Privacy Impact Assessment for the VA IT System called:

Emergency Department Integration System (EDIS)

Office of the Assistant Deputy Under Secretary for Health for Quality, Safety and Value

Date PIA submitted for review:

April 15, 2021

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Christian Loftus	christian.loftus@va.gov	859-281-2470
Information System Security Officer (ISSO)	Joseph Messina	joseph.messina@va.gov	732-440-9668
Information System Owner	Christopher Brown	christopher.brown@va.gov	202-270-1432

Abstract

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

The Emergency Department Integration System (EDIS/EDIS) is an extension to the Veterans Health Information System and Technology Architecture/Computerized Patient Record System (VistA/CPRS) for tracking and managing the delivery of care to patients in an Emergency Department (ED).

Overview

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

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *If your system is a regional GSS, VistA, or LAN, include a list of the hospitals/medical centers, or other regional offices that fall under your system. Additionally, what region is the system under?*
- *A general description of the information in the IT system.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.*
- *A citation of the legal authority to operate the IT system.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*
- *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval?*
- *Does the system use cloud technology? 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.*
- *Does a contract with Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII?*
- *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 is the magnitude of harm if privacy related data is disclosed, intentionally or unintentionally? Would the reputation of the CSP or its customers (VA) be affected?*

The Emergency Department Integration System (EDIS) is an extension to the Veterans Health Information System and Technology Architecture/Computerized Patient Record System (VistA/CPRS) 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. 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. 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.

The expected number of individuals that will have their PII stored in the system is 250,000. EDIS is hosted at VAEC Microsoft Azure Government (MAG) East and South regions. EDIS does not store patient data in these tables. The application uses remote procedure calls (RPCs) against local VistA implementations to populate patient and provider selection lists, provide limited data synchronization between EDIS and Computerized Patient Record System (CPRS), and determine users access levels. If any privacy related data would be exposed, the magnitude of harm could be significant and affect the reputation of CSP and VA. The Legal Authority for Operating this system is: Title 38, United States Code (U.S.C.), Sections 7301.

EDIS will not require any changes to the business processes and all technology is currently in place. There is a contract in place with VAEC Azure, Liberty IT Solutions, and VA Customers to establish who has ownership rights over the data.

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.

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 Account Information
- ☐ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☒ Current Medications
- ☐ Previous Medical Records
- ☐ Race/Ethnicity
- ☐ Tax Identification Number
- ☐ Medical Record Number
- ☒ Other Unique Identifying Number (list below)

Medical information such as: Patient Status, Diagnosis, and Associated Lab and Imaging Order Status.

PII Mapping of Components

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

PII Mapped to Components

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 ED, and more. This information is input manually by healthcare personnel. Some information is obtained from the patient's VistA record.

PII Mapped to Components

Components of the information system (servers) collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
EDIS Java Application	Yes	No	Phone Number	Unknown	n/a
EDIS Kiosk	No	No	n/a	n/a	n/a
EDIS VistA	No	Yes	Data File Number (DFN), Phone 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

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

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

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

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

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

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.

1.3 How is the information collected?

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

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

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

The data is collected either manually by healthcare personnel and/or received electronically from Veterans Health Information System and Technology Architecture/Computerized Patient Record System (VistA/CPRS), Patient Care Encounter (PCE) and lastly some information created during the ED visit.

1.4 What is the purpose of the information being collected, used, disseminated, created, or maintained?

Include a statement of why the particular SPI is collected, maintained, used, or disseminated in the system is necessary to the program's or agency's mission. Merely stating the general purpose of the system without explaining why this particular type of information should be collected and stored is not an adequate response to this question.

If the system collects, uses, disseminates, or maintains publicly available or commercial data, include a discussion of why commercial data is relevant and necessary to the system's purpose.

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

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 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.

