected, information is transmitted using Federal Information Protection Standard (FIPS) compliant encryption and stored in secure servers behind VA firewalls.

Section 2. Uses of the Information

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

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

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

PII/PHI Data Element	Internal Use	External Use

Name	Used to identify the Veteran and/or Dependent (patient).	Not used
Social Security Number (SSN)	Used to verify the Veteran and/or Dependent (patient) and as a file number for Veteran	Not used
Date of Birth	Used to verify the Veteran and/or Dependent (patient).	Not used
Personnel Mailing Address	Used to correspond with the Veteran	Not used
Personnel Phone Number	Used to correspond with the Veteran	Not used
Emergency Contract Information	Used to notify contract in an emergency situation	Not used
Current Medications	Used for records and reporting	Not used
Unique Identifying Number (includes Data File Number (DFN), Patient health Information: Patient Status, Diagnosis, Complaint, Vitals, Active Medications/Issues, and Associated Lab and Imaging Order Status)	Used to identify the Veteran and/or Dependent (patient) and for records and reporting	Not used

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?
EDIS is a web-based application that connects to VistA systems deployed on each of the Veterans Integrated Services Networks (VISNs). The system uses VistALink to access the VistA Patient file, against which it will perform patient lookup. Selecting a patient from the lookup list will add the patient to the ED Log file, which will serve as the key source of information for EDIS tracking and reporting.

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.
Any information created in EDIS stays in File 230 in VistA and most of that information only relates to the emergency room.

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?

EDIS uses Transport Layer Security (TLS) for data in transit. EDIS uses Secure Socket Layer (SSL) certificates to maintain confidentiality /integrity of data during preparation and reception of transmission.

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

Strict Role-based Access Control (RBAC) controls are in place only allowing special permission levels to access any PII/PHI retained. Access is granted on a need-to-know basis and the system maintains rigorous logging and auditing.

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

The EDIS application team has implemented the required security controls based on the tailoring guidance of NIST Special Publication 800-53 Rev 4 and VA directives or handbooks. VA Records Management Policy VA 6300.1, VA 6500 HB, National Rules of Behavior (ROB), and VA 6502.1, VA6502.3, VA 6502.4 Privacy Policies govern how Veterans information is used, stored, and protected.

Following the NIST and VA policy guidance listed above, the Separation of Duties policy applied, allows EDIS personnel to receive focused and recorded training that provides access only to the areas of the application that applies to their job task and responsibilities. EDIS utilizes Role-based Access Control (RBAC) making PII/PHI controlled based predefined roles, ensuing only authorized individuals are able to access the information and does not share information externally.

EDIS utilizes a thorough, multi-tiered strategy to safeguard highly sensitive data, ensuring compliance with relevant regulations and significantly reducing the risk of data breaches or unauthorized access:

Encryption:

- Data-in-Transit: All data transmitted over the VA network is encrypted using strong encryption protocols such as FIPS approved TLS (Transport Layer Security).
- Data-at-Rest: All PII/PHI is stored within VistA, and are responsible for providing encryption and use FIPS compliant approved encryption algorithms.

Access Control:

- Role-based Access Control (RBAC): Access to PII/PHI is strictly controlled based on predefined roles, ensuring only authorized individuals can access this information.
- Multi-Factor Authentication (MFA): Users are required to go through MFA procedures to access EDIS
- Least Privilege Principle: Access rights are assigned based on the least amount of data privileges needed for users to perform their tasks on a need-to-know basis.

Audit and Accountability:

- Audit Logs: All access to and actions performed are logged and regularly reviewed.
- Incident Response Plan: A comprehensive plan is in place to address any unauthorized access or disclosure of PII/PHI.

Data Minimization:

- Need-to-Know Basis: Data is only collected if it's strictly necessary for the purpose of the information system.

Training:

- User Training: All personnel must complete mandatory training on data protection policies and procedures.
- Regular Updates: Training is regularly updated to include new policies or regulation changes and taken on an annual basis.

Network Security:

- Network firewalls and intrusion detection systems are used to monitor and control traffic flow, thereby preventing unauthorized access or data breaches.
- EDIS can only be accessed on the VA Network and user access is granted upon successful authentication against the VA Multifactor Authentication using Single Sign On (SSOi).
- Virtual Private Network (VPN): In order to gain access to the VA Network, uses must first log onto the VPN for an added layer of security.

