Privacy Impact Assessment for the VA IT System called:

Electronic Data Interchange – General – Application Code (EDI)

VA Central Office VACO

Financial Services Center (FSC)

Date PIA submitted for review:

05/24/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Deea Lacey	Deea.Lacey@va.gov	512-386-2246
Information System Security Officer (ISSO)	Ruben Rosales	Ruben.Rosales@va.gov	505-917-4906
Information System Owner	Jonathan Lindow	jonathan.lindow@va.gov	512-568-0626

Abstract

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

The Electronic Data Interchange - General (EDI) is a compilation of multiple processes which translate business data such as purchase orders, vendor invoices, vendor acknowledgements, and vendor registration into agreed upon formats for processing.

Overview

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

1 General Description

A. The IT system name and the name of the program office that owns the IT system.
Electronic Data Interchange – General – Application Code (EDI); Austin Information Technology Center (AITC)

B. The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.
The applications translate business data such as purchase orders, vendor invoices, vendor acknowledgements, and vendor registration into agreed upon formats for processing. Data formats include industry standards, such as X12 (an industry standard for EDI messaging syntax) and proprietary formats.

C. Indicate the ownership or control of the IT system or project.
VA Owned and VA Operated

2. Information Collection and Sharing

D. The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.
The approximate number of records containing PII on individuals is approximately 1000 per month.

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

The Electronic Data Interchange General (EDI) – General (EDI) owned by the Office of Finance is a compilation of **EDI jobs** (EDP, EDF, EDS, and EDD) that reside on the AITC z15 mainframe located at the Austin Information Technology Center (AITC).

General (EDI) includes the following processes:

- EDI Denver Distribution Center (EDD)

- EDI Financial (EDF)
- EDI Procurement (EDP)
- EDI Prime Vendor Subsistence (EDS)

These processes translate business data such as purchase orders, vendor invoices, vendor acknowledgments, and vendor registration into agreed upon formats for processing so the data can be read and processed by VA business partners. Data formats include industry standards, such as X12 and proprietary formats. The only component that uses and disseminates Sensitive Personal Information (SPI) is EDI Denver Distribution (EDD) Center using the partial Social Security Number (SSN) to identify the patient for the purpose of verifying eligibility and payment.

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

The data collected from the **EDI jobs** (EDP, EDF, EDS, and EDD) are shared internally with the FSC's Managed File Transfer system VL Trader which when in transit, is secured via sFTP with Transport Layer Security Data.

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

EDI General components share information internally with the Financial Service Center (FSC) servers, Data Management Interface (DMI), Veterans Health Information Systems and Technology Architecture (VISTA) sites (VA Hospitals and facilities), Subsistence Prime Vendor (SPV) and the Invoice Payment and Processing System (IPPS).

Authority for maintenance of the system is the Budget and Accounting Act of 1950 and General Accounting Office Title 8, Chapter 3 and 38 U.S.C. 501(a); 5 U.S.C. Part III, Subparts D and E.

3. Legal Authority and SORN

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

As stated in System of Records Notice (SORN) 13VA047 "Individuals Submitting Invoices/Vouchers For Payment-VA", authority for maintenance of the system is the Budget and Accounting Act of 1950 and General Accounting Office Title 8, Chapter 3.

- SORN 131VA047 "Purchase Credit Card Program-VA" states authority is Federal Acquisition Regulation (FAR), Part 13, 48 CFR part 13, and Public Law 93–579, section 7(b). https://www.govinfo.gov/content/pkg/FR-2020-04-23/pdf/2020-08611.pdf

- SORN 13VA047 ''Individuals Submitting Invoices-Vouchers For Payment-VA" https://www.oprm.va.gov/docs/sorn/SORNsPriorto1995.docx

- SORN 88VA244 "Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line System (CAR/CAROLS, combined system referred to as CAO) https://www.govinfo.gov/content/pkg/FR-2018-08-13/pdf/2018-17228.pdf

- SORN 27VA047 "Personnel and Accounting Integrated Data System-VA" https://www.govinfo.gov/content/pkg/FR-2012-07-02/pdf/2012-16167.pdf

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

N/A

- SORN 27VA047 ‘‘Personnel and Accounting Integrated Data System’’-VA states authority is 38 U.S.C. 501(a); 5 U.S.C. Part III, Subparts D and E.