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

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

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

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

Data is collected directly from the Veteran during the emergency visit at the hospitals. As the information is collected straight from the individual, the accuracy of the information is confirmed during the emergency visit by ED personnel. Some of the data that is collected from the VistA program, as information is imported from existing VA systems, the accuracy is verified by the original source. EDIS does not verify as it only transmits PII/PHI and does not store or collect.

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

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

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

The Legal Authority for Operating this system is: Title 38, United States Code (U.S.C.), Sections 7301. 79VA10 / 85 FR 84114 Veterans Health Information Systems and Technology Architecture (VistA) Records - https://www.oprm.va.gov/docs/Current_SORN_List_04_09_21.pdf

1.7 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks.

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

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

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

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

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

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

Privacy Risk:
EDIS collects Personally Identifiable Information (PII) in VHA Emergency Departments when assessing the patient's care. The information is collected directly from the individual and is needed to identify the parties involved in an incident, identify potential issues and concerns, and offer any assistance to the affected parties so that they may find the help they need to get through their crisis. If this information was breached or accidentally released to inappropriate parties or the public, it could result in financial, personal, and/or emotional harm to the individuals whose information is contained in the system.

Mitigation:
EDIS is careful to only collect the information necessary to identify the parties involved. By only collecting the minimum necessary information, VA is able to better protect the individual's information. EDIS receives the information via a secured internal Intranet and no external exposure results from this connection.

Section 2. Uses of the Information

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

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

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

Name: Veteran's Identification - Internal
Social Security Number: Used to verify Veteran identity and as a file number for Veteran – Internal
Mailing Address: Used to correspond with the Veteran
Patient Status: Used for records and reporting
Diagnosis: Used for records and reporting
Associated Lab and Imaging Order Status: Used for records and reporting

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

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

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

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

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. 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.

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

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. Example: Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.

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

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

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?

This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

The security controls for the EDIS application cover 17 security areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. 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 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. EDIS access is controlled through menu options, and security keys that is approved by the EDIS manager.

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 have a storage system.

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.

This question is related to privacy control DM-2, Data Retention and Disposal.

Data retention is handled by VistA; however, data is transmitted to the EDIS application as a function of addressing patient encounters within the Emergency Department. 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, whereby the VistA retention period is indefinite.

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

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner.

This question is related to privacy control DM-2, Data Retention and Disposal.

EDIS does not store data collected and does not have a storage system. Data retention is handled by VistA; however, data is transmitted to the EDIS application as a function of addressing patient encounters within the Emergency Department (ED). As soon as the patient ED is completed, the data is then saved and stored on the VistA system. EDIS does not retain PII data, whereby the VistA retention period is indefinite. These records are retained and stored indefinitely in accordance with the General Records Schedule 31, approved by National Archives and Records Administration (NARA) Transmittal 31 (archives.gov); 79VA10 / 85 FR 84114 Veterans Health Information Systems and Technology Architecture (VistA) Records-VA Current SORN List (va.gov); and VA Handbook 6300.1 Records of Management Procedures explains the Records Control Schedule procedures. Shredding or burning of Hard Copies.

3.4 What are the procedures for the elimination of SPI?

Explain how records are destroyed or eliminated at the end of the retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc.?

This question is related to privacy control DM-2, Data Retention and Disposal.

EDIS does not eliminate SPI, the data is kept indefinitely in the VistA system in accordance with the General Records Schedule 31 approved by National Archives and Records Administration (NARA). Transmittal 31 (archives.gov); VA Handbook 6300.1 Records Management Procedures explains the Records Control Schedule procedures. Shredding or burning of hard copies.

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

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?

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

Users are required to complete VA Privacy and Information Security Rules of Behavior Training on an annual basis. The training records are retained for 7 years. This documentation and monitoring are performed through the use of the Talent Management System (TMS). Privacy training is used as an indicator to verify users of EDIS are managing PII correctly. 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.

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.

Privacy Risk:

There is a risk that the information maintained by EDIS/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 released or breached.