By rigorously adhering to these principles, EDIS aims to fully comply with the guidelines set forth in OMB Memorandum M-06-15, thereby ensuring the highest level of security and privacy for PII/PHI.

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?

Following the NIST Special Publication 800-53 and VA policy guidance listed in section 2.3b, the separation of duties policy applied, allows HTR staff members to receive focused and recorded training that provides access only to the areas of the application that applies to their job task and responsibilities. Elevated privilege access is requested through the Electronic Permission Access System (ePAS) and is approved by their Contracting Officer's Representative (COR) and the HTR manager.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented?
All access is documented via the Electronic Permission Access System (ePAS) and training records are documented via VA Talent Management System (TMS 2.0). All VA personnel must sign the Rule of Behavior (ROB) which outlines what behaviors are allowed and not allowed on US Government computer systems.

Following the NIST 800-53 security controls, the EDIS application cover security areas with regard to protecting the Confidentiality, Integrity, and Availability (CIA) of VA information systems and the information processed, stored, and transmitted by those systems. These security controls are documented in Enterprise Mission Assurance Support Services (eMASS) the GRC tool.

2.4c Does access require manager approval?
Yes, all requested access is approved by their Contracting Officer's Representative (COR) and the EDIS manager via the Electronic Permission Access System (ePAS).

2.4d Is access to the PII being monitored, tracked, or recorded?
Yes, all EDIS personnel must receive annual security and privacy training which is monitored, tracked and recorded via VA Talent Management System (TMS 2.0), Rules of Behavior (ROB) are signed and recorded in the VA Human Resources system, and all user accounts are reviewed on a quarterly basis by the System Owner.

The information system records access using audit trails, real-time alerts, and regular audits to monitor access to any sensitive information.

2.4e Who is responsible for assuring safeguards for the PII?
Safeguarding PII is a shared responsibility across different roles within the organization. There are specific roles primarily responsible for ensuring that safeguards are effectively implemented and maintained. The following provides for these specific roles:

- Chief Information Officer (CIO): The CIO holds overall responsibility for the information technology strategy, including the safeguarding of PII. They ensure that adequate resources and technologies are in place for data protection.
- Information System Security Officer (ISO): The ISSO directly oversees the technical implementation of security controls and safeguards for PII. They regularly audit and monitor access and usage to ensure compliance with security policies.

Section 3. Retention of Information

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

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

None of the information in section 1.1 is retained by EDIS. EDIS does not store any information and only processes information from the source VistA.

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.*

Data retention is handled by VistA. Data is transmitted to the EDIS application as a function of addressing patient encounters within the Emergency Department and as soon as the patient Emergency Department visit is complete, the data is then saved and stored on the VistA system. EDIS does not retain PII data.

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?

EDIS does not store any information and only processes information from the source system VistA via XML configuration file.

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

Retention is handled by the source system, VistA which retains information in accordance with Record Control Schedule (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).

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.

Elimination or transfer of SPI is handled by the source system, VistA.

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.

EDIS data is used for training purposes via a local site's support account. All patient data used is scrambled, therefore, eliminating the risk of PII data being shared or accessed by unauthorized individuals. All environments use dummy data except for pre-production contains PII for testing the system. The individuals testing are the same individuals that have access to the same data in production. Obtaining an account in pre-prod is just as stringent as production.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

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

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

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

Follow the format below:

Privacy Risk:

The risk of maintaining data within the source system, VistA, could be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally compromised or breached.

Mitigation:

To mitigate this risk, the system employs multiple layers of security controls, including advanced encryption, Multi-factor Authentication (MFA), and robust access management policies. Regular security audits and vulnerability assessments are conducted to ensure the data remains secure during the entire retention period. VistA strictly adheres to the Records Management Schedule, in

order to ensure that no records are maintained longer than permitted by the records control schedule.

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?

Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system within VA with which information is shared.

State the purpose for the internal sharing. If you have specific authority to share the information, provide a citation to the authority.