- SORN 88VA244 ‘‘Accounts Receivable Records-VA’’ states: Government records are maintained and managed under the authority set forth in 31 U.S.C. 3101 and 31 U.S.C. 3102. The purpose of the system is consistent with the financial management provisions of title 31, United States Code, chapter 37, the pay administration provisions of title 5, United States Code, chapter 55, and special provisions relating to VA benefits in title 38, United States Code, chapter 53.
    - The System of record Notice (SORN) ‘‘Accounts Receivable Records—VA’’ (88VA244). The SORN can be found online at: https://www.gpo.gov/fdsys/pkg/FR-1998-04-06/pdf/98-8868.pdf

D. System Changes

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

No

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

No

Section 1. Characterization of the Information

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

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

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

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

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

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

☒ Name ☒ Social Security Number ☐ Date of Birth ☐ Mother’s Maiden Name

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

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

PII Mapping of Components (Servers/Database)

Electronic Data Interchange – General (EDI) consists of **4** key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **Electronic Data Interchange – General (EDI)** and the reasons for the collection of the PII are in the table below.

Note: Due to the PIA being a public facing document, please do not include the server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

Internal Database Connections

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
EDI Denver Distribution Center (EDD) Vafscsqlecb201 (development) Limited access database	**No – uses (converts input format to EDI standard formats) but does not directly collect or store**	**No**	**Partial SSN**	**Partial SSN is used to identify patient for the purpose of verifying eligibility and payment of medical claims**	**Backed by the necessary contractual and Business Associate Agreement (BAA) controls in**

					accordance with HIPAA guidelines

VL Trader Archive – Denver Logistics Center – See above \\vafscsvm03.aac.dva.va.gov\dataexchange_prod$\archive	**No – uses (converts input format to EDI standard formats) but does not directly collect or store**	**No**	**Partial SSN Last name**	**Partial SSN is used to identify patient for the purpose of verifying eligibility and payment of medical claims**	**Backed by the necessary contractual and Business Associate Agreement (BAA) controls in accordance with HIPAA guidelines**

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?

Sources of the EDI data are from the following internal VA systems: Financial Service Center (FSC) servers, Data Management Interface (DMI), Veterans Health Information Systems and Technology Architecture (VISTA) sites (VA Hospitals and facilities), VL Trader, Invoice Payment and Processing System (IPPS). servers, Data Management Interface (DMI), Veterans Health Information Systems and Technology Architecture (VISTA) sites (VA Hospitals and facilities), VL Trader, Invoice Payment and Processing System (IPPS).

EDI does not directly collect the information contained in the processes. The information is pulled from other VA systems (such as VISTA). Any notice provided would be made through those applications or the source locations.

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.

See above

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

N/A

1.3 How is the information collected?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

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

technologies or other technologies used in the storage or transmission of information in identifiable form?

Information is obtained via electronic transfer from internal VA systems listed above in section 1.2 and manually input from authorized VA employees/contractors.

1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form's OMB control number and the agency form number.

N/A

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.

EDI does not check the information within each file for accuracy. EDI does validate that any received X12 file header count is matched to the number of transactions within the file and file syntax meets industry standards to ensure that we have processed all transactions in the file. Any outbound X12 files would be caught when a 997 is received indicating an error in the transaction counts or syntax errors with the fil

1.4b If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

N/A

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

As stated in System of Records Notice (SORN) 13VA047" Individuals Submitting Invoices/Vouchers For Payment-VA", authority for maintenance of the system is the Budget and Accounting Act of 1950 and General Accounting Office Title 8, Chapter 3.

SORN 27VA047 ''Personnel and Accounting Integrated Data System''-VA states authority is 38 U.S.C. 501(a); 5 U.S.C. Part III, Subparts D and E.

SORN 88VA244 ''Accounts Receivable Records-VA'' states: Government records are maintained and managed under the authority set forth in 31 U.S.C. 3101 and 31 U.S.C. 3102. The purpose of the system is consistent with the financial management provisions of title 31, United States Code, chapter 37, the pay administration provisions of title 5, United States Code, chapter 55, and special provisions relating to VA benefits in title 38, United States Code, chapter 53.