Mitigation:

To mitigate the risk posed by information retention, EDIS/VistA adheres to the NARA General Records Schedule. When the retention date is reached for a record, the individuals' information is carefully disposed of by the determined method as described in General Records Schedule 20.

EDIS does not collect or store PII as its collected and stored by other applications. Therefore, the only PII that EDIS has is the patients DFN which is the internal VistA identifier that links EDIS data to the patient in the patient file.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing / receiving / transmitting within VA. NOTE: Question 5 on Privacy Threshold Analysis should be used to answer this question.

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 data element types such as PII/PHI that are shared/received with the Program Office or IT system***	***Describe the method of transmittal***
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 Date of Birth Phone Number, Address, Email Emergency Contact Medications Patient Status Diagnosis Associated Lab and Imaging Order Status	Hyper Text Transfer Protocol with Secure Sockets Layer (HTTPS) carrying Extensible Markup Language (XML)

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 data element types such as PII/PHI that are shared/received with the Program Office or IT system*	*Describe the method of transmittal*
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 Date of Birth Medications Associated Lab and Imaging Order Status	Remote procedure and broker calls. Patient name, social security number and visit information related.

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Privacy Risk:

The privacy risk associated with maintaining PII is that sharing data within the Department of Veterans' Affairs could happen and the 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 the EDIS personnel. Only personnel with a clear business purpose are allowed access to the system and the information contained within.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

Note: This question is #7 in the Privacy Threshold Analysis.

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 data element types such as PII/PHI that are shared/received 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

If specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16, note them here.

EDIS does not share information externally.

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

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

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

Privacy Risk:

The privacy risk associated with maintaining PII is that sharing data outside of the Department of Veteran's Affairs could increase the risk that data may be disclosed to individuals who do not require access and heightens the threat of the information being misused.

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.

Section 6. Notice

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

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

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

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

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

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

The Notice of Privacy Practice (NOPP) is a document which explains the collection and use of protected information to individuals applying for VHA benefits. A signed statement acknowledging that they individual read and understood the NOPP is scanned into each applicant's electronic file. When updates are made to the NOPP copies are mailed to all VHA beneficiaries. Employees and contractors are required to review, sign and abide by the National Rules of Behavior on an annual basis.

1) The SORN defines the information collected from Veterans, use of the information, and how the information is accessed and stored. 79VA10 / 85 FR 84114 Veterans Health Information Systems and Technology Architecture (VistA) Records-VA Current SORN List (va.gov)
2) This Privacy Impact Assessment (PIA) also serves as notice of the EDIS System. As required by the Government 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, depending on the information required, some data collection is mandatory while others are voluntary. Failure to provide information may result in denial of access to the health care system.

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.

Any right to consent to particular uses of the information would be handled by the source systems that collect the information from the Veteran and feed EDIS with information. The source system is VistA.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks.

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

Principle of Transparency: Has sufficient notice been provided to the individual?

Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?

This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.

Privacy Risk:
There is a risk that members of the public may not know that the EDIS system exists within the Department of Veterans Affairs.

Mitigation:
The VA mitigates this risk by providing the public with two forms of notice that the system exists, as discussed in detail in question 6.1, including the Privacy Impact Assessment and the System of Record Notice.

Section 7. Access, Redress, and Correction

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

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

Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in

addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.

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

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

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

Individuals wishing to obtain more information about access, redress, and record correction of EDIS should contact the VA facility location at which they are or were employed or made contact. SORN 79VA10 / 85 FR 84114 Veterans Health Information Systems and Technology Architecture (VistA) Records-VA Current SORN List (va.gov)

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.

Under the jurisdiction of VHA, VHA Handbook 1605.1 Appendix D 'Privacy and Release Information', section 8 states the rights of the Veterans to amend to their records via submitting VA Form 10-5345a, Individual's Request for a Copy of Their Own Health Information, may be used as the written request requirement, which includes designated record sets, as provided in 38 CFR 1.579 and 45 CFR 164.526. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the facility Privacy Officer, or designee, to be date stamped; and be filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579.