For each interface with a system outside your program office, state what specific data elements (PII/PHI) are shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?
This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Veterans Health Administration (VHA) Veterans Health Information System and Technology Architecture (VistA)	VistA serves as the main source of the information for EDIS to provide actual data for EDs.	• Name • Social Security Number (SSN) • Date of Birth (DOB) • Personal Mailing Address • Personal Phone Number • Personal Email Address • Emergency Contact Information	Hyper Text Transfer Protocol with Secure Sockets Layer (HTTPS) carrying Extensible Markup

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*
		• Current Medications • Unique Identifying Number	Language (XML)
Veterans Health Administration (VHA) Computerized Patient Record System (CPRS)	EDIS uses CPRS GUI interface to track and manage the delivery of care to patients in the ED. CPRS is module within VistA.	• Name • Social Security Number (SSN) • Date of Birth (DOB) • Current Medications • Unique Identifying Number	Remote procedure and broker calls.

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk:
The privacy risk associated with sharing data within the Department of Veterans Affairs (VA) is that data may be disclosed to individuals who do not require access and heightens the threat of the information being misused.

Mitigation:
The principle of need-to-know is strictly adhered to by EDIS personnel. Only personnel with a clear business purpose are allowed access to the system and the information contained within the system.

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.

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***
N/A	N/A	N/A	N/A	N/A

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

If no External Sharing listed on the table above, ***(State there is no external sharing in both the risk and mitigation fields).***

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

Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.
This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

Privacy Risk:
The risk that EDIS data may be shared with unauthorized users or authorized users may share it with other unauthorized individuals.

Mitigation:
Although EDIS does not share information externally. The principle of need-to-know is strictly adhered to by EDIS personnel. Only personnel with a clear business purpose are allowed access to the system and the information contained within the system. All personnel with access to EDIS information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually.

Section 6. Notice

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

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

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

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

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

Notice is also provided in the Federal Register with the publication of the SORN: 79VA10 "Veterans Health Information Systems and Technology Architecture (VistA)Records-VA": 79VA10 / 85 FR 84114, https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf.

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."

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

Notice was provided as described in question 6.1a above.

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

The VHA 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.

Notice is also provided in the Federal Register with the publication of the SORN: 79VA10 "Veterans Health Information Systems and Technology Architecture (VistA)Records-VA": 79VA10 / 85 FR 84114, https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf.

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."

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.

While EDIS does not collect information directly from the Veteran but instead from the source application of VistA, information is requested when it is necessary to administer benefits to veterans and other potential beneficiaries. While an individual may choose not to provide information, this may prevent them from obtaining the benefits necessary to them. The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VHA an SSN (see 38 CFR 1.575(a)).

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. Individuals may also request to Opt-Out of the facility directory during an inpatient admission. If the individual chooses to opt-out, information is not disclosed from the facility directory unless otherwise required by law.

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 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 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 https://department.va.gov/foia/ to obtain information about FOIA points of contact and information about agency FOIA processes.***

Individuals wishing to gain access to their information should contact the VA facility location at which they made contact to provide them their information.

There are several ways a veteran or other beneficiary may access information about them. The Department of Veterans' Affairs has created the My HealtheVet 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 Release of Information (ROI) office at the VA medical facility where they are treated.

VHA Directive 1605.01, Privacy and Release of Information, Paragraph 7 outlines policy and procedures for VHA and its staff to provide individuals with access to and copies of their PII in compliance with the Privacy Act and HIPAA Privacy Rule requirements. VHA also created VA form 10-5345a for use by individuals in requesting copies of their health information under right of access.VA Form 10-5345a is voluntary but does provide an easy way for individual to request their records.

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 EDIS system is not exempt from the Privacy Act.

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

Inaccurate information can be corrected by contacting the VA facility location at which they made contact.

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. Further information regarding access and correction procedures can be found in the notices listed in Appendix A. 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 VHA 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

Individuals seeking information regarding access to and contesting of VA benefits records may write, call or visit the nearest VA regional office.

Additional notice is provided through the SORS listed in 6.1 of this PIA and through the Release of Information Office where care is received.

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***

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

Formal redress via the amendment process is available to all individuals, as stated in questions 7.1-7.3.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

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

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

Follow the format below:

Privacy Risk:

There is a risk that members of the public will not know the relevant procedures for gaining access to, correcting, or contesting their information.

Mitigation:

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.

Section 8. Technical Access and Security

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

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

These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.

8.1a Describe the process by which an individual receives access to the system?
The Agency establishes privacy procedures, responsibilities, and departmental framework for incorporating privacy in the System Development Life Cycle (SDLC) of Information Technology (IT) assets that store, process, or transmit VA information.