SORN 131VA047 "Purchase Credit Card Program-VA" states authority is Federal Acquisition Regulation (FAR), Part 13, 48 CFR part 13, and Public Law 93–579, section 7(b).

1) The System of record Notice (SORN) ''Individuals Submitting Invoices-Vouchers For Payment-VA" (13VA047) https://www.oprm.va.gov/docs/sorn/SORNsPriorto1995.docx

The System of record Notice (SORN) ''Accounts Receivable Records—VA'' (88VA244). The SORN can be found online at: https://www.gpo.gov/fdsys/pkg/FR-1998-04-06/pdf/98-8868.pdf

SORN 131VA047 "Purchase Credit Card Program-VA" can be found at: https://www.gpo.gov/fdsys/pkg/FR-2015-09-09/pdf/2015-22620.pdf

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: EDI uses Personally Identifiable Information (PII) and other sensitive information previously collected from Veterans and dependents by other VA systems. 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: The Department of Veterans Affairs is careful to only collect the information necessary to identify the parties involved in an incident, identify potential issues and concerns, and offer assistance to the affected parties so that they may find the help they need to get through their crisis. By only collecting the minimum necessary information, the VA is able to better protect the individual's information. Any exchange of information or data between the VA and external (non-VA) trading partners is done via FSC owned software that meets federal and VA data security requirements.

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 – used to identify business/vendor
- SSN (Partial-last 4) – used to uniquely identify the record
- Mailing Address – used to document locations and to communicate with vendors/financial institutions and recipients
- Zip Code – part of mailing address
- Financial Data – Uses described below:
    - EDP processes financial data, which primarily includes purchase orders, payment information, credit card data, vendor product information, and buyer information Used for purchasing goods
    - EDS processes financial data, which includes state bank information, federal tax information and IDs, state GSA codes, payments
    - EDD processes financial data, which includes purchase orders, costs, sender and billing information, facilities, credit card and payment information, product descriptions, recipients, and locations
    - EDF processes invoices

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.

EDI does not have the capability to analyze data. EDI does have the ability to review the format of a file (protocol/programming of the data) and convert the format into an EDI standard format (such as X12).

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.

N/A

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?

Data is shared internally with the FSCs Managed File Transfer system VL Trader. Data in transit is secured via sFTP with Transport Layer Security, Data. Data at rest is secured via hardware encrypted devices residing on the AITC mainframe and FSC SAN.

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

For EDI Denver Distribution Center (EDD), the system does not collect or store PII. However, part of the Veteran's Social Security Number (SSN) is used for the purpose of verifying eligibility and payment of medical claims. The SSN is backed by the necessary contractual and Business Associate Agreement (BAA) controls in accordance with HIPAA guidelines.

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

In order to protect veteran personally identifiable information (PII) the following activities occur as part of the overall information assurance activities:

1. The information with each application is categorized in accordance with FIPS 199 and NIST SP 800-60. As part of the categorization any PII is identified.

2. The VA has policies which direct and guide the activities and processes performed by the VA. The policies are periodically reviewed to ensure completeness and applicability.

3. The NIST SP 800-53 controls are selected based on the categorization. The controls provide protection for veteran PII while developed or stored by an application or IT system, physically transported, between facilities, least privilege, stored offsite, or transmitted between IT centers.

4. Internal protection is managed by access controls such as user IDs and passwords, authentication, awareness and training, auditing, and internal network controls. Remote protection is provided by remote access control, authenticator management, audit, and encrypted transmission.

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?

Access privileges are determined as part of the account request process. Users submit a form or apply electronically (using CARS or ePAS) requesting access; and acknowledging that they are current on their Privacy and Cyber Security training and Rules of Behavior. The user's supervisor must sign the request to indicate approval; the appropriate ISO, after verifying the training, also signs to indicate approval. Once the ISO signs off, he/she forwards the request to the application administration group for account creation. Service accounts are created through the account request process.

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

EDI currently uses three different mechanisms for account management:
1. VA 9957
2. Computer Access Request System (CARS)
3. Electronic Permission Access System (ePAS)

2.4c Does access require manager approval?

Yes

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

Mainframe administration staff handle all account provisioning for EDI. Users are only granted the level access they need to accomplish the tasks they are assigned too.