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.

Individuals are not notified if there is missing or inaccurate information in their record. An individual who wishes to determine whether a record is being maintained under his or her name in the EDIS

system or wishes to determine the contents of such records should submit a written request or apply in person to the VA facility where the records are located. Per SORN 79VA10 / 85 FR 84114 Veterans Health Information Systems and Technology Architecture (VistA) Records-VA Current SORN List (va.gov).

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

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

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

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

Individuals are not notified if there is missing or inaccurate information in their record. An individual who wishes to determine whether a record is being maintained under his or her name in the EDIS system or wishes to determine the contents of such records should submit a written request or apply in person to the VA facility where the records are located. Per SORN 79VA10 / 85 FR 84114 Veterans Health Information Systems and Technology Architecture (VistA) Records-VA Current SORN List (va.gov).

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

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

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

Privacy Risk:
There is a risk that individuals may seek to access or redress records about them held by the VA Office and become frustrated with the results of their attempt.

Mitigation:
By publishing this PIA, and the applicable SORN, the VA makes the public aware of the unique status of applications and evidence files, such as those stored on the Virtual VA platform. Furthermore, this

document and the SORN provide the point of contact for members of the public who have questions or concerns about applications and evidence files.

Section 8. Technical Access and Security

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

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

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

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

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

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

1) Access to VA working and storage areas is restricted to VA employees on a ''need-to-know'' basis. Strict physical security control measures are enforced to ensure that disclosure to these individuals is also based on this same principle. Generally, VA file areas are locked after normal duty hours and the facilities are protected from outside access by the Federal Protective Service or other security personnel.

2) Access to computer rooms at health care facilities and regional data processing centers is generally limited by appropriate locking devices and restricted to authorized VA employees. Automated Data Processing (ADP) peripheral devices are placed in secure areas (areas that are locked or have limited access) or are otherwise protected. Information in VistA may be accessed by authorized VA employees. Access to file information is controlled at two levels. The systems recognize authorized employees by series of individually unique passwords/codes as a part of each data message, and the employees are limited to only that information in the file which is needed in the performance of their official duties.

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 or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

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

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

Yes, contractors will have access to the system. Contracts are reviewed annually at a minimum. The contractors who provide support to the system are required to complete annual VA Privacy and

Information Security and Rules of behavior training via the VA's TMS. All contractors are cleared using the VA background investigation process and must obtain a Moderate Background Investigation (MBI). This process is taken care of during the onboarding process of the EDIS project.

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.

Users are required to complete information system security training activities including annual security awareness training and specific information system security training. The training records are retained for 7 years. The documentation and monitoring are performed through the use of the Talent Management System (TMS).

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

If Yes, provide:

1. *The date the Authority to Operate (ATO) was granted,*
    a. ***10/01/20***
2. *Whether it was a full ATO or ATO with Conditions,*
    a. ***Full ATO***
3. *The amount of time the ATO was granted for, and*
    a. ***1 year***
4. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH).*
    a. ***MODERATE***

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

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

Section 9. 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

ID	Privacy Controls
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 provided in this Privacy Impact Assessment is true and accurate.

CHRISTIAN D LOFTUS 222466

Digitally signed by CHRISTIAN D LOFTUS 222466
Date: 2021.05.10 14:11:50 -04'00'

Privacy Officer, Christian Loftus

Joseph A. Messina 440499

Digitally signed by Joseph A. Messina 440499
Date: 2021.05.11 07:04:26 -04'00'

Information Systems Security Officer, Joseph Messina

Christopher Brown 101386

Digitally signed by Christopher Brown 101386
Date: 2021.05.10 14:39:46 -05'00'

System Owner, Christopher Brown

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).

79VA10 / 85 FR 84114 Veterans Health Information Systems and Technology Architecture (VistA) Records-VA Current SORN List (va.gov).