Administrative procedures are in place for the two primary types of users that access the EDIS application, EDIS System Administrators, and VA clinical staff. All access to EDIS is handled through VistA keys.

EDIS System Administrator(s) access the information system in order to maintain the functionality of the system, which requires elevated privileges and is associated with their position. The access is granted through the VA onboarding process via the Electronic Permission Access System (ePAS) process. Only users with a need-to-know and a valid business need are granted access. Administrative access requires management approval, provided on a least privilege basis, and is reviewed quarterly.

VA clinical staff are granted access to the system in order to access the EDIS application regarding Veterans receiving care. This provides the ability for VA clinical staff to provide quality care to the Veterans. Access is granted by going to the EDIS application Uniform Resource Locator (URL) accessible on the VA network only where they are presented with a registration screen (after passing SSOi) which allows them to request access upon authorized approval. Only users with a need-to-know and a valid business need are granted access.

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?
The EDIS application is only accessible on the VA network.

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.
The roles in EDIS are views that users choose when requesting access to the application and are as follows:

View Name	Description	Create (C) Read (R) Write (W) Delete (D)
EDPF TRACKING VIEW BOARD	View the display board	Read
EDPF TRACKING VIEW CONFIGURE	Configure the tracking board	Create Write Read Delete
EDPF TRACKING VIEW DISPOSITION	Disposition the patient(s)	Create Write Read
EDPF TRACKING VIEW EDIT CLOSED	Edit closed patient(s)	Create Write Read
EDPF TRACKING VIEW REPORTS	Tracking reports	Read
EDPF TRACKING VIEW SIGNIN	Sign-In patient(s)	Create Write Read
EDPF TRACKING VIEW STAFF	Assign staff	Create Write Read Delete
EDPF TRACKING VIEW TRIAGE	Triage patient(s)	Create Write Read
EDPF TRACKING VIEW UPDATE	Update tracking board	Create Write Read
EDIS System Administrators	Maintains the information system	Create, Read, Update, and Delete

Table 1: EDIS Views

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

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII. This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.

Yes, VA Contractors maintain the EDIS system and those with Administrative level privileges have full access to the system. All contactors involved in the operations of EDIS have completed the initial and Annual Security and Privacy training. Users with elevated privileges have undergone training unique to their specific role, and refresher training is mandatory and tracked in the Training Management System (TMS).

All VA contractors go through the VA onboarding process which includes an executed Information Protection and Risk Management Non-Disclosure Agreement (NDA).

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.

Part of the VA onboarding process is all personnel are required to take the following training courses in TMS prior to accessing the VA network:

- Course #VA 10176 - VA Privacy and Information Security Awareness and Rules of Behavior (ROB).
- Course #VA 10203 - Privacy and HIPPA Training

Users with elevated privileges are required to take additional training unique to their specific role. All training is maintained by taking refresher courses on an annual basis and tracked in TMS.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* July 1, 2024
3. *The Authorization Status:* Authorization to Operate (ATO)
4. *The Authorization Date:* September 23, 2021
5. *The Authorization Termination Date:* September 21, 2024
6. *The Risk Review Completion Date:* September 2, 2021
7. *The FIPS 199 classification of the system:* 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.***
N/A

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)*

VA Enterprise Cloud (VAEC) Microsoft Azure Government (MAG) Infrastructure as a Service (IaaS).

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

Not Applicable

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

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

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

Not Applicable

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, 4particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

Not Applicable

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).

Not Applicable

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.

PHILLIP CAUTHERS

Digitally signed by PHILLIP CAUTHERS
Date: 2024.08.08 07:43:55 -07'00'

Privacy Officer, Phillip Cauthers

ERIC BAILEY

Digitally signed by ERIC BAILEY
Date: 2024.08.08 11:53:52 -04'00'

Information System Security Officer, Eric Bailey

TONY SINES

Digitally signed by TONY SINES
Date: 2024.08.08 09:07:56 -05'00'

Information System Owner, Tony Sines

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).

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

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

HELPFUL LINKS:

General Records Schedule
https://www.archives.gov/records-mgmt/grs.html

National Archives (Federal Records Management):
https://www.archives.gov/records-mgmt/grs

VA Publications:
https://www.va.gov/vapubs/

VA Privacy Service Privacy Hub:
https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):
VHA Notice of Privacy Practices
VHA Directive 1605.04: Notice of Privacy Practices