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

Every authorized user is responsible for safeguarding PII.

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*

General (EDI) processes translate data and transmit the data for further retention/processing by other applications/processes. Data is only retained for 10years for medical claims, last 4 of Social Security numbers and name of users on the financial side is retained for 6 years.

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.*

General (EDI) data is not retained.
Official record held in the office of record
Temporary; destroy 6 years after final payment or cancellation, but longer retention is authorized if required for business use. (GRS 1.1, Item 010) (DAA-GRS-2013-0003-0001)
13VA047: Governed by General Accounting Office Regulations which require retention for records created prior to July 2,1975: 10 years and 3 months after the period of the account; records created on and after July 2, 1975: 6 years and 3 months after the period of the account. Records are normally retired to Federal Record Centers within 1 or 2 years after payment and audit.

b. All other copies.
Temporary; destroy when business use ceases. (GRS 1.1, Item 011) (DAA-GRS-2013-0003-0002)
[NOTE 1: Procurement and other financial files that stand out because of high dollar value, media attention, historical value, research value, or other extenuating circumstances may have permanent value. Agencies that believe they hold such files should submit a records schedule to NARA.]
[NOTE 2: Accounts and supporting documents pertaining to American Indians are not authorized for disposal by this schedule. Such records should be reviewed and scheduled appropriately by the agency since they may be needed in litigation involving the Government's role as trustee of property held by the Government and managed for the benefit of Indians.]
[NOTE 3: The Comptroller General has the right to require an agency to retain any portion of these records for a period of up to 10 years.]

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.
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?

EDI data is temporary and follows Records Control Schedule (RCS) 10-1 which has been approved by NARA. RCS 10-1 is available online at: https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

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

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

EDI data is temporary and follows Records Control Schedule (RCS) 10-1 which has been approved by NARA. RCS 10-1 is available online at: https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

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

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

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

Electronic media sanitization, when the records are authorized for destruction (or upon system decommission), will be carried out in accordance with VA 6500.1 HB Electronic Media Sanitization.

Disposition of Printed Data:
Forms and other types of printed output produced by any computer systems and related peripherals will be evaluated by the responsible staff member for data sensitivity. Printed output containing sensitive data will be stored in locked cabinets or desks and disposed of properly (when the approved records schedule permits destruction) by shredding or similar VA approved methods in accordance with VA Directive 6371. Program listings and documentation relating to the use of or access to a computer system require special handling if the listings or documentation provide information about a system which processes sensitive data. VA personnel are responsible for retrieving/removing all printed outputs they request from printers.

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.

VA minimizes where feasible the risk to privacy of using PII for training and research by following VA policy and performing privacy reviews as necessary. VA OI&T must address risk to privacy regarding testing per their software quality assurance processes.

VA Handbook 6500 mandates that Systems under development should not process "live data" or do any real processing in which true business decisions will be based. Test data that is de-identified should be used to test systems and develop systems that have not yet undergone security A&A. Furthermore, systems that are in development (pilot, proof-of-concept, or prototype) should not be attached to VA networks without first being assessed and authorized.

VA wide Directive 6511 describes the responsibilities, requirements, and procedures for eliminating PII or information exempt from release under FOIA from presentations that may be seen by non-VA parties. This Directive includes guidance for conducting privacy reviews of presentations, and the criteria for when presenters must self-certify that their presentations are devoid of PII or information exempt from release under FOIA.

When testing is performed, test data with all personally identifying information removed is sent to FSC ECD for testing purposes.

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

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

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

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

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

<u>Principle of Data Quality and Integrity:</u> Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?

This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:

Privacy Risk: Though General (EDI) does not retain data at this time, should there be a future need to retain information, there is a risk that the information processed by EDI 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, the EDI adheres to the VA RCS schedules for each category or data it maintains. When the retention date is reached for a record, EDI staff will carefully dispose of the data by the determined method as described in question 3.4. VA Handbook 6500.2, Management of Data Breaches Involving Sensitive Personal Information (SPI), which contains the policies and responsibilities that VA components are required to follow to manage data breaches, including detection, correlation, notification, remediation, and reporting.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA.

4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

NOTE: Question 3.9 (second table) on Privacy Threshold Analysis should be used to answer this question.

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Financial Service Center (FSC)	Hearing aid orders and related Invoices in support of Hearing Aids are sent to the FSC servers so the information can be reformatted and sent to the vendor	Name, Mailing Address, Zip Code, Financial Account Information, , and Last 4 Numbers of SSN	MLLP, AS2, SSH FTP & FTP/s with TLS
Data Management Interface (DMI)	Hearing aid orders and related Invoices in support of Hearing Aids are sent to the FSC servers so the information can be reformatted and sent to the vendor	Name, Mailing Address, Zip Code, Financial Account Information, , and Last 4 Numbers of SSN	MLLP, AS2, SSH FTP & FTP/s with TLS
FSC VL Trader	Hearing aid orders and related Invoices in support of Hearing Aids	Name, Mailing Address, Zip Code, Financial Account	MLLP, AS2, SSH FTP & FTP/s with TLS

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*
	are sent to the FSC servers so the information can be reformatted and sent to the vendor	Information, and Last 4 Numbers of SSN	

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 transmitting PII within the Department of Veterans' Affairs is that the data may be disclosed to individuals who do not require access or have a need to know. Inappropriate/unauthorized disclosure heightens the threat of the information being misused.

Mitigation: The principle of need-to-know is strictly adhered to by EDI 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: Question 3.10 on Privacy Threshold Analysis should be used to answer this question.

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

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

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

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

Data Shared with External Organizations

Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system <u>outside</u> the VA with which information is shared	**Specifically list the Data Elements Shared/Received**	**Type of Connection**	**Agreement Type (Can be more than one)**
EDI does not share data externally	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.

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

Follow the format below:

Privacy Risk: There is no risk or mitigation because EDI does not share/receive data externally.

Mitigation: Not applicable

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.

EDI does not directly collect the information contained in the processes. The information is pulled from other VA systems (such as VISTA). Any notice provided would be made through those applications or the source locations.

For VHA related Privacy Notification online can be found at: http://www.va.gov/health after getting to the website, select VA Privacy Practices link on the lower right side of the web page.

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

The System of record Notice (SORN) ‘‘Individuals Submitting Invoices-Vouchers For Payment-VA” (13VA047) https://www.oprm.va.gov/docs/sorn/SORNsPriorto1995.docx

The System of record Notice (SORN) ‘‘Accounts Receivable Records—VA’’ (88VA244). The SORN can be found online at: https://www.gpo.gov/fdsys/pkg/FR-1998-04-06/pdf/98-8868.pdf

SORN 131VA047 “Purchase Credit Card Program-VA” can be found at: https://www.gpo.gov/fdsys/pkg/FR-2015-09-09/pdf/2015-22620.pdf

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

This Privacy Impact Assessment (PIA) also serves as notice of the EDI system. As required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs “after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means.” PIAs are published at: https://www.oprm.va.gov/privacy/pia.aspx

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.

VHA Handbook 1605.1 Appendix D ‘Privacy and Release Information’, section 5 lists the rights of the Veterans to request VHA to restrict the uses and/or disclosures of the individual’s individually identifiable health information to carry out treatment, payment, or health care operations. The Veterans have the right to refuse to disclose their SSN to VHA. 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).

No information is directly collected from the Veteran by EDI so there is no opportunity to decline to provide information. A Veteran may have the opportunity or notice of the right to decline to provide information to the source systems that collect the information from the Veteran. By declining to supply information to the source system, the Veteran would also be declining the information to the EDI system and other downstream applications.

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 uses of the information would be handled by the source systems that collect the information from the Veteran and feed EDI with information. Source systems for EDI are Financial Service Center (FSC) servers, Data Management Interface (DMI), Veterans Health Information Systems and Technology Architecture (VISTA) sites (VA Hospitals and facilities), VL Trader, Invoice Payment and Processing System (IPPS).

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 members of the public may not know the EDI 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.
EDI does not collect information directly from Veterans. Notice would be given upstream by the departments at time of collection.
Annual Privacy and security awareness and rules of behavior training along with restricted access are in place to ensure the users know the information is only to be used for the purpose of the system.

Section 7. Access, Redress, and Correction

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

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

These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. ***For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.***

Since EDI does not collect data directly from Veterans/individuals, the following procedures would apply:
The following procedures are from VA Handbook 6300.4:
(1) An individual may request amendment of a record pertaining to him or her contained in a specific VA system of records by mailing or delivering the request to the office concerned. The request must be in writing and must conform to the requirements in paragraph 3b(3) of this handbook. It must state the nature of the information in the record the individual believes to be inaccurate, irrelevant, untimely, or incomplete; why the record should be changed; and the amendment desired. The requester should be advised of the title and address of the VA official who can assist in preparing the request to amend the record if assistance is desired.
(2) Not later than 10 days, excluding Saturdays, Sundays, and legal public holidays, after the date of receipt of a request to amend a record, the VA official concerned will acknowledge in writing such receipt. If a determination has not been made, the acknowledgement will inform the individual when he or she may expect to be advised of action taken on the request. VA will complete a review of the request to amend or correct a record as soon as reasonably possible, normally within 30 days from receipt of the request (excluding Saturdays, Sundays, and legal public holidays)
(3) Where VA agrees with the individual's request to amend his or her record(s), the requirements of 5 U.S.C. 552a(d) will be followed. The record(s) will be corrected promptly, and the individual will be advised promptly of the correction. Amendment consists of adding information to the record, altering information in the record, or deleting information in the record. Under the Privacy Act, if information is altered or deleted, the previous version must be obliterated and illegible after amendment. The amendment should be annotated "Amended, Privacy Act, (date), (signature and title of amending official)."
(4) If the record has previously been disclosed to any person or agency, and an accounting of the disclosure was made, prior recipients of the record will be informed of the correction. FL 70- 19, Notification to Other Person or Agency of Amendment to a Record, may be used.
(5) If it is determined not to grant all or any portion of the request to amend a record, the official will promptly notify the individual in writing. The individual will be advised of his or her right to file a concise statement of reasons for disagreeing with the refusal to amend. The notice will specify the reason(s) for denying the request, identify the VA regulations or statutes upon which the denial is based, and advise that the denial may be appealed in writing to the General Counsel (024),

Department of Veterans Affairs, 810 Vermont Avenue, NW, Washington, DC 20420. FL 70-20, Notification of Initial Refusal to Amend a Record Under the Privacy Act, may be used for this purpose.
(6) The determination on an appeal will be made not later than 30 days, excluding Saturdays, Sundays, and legal public holidays, from the date the individual's letter of appeal is received unless the Secretary or Deputy Secretary, for good cause shown, extends such 30-day period. If the 30-day period is so extended, the individual will be notified promptly of the reasons for the extension and the date on which a final determination may be expected. The final determination in such appeals will be made by the General Counsel or Deputy General Counsel.
(7) If the General Counsel or Deputy General Counsel finds that the adverse determination should be reversed, he or she will notify the VA office or station of the remedial action to be taken. The VA office or station will promptly carry out that action. The General Counsel or Deputy General Counsel will promptly notify the individual in writing of the corrective action. The field station or Central Office organization that provided the initial decision will inform previous recipients of the record that a correction has been made.
(8) If the General Counsel or Deputy General Counsel determines that the adverse determination will not be reversed, the individual will be notified promptly in writing of that determination, the reasons therefor, and of his or her right to seek judicial review of the decision pursuant to section 3 of the Privacy Act (5 U.S.C. 552a(g)).
(9) If the adverse determination is sustained by the General Counsel or Deputy General Counsel, the individual will also be advised promptly of his or her right to file a concise statement of reasons for disagreeing with the refusal to amend. The statement may contain information that the individual believes should be substituted.
(10) When an individual files a statement disagreeing with VA's decision not to amend a record, the record will be clearly annotated so that the fact that the record is disputed is apparent to anyone who may subsequently access, use, or disclose it. When the disputed record is disclosed to persons or other agencies, the fact of the dispute will be clearly noted. Copies of the statement of disagreement will be provided, and, when appropriate, copies of a concise statement of VA's reasons for not making the amendment(s) requested will also be provided.
(11) A decision by either the General Counsel or Deputy General Counsel pursuant to paragraph 3f(7) of this handbook is final. It is subject to judicial review in the district court of the United States in which the complainant resides, or has his or her principal place of business, or in which the VA records are located, or in the District of Columbia.

SORN 131VA047 states: Individuals seeking information concerning the existence of a record pertaining to them must submit a written request to the VA station where the records are maintained. Such request must contain a reasonable description of the records requested. In addition, identification of the individual requesting the information will be required in the written request and will consist of the requester’s name, signature, and address, at a minimum.

SORN 88VA244 states: An individual who wishes to determine whether a record is being maintained in this system under his or her name or other personal identifier, or wants to determine the contents of such record, should submit a written request to the system manager. Director, Debt Management Center (389/00), U.S. Department of Veterans Affairs, Bishop Henry Whipple Federal Building, 1 Federal Drive, Ft. Snelling, MN 55111.

SORN 27VA047 states: Individuals seeking information concerning the existence of a record pertaining to themselves must submit a written request to the VA station of employment. Such

request must contain a reasonable description of the records requested. In addition, identification of the individual requesting the information will be required in the written request and will consist of the requester's name, signature, address, and social security number, or other identifier, as a minimum.

SORN 13VA047 states: Individuals or authorized representatives seeking information regarding access to and contesting of records may write, call or visit the VA office to which the invoice/voucher was submitted.

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).

See above, 7.1a

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.

See above, 7.1a

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.

For data 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.

The correction procedures are the same as those given in question 7.1a.

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.

Data provided to the EDI system is derived from other VA systems: Financial Service Center (FSC) servers, Data Management Interface (DMI), Veterans Health Information Systems and Technology Architecture (VISTA) sites (VA Hospitals and facilities), VL Trader, Invoice Payment and Processing System (IPPS). The opportunity to notify individuals may be provided during collection of the data for those systems prior to data being transferred to EDI. For data under the jurisdiction of VHA procedures are described in section 7.2 above.

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.

There is no formal redress for records stored with EDI; however, Veterans and other beneficiaries may contact their supporting VA regional office or VHA center to learn how to access, correct, or contest their information.

Formal redress procedures are provided in the SORNs that are designated for the systems that generate the input to EDI. Formal redress procedures are provided in SORNs 131VA047, 88VA244, 27VA047 and 13VA047.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that a Veteran could accidentally provide incorrect information to the VA when enrolling for health benefits and that incorrect information could be disseminated by EDI.
There is a risk that individuals may seek to access or redress records about them held in EDI General and become frustrated with the results of their attempt.

Mitigation: There is no direct mitigation for EDI. All access, redress and correction would fall on the source systems that provide input data to EDI. EDI only disseminates information provided by other systems. However, Veterans have the ability to update their enrollment information in the source systems using VA form 10-10EZR and turning that into the VA Office or VA Station they work with locally for benefits.
Individuals would have the opportunity to address access, redress and correction of their data with the departments and facilities that oversee the source systems that provide data to EDI.

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.

EDI currently uses three different mechanisms for account management:
1. VA 9957
2. Computer Access Request System (CARS)
3. Electronic Permission Access System (ePAS)
4. VA Identity and Access Management System (IAM)

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?

Access privileges are determined as part of the account request process. Users submit a form or apply electronically (using CARS or ePAS) requesting access; and acknowledging that they are current on their Privacy and Cyber Security training and Rules of Behavior. The user's supervisor must sign the request to indicate approval; the appropriate ISO, after verifying the training, also signs to indicate approval. Once the ISO signs off, he/she forwards the request to the application administration group for account creation. Service accounts are created through the account request process. Mainframe administration staff handle all account provisioning for EDI. Users are only granted the level access they need to accomplish the tasks they are assigned too.

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.

Access privileges are determined as part of the account request process. Users submit a form or apply electronically (using CARS or ePAS) requesting access; and acknowledging that they are current on their Privacy and Cyber Security training and Rules of Behavior. The user's supervisor must sign the request to indicate approval; the appropriate ISO, after verifying the training, also signs to indicate approval. Once the ISO signs off, he/she forwards the request to the application administration group for account creation. Service accounts are created through the account request process. Mainframe administration staff handle all account provisioning for EDI. Users are only granted the level access they need to accomplish the tasks they are assigned too.

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.

VA contract employee access is verified through the Contracting Officer's Representative (COR) and other VA supervisory/administrative personnel before access is granted to any VA system. Contractor access is 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 Talent Management System (TMS). All contractors are vetted using the VA background investigation process and must obtain the appropriate level background investigation for their role. Contractors with systems administrative access are required to complete additional role-based training prior to gaining system administrator access. Generally, contracts are reviewed at the start of the initiation phase of acquisitions and again during procurement of option years by the Contracting Officer, Information Security Officer, Privacy Officer, COR, Procurement Requestor/Program Manager and any other stakeholders required for approval of the acquisition.

Contracts generally have an average duration of 1-3 years and may have option years stipulated in the original contract.

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.

Personnel that will be accessing information systems or VA sensitive data must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the annual security awareness training which all personnel must complete via the VA's Talent Management System (TMS). After the user's initial training and acceptance of the Rules, the user must reaffirm their acceptance annually as part of the privacy and security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system. System administrators are required to complete additional role-based training. Users with access to PHI are required to complete HIPAA privacy training annually.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Current
2. *The System Security Plan Status Date:* 4/11/2023
3. *The Authorization Status:* Current
4. *The Authorization Date:* 21 May 2021
5. *The Authorization Termination Date:* 20 May 2024
6. *The Risk Review Completion Date:* 21 May 2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

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

EDI was granted a full ATO on 26 December 2017 which expires on 25 December 2020. FIPs 199 classification of the system is Mode.

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)*

No

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.*

No

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

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

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

No

9.4 NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

N/A

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).

No

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

ID	Privacy Controls
AP	**Authority and Purpose**
AP-1	Authority to Collect
AP-2	Purpose Specification
AR	**Accountability, Audit, and Risk Management**
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-7	Privacy-Enhanced System Design and Development
AR-8	Accounting of Disclosures
DI	**Data Quality and Integrity**
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
DM	**Data Minimization and Retention**
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
IP	**Individual Participation and Redress**
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
SE	**Security**
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR	**Transparency**
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**

ID	Privacy Controls
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

DEEA LACEY

Digitally signed by DEEA LACEY
Date: 2023.07.18 14:32:09 -05'00'

Privacy Officer, Deea Lacey

RUBEN ROSALES 159850

Digitally signed by RUBEN ROSALES 159850
Date: 2023.07.19 07:11:36 -06'00'

Information System Security Officer, Ruben Rosales

JONATHAN LINDOW

Digitally signed by JONATHAN LINDOW
Date: 2023.07.19 08:58:18 -05'00'

Information System Owner, Jonathan Lindow

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).

SORN 131VA047 "Purchase Credit Card Program-VA" states authority is Federal Acquisition Regulation (FAR), Part 13, 48 CFR part 13, and Public Law 93–579, section 7(b).

- The System of record Notice (SORN) ''Individuals Submitting Invoices-Vouchers For Payment-VA" (13VA047) https://www.oprm.va.gov/docs/sorn/SORNsPriorto1995.docx
- SORN 131VA047 "Purchase Credit Card Program-VA" can be found at: https://www.gpo.gov/fdsys/pkg/FR-2015-09-09/pdf/2015-22620.pdf.

- SORN 27VA047 ''Personnel and Accounting Integrated Data System''-VA states authority is 38 U.S.C. 501(a); 5 U.S.C. Part III, Subparts D and E.
  https://www.govinfo.gov/content/pkg/FR-2012-07-02/pdf/2012-16167.pdf

- SORN 88VA244 ''Accounts Receivable Records-VA'' states: Government records are maintained and managed under the authority set forth in 31 U.S.C. 3101 and 31 U.S.C. 3102. The purpose of the system is consistent with the financial management provisions of title 31, United States Code, chapter 37, the pay administration provisions of title 5, United States Code, chapter 55, and special provisions relating to VA benefits in title 38, United States Code, chapter 53.
  - The System of record Notice (SORN) ''Accounts Receivable Records—VA'' (88VA244). The SORN can be found online at: https://www.gpo.gov/fdsys/pkg/FR-1998-04-06/pdf/98-8868.pdf

HELPFUL LINKS:

Record Control Schedules:

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

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

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

National Archives (Federal Records Management):

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

VHA Publications:

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

VA Privacy Service Privacy Hub:

https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices