Privacy Impact Assessment for the VA IT System called:

Payer Electronic Data Interchange (EDI) Transactions Application Suite (TAS)

Veterans Health Administration (VHA)

Office of Integrated Veteran Care

eMASS ID # 1317

Date PIA submitted for review:

01/16/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Michael Hartmann	Michael.Hartmann@va.gov	303-780-4753
Information System Security Officer (ISSO)	Richard Alomar-Loubriel	Richard.Alomar-Loubriel@va.gov	787-641-7582 x11411
Information System Owner	Dena Liston	Dena.Liston@va.gov	304-886-7367

Abstract

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

Payer Electronic Data Interchange (EDI) Transactions Applications Suite (TAS) (PED) is a cloud based Microservices Architecture system that delivers Community Care Payer business services. The platform transitions business logic from existing capabilities to a modernized solution. The solution includes a gateway to send and receive EDI transactions to industry partners, ensures X12 compliance, and routes and maps data to appropriate repositories and systems. The solution supports Veterans Administration (VA) funded industry provided services to Veterans and Veteran beneficiaries. Payer EDI TAS will interface with both internal and external systems in end-to-end healthcare claim processing. Payer EDI TAS is key to timely payments to industry Providers providing Veteran service-related services - an incentive for the private healthcare community to welcome Veteran business.

Overview

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

1 General Description

A. What is the IT system name and the name of the program office that owns the IT system?

Payer Electronic Data Interchange (EDI) Transactions Applications Suite (TAS). Office of Integrated Veteran Care (IVC)

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

The system provides automation to process related Healthcare (professional, institutional, dental, and pharmacy) claims is accomplished via the interaction of several applications, both internal and external. Payer Electronic Data Interchange (EDI) Transactions Application Suite (TAS) is the single-entry point for data from interfacing applications and the single exit point for data to interfacing applications. As a part of its controlled routing of data, Payer EDI TAS also serves as a master scheduler of processing against the data, i.e., what interfacing partner needs what data and when. Payer EDI TAS archives raw data, but it also records in-progress states of data and fully processed data in a SQL database. Regardless of where a claim is at any time, the VA always retains ownership of the data, and MOU/ISA documents reflect that ownership.

C. Who is the owner or control of the IT system or project?

VA Owned and VA Operated.

2. Information Collection and Sharing

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

Payer EDI TAS supports approximately 660,000+ Veterans and beneficiaries. Receives health care claims and translate and pass them to the destination systems that conduct the transactions. System does not make payment transactions but contains claims data. Processing is automated; no individuals are involved.

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

Receiving claims, adjudicating claims, and paying providers relies on connectivity between the VA and Signature Choice CXM processing, Change Healthcare Clearinghouse processing, Optum Rx processing, Claims Eligibility & Processing (CPE), Financial Management System (FMS), Program Integrity Tool (PIT), and possibly others as the application matures. While a few transaction exchanges are real-time, the majority are batch exchanges. In fact, the bulk of Payer EDI TAS processing is batch. Payer EDI TAS resides in the VAEC Amazon Web Services (AWS) cloud. Though Patient care is not dependent on Payer EDI TAS processing, Payer EDI TAS data does include extensive VA sensitive data, including Personally Identifiable Information (PII) and Protected Health Information (PHI). Processing data covered by the Privacy Act and the Title 38 confidentiality statutes in addition to HIPAA, extra steps are taken to limit gateway access by interfacing partners. All Payer EDI TAS data is understandably encrypted in transit and at rest.

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

Payer EDI TAS delivers Community Care Payer business services and is a fully automated system with minimum human interaction. It receives and translates health care claims and passes them to the destination organization/systems for processing. Currently Payer EDI TAS contains data on approximately 660,000+ Veterans and beneficiaries. The data include PII, PHI, and financial data.

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

The system operates in the Enterprise Cloud (VAEC) Amazon Web Services (AWS).

3. Legal Authority and SORN

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

SORN numbers applicable to Payer EDI TAS are listed below:

23VA10NB3, Non-VA Care (Fee) Records - VA (7/30/2015): Title 5 U.S.C 301, Title 26 U.S.C 61. Title 38, U.S.C. sections 31, 109, 111, 501, 1151 1703, 1705, 1710, 1712, 1717, 1720, 1721, 1724, 1725, 1727, 1728, 1741–1743, 1781, 1786, 1787, 3102, 5701 (b)(6)(g)(2)(g)(4)(c)(1), 5724, 7105, 7332, and 8131–8137. 38 Code of Federal Regulations 2.6 and 45 CFR part 160 and 164. Title 44 U.S.C and Title 45 U.S.C. Veterans Access, Choice, and Accountability Act of 2014.

24VA10A7, Patient Medical Records - VA (10/2/2020): Title 38, United States Code, Sections 501(b) and 304.

54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files - VA (3/3/2015): Title 38, United States Code, sections 501(a), 501(b), 1703, 1720G, 1724, 1725, 1728, 1781, 1787, 1802, 1803, 1812, 1813, 1821, Public Law 103–446 section 107 and Public Law 111–163 section 101.

58VA21, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records - VA (11/8/2021): Title 10 U.S.C. chapters 106a, 510, 1606 and 1607 and title 38, U.S.C. §501(a) and Chapters 3, 11, 13, 15, 18, 19, 21, 23, 30, 31, 32, 33, 34, 35, 36, 37, 39, 51, 53, 55 and 77. Title 5 U.S.C. 5514.

79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records – VA: Title 38, United States Code, section 7301(a).

147VA10, Enrollment and Eligibility Records - VA (8/17/2021): Title 28, United States Code, title 38, U.S.C., sections 501(a), 1705, 1710, 1722, and 5317.

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?

Yes, SORN is over 6 years old and out of date, SORN POC is aware and working on update.

4. System Changes

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

Completion of this PIA will not result in circumstances that require changes to business processes.

K. Will the completion of this PIA could potentially result in technology changes?

Completion of this PIA will not potentially result in technology changes.

Section 1. Characterization of the Information

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

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

Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy- Protected Information. For additional information on

these information types and definitions, please see VA Directives and Handbooks in the 6500 series (https://vaww.va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

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

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

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

- ☒ Name
- ☒ Social Security Number
- ☒ Date of Birth
- ☐ Mother's Maiden Name
- ☒ Personal Mailing Address
- ☒ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☒ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☒ Financial Information
- ☒ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers[1]
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☒ Medications
- ☒ Medical Records
- ☐ Race/Ethnicity
- ☒ Tax Identification Number
- ☒ Medical Record Number
- ☐ Gender
- ☐ Integrated Control Number (ICN)
- ☐ Military History/Service Connection
- ☐ Next of Kin
- ☒ Other Data Elements (list below)

Other PII/PHI data elements:

Coverage Dates
Plan Name
Current Procedural Terminology (CPT)/International Code Designator (ICD)
Coded Billing Information (Claim Index)
Billed Amounts
Other Health Insurance Information
Insurance Financial Management System (FMS)Document ID
Paid Amounts
Check or Remittance Numbers
Provider Name

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

Provider Phone Number
Provider Billing Address
Provider Physical Address
Provider Remit to Address)
Diagnosis Codes
Treatment Codes
Prescription Numbers
National Council for Prescription Drug Programs (NCPDP) Codes
Date of Service (DOS)
Place of Service (POS)
Data of Death (DOD)
2nd Address
Member Identification Number
Patient Control Number
Health Insurance Numbers (Policy Number)

PII Mapping of Components (Servers/Database)

Payer EDI TAS consists of 3 key component (Server/Database) application interfaces, Payer EDI TAS gateway, to exchange data with other applications. The component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by FPPS-Cloud and the reasons for the collection of the PII are in the table below.

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

Internal Components Table

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
Claims Oracle Database	Yes	Yes	Name, Social Security Number (SSN), Date of Birth (DOB), Data of Death (DOD), Street Address,	Data is used to track, store, and process Veteran healthcare claims	Data is encrypted at rest and in transit.

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
			City, Zip Code, Country, Email, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Number, Plan/Policy Number, Member Identification, Plan Name, Coverage Effective Dates, Coverage Limits, Co-Pays, International Code Designator (ICD), Coded Billing Information (Claim Index), Billed Amounts, Other Health Insurance Information, Other Health Insurance FMS Document ID, Tax Identification		

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
			Number (TIN),Phone Number, Place of Service (POS) Name, Place of Service Address (Street, City, Zip, Country),Date of Service, Charge Amount, Paid Amount, Diagnosis Codes, Treatment Codes, Prescription Number, NCPDP Codes, (National Council For Prescription Drug Programs)		
• Aurora Postgres (AWS Service)	Yes	Yes	Coverage Dates, Plan Name, Current Procedural Terminology, International Code Designator (ICD), Coded Billing Information (Claim	Data is used to track, store, and process Veteran healthcare claims	Data is encrypted at rest and in transit.

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
			Index), Billed Amounts, Other Health Insurance Information, Insurance FMS Document ID, Paid Amounts, Check or Remittance Numbers, Provider Name, Provider Phone Number, Provider Billing Address, Provider Physical Address, Provider Remit to Address), Tax Identification Number, Diagnosis Codes, Treatment Codes, Prescription Numbers, NCPDP Codes, Date of Service (DOS),		

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
			Place of Service (POS), Patient Name, Social Security Number (SSN), Date of Birth (DOB), Data of Death (DOD), Address, 2nd Address, Email, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Numbers, Health Insurance Numbers (Policy Number).		
• S3 Bucket (AWS Service)	Yes	Yes	Coverage Dates, Plan Name, Current Procedural	Data is used to track, store, and process Veteran	Data is encrypted at rest and in transit.

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
			Terminology, International Code Designator (ICD), Coded Billing Information (Claim Index), Billed Amounts, Other Health Insurance Information, Insurance FMS Document ID, Paid Amounts, Check or Remittance Numbers, Provider Name, Provider Phone Number, Provider Billing Address, Provider Physical Address, Provider Remit to Address), Tax Identification Number, Diagnosis	healthcare claims	

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
			Codes, Treatment Codes, Prescription Numbers, NCPDP Codes, Date of Service (DOS), Place of Service (POS), Patient Name, Social Security Number (SSN), Date of Birth (DOB), Data of Death (DOD), Address, 2nd Address, Email, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Numbers, Health		

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
			Insurance Numbers (Policy Number).		

1.2 What are the sources of the information in the system?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.2a List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

Ultimately, the data is sourced from a Veteran or Veteran beneficiary, but that information is provided to an industry provider who then submits the data to the VA via a clearing house transmission. The Payer Electronic Data Interchange (EDI) Transactions Application Suite (TAS) does not received information directly from the Veteran/Beneficiary. The system is a privacy sensitive system that collects, maintains, and/or processes Personally Identifiable Information on Veterans and/or beneficiaries. During claims processing additional information related to the claim is tagged with a Patient Document Identifier (PDI) for traceability to all related claims.

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.

Payer EDI TAS provides processing system for claims from the Clearinghouse to EDI Gateway. This is an automated process with no system administrators/users involved.

1.2c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?

The Payer EDI TAS does not create information. Information is provided to an industry provider who then submits the data to the VA via a clearing house transmissions.

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

1.3a This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from

another system, or created by the system itself. Specifically, is information collected through technologies or other technologies used in the storage or transmission of information in identifiable form?

The Payer Electronic Data Interchange (EDI) Transactions Application Suite (TAS) is a privacy sensitive system that collects, maintains, and processes healthcare claim related data for Veterans and beneficiaries. Most of claim information is collected directly from healthcare service providers via the Change Healthcare Clearinghouse. A small percentage of claims are collected directly from Veterans or their beneficiaries via United States Mail.

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

Payer EDI TAS does not collect information on a form. Information is provided to a industry providers who then submits the data to the VA via Secure Sockets Layer (SSL) transmissions

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.

Payer EDI TAS data will be subject to a variety of internal edits and reconciliations. Reports aggregating claim activity will be developed according to standard VHA controls, e.g., Claim ID, Sponsor, system performs batch and real-time processing and moves data between tables and modified data within the tables to make processed data sharable. The systems have commercially acquired integrity checks that automatically reject claims that do not meet HIPAA mandated requirements. If a claim is not properly developed the system rejects it and the clearinghouse must go back to the provider to correct the information prior to acceptance by VA.

1.4b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?

Payer EDI TAS does not utilize a commercial aggregator of information to operate or function, and it does not check the information for accuracy. The system has a number of commercially acquired integrity checks that automatically reject claims that do not meet HIPAA mandated requirements. If a claim is not properly developed the system rejects the claim and the clearinghouse must go back to the provider to correct the information prior to acceptance by VA.

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

This system supports electronic payment of health care claims and ensures VA is not in violation of the Health Insurance Portability and Accountability Act (HIPAA). The rules for data sharing are clearly laid out in the transactions sets and must be followed to the letter or claims will fail to process. The Payer EDI TAS system's legal authority for operating the system, specifically the authority to collect the information listed is found in the following SORNS and corresponding Legal Authorities:

23VA10NB3, Non-VA Care (Fee) Records - VA (7/30/2015): Title 5 U.S.C 301, Title 26 U.S.C 61. Title 38, U.S.C. sections 31, 109, 111, 501, 1151 1703, 1705, 1710, 1712, 1717, 1720, 1721, 1724, 1725, 1727, 1728, 1741–1743, 1781, 1786, 1787, 3102, 5701 (b)(6)(g)(2)(g)(4)(c)(1), 5724, 7105, 7332, and 8131–8137. 38 Code of Federal Regulations 2.6 and 45 CFR part 160 and 164. Title 44 U.S.C and Title 45 U.S.C. Veterans Access, Choice, and Accountability Act of 2014.
24VA10A7, Patient Medical Records - VA (10/2/2020): Title 38, United States Code, Sections 501(b) and 304.
54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files - VA (3/3/2015): Title 38, United States Code, sections 501(a), 501(b), 1703, 1720G, 1724, 1725, 1728, 1781, 1787, 1802, 1803, 1812, 1813, 1821, Public Law 103–446 section 107 and Public Law 111–163 section 101.
58VA21, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records - VA (11/8/2021): Title 10 U.S.C. chapters 106a, 510, 1606 and 1607 and title 38, U.S.C. §501(a) and Chapters 3, 11, 13, 15, 18, 19, 21, 23, 30, 31, 32, 33, 34, 35, 36, 37, 39, 51, 53, 55 and 77. Title 5 U.S.C. 5514.
79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records – VA: Title 38, United States Code, section 7301(a).
147VA10, Enrollment and Eligibility Records - VA (8/17/2021): Title 28, United States Code, title 38, U.S.C., sections 501(a), 1705, 1710, 1722, and 5317

Notice is provided by the system's System of Record Notice (SORN), **Electronic Document Management System (EDMS)-VA, VA SORN 54VA10NB3:** that covers Veterans, Dependents, Healthcare providers treating individuals and caregivers of Veterans.

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

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: The system collects more information PII and/or PII than is necessary to complete the business need and process.

Mitigation: The information contained within the system is not originated by VA but is used by VA for purpose of Attachment process to providers and beneficiaries. The system contains coded data that is industry standard and complies with the Health Insurance Portability and Accountability Act (HIPAA) requirements. The system is scanned by National Security Operations Center NSOC for vulnerabilities and those vulnerabilities addressed to the extent possible. The system is also only accessible by authorized staff on the VA network. The system is unreachable without approved remote access protocols from the outside world. All incoming and outgoing data to and from the system is sent through Federal Information Processing Standard (FIPS) 140-2 approved encryption.

Section 2. Uses of the Information

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

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

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

PII/PHI Data Element	Internal Use	External Use
Patient Name	To properly identify, adjudicate and pay claims	To support electronic payment of health care claims.

PII/PHI Data Element	Internal Use	External Use
Social Security Number (SSN)	To properly identify, adjudicate and pay claims	To support electronic payment of health care claims.
Member Identification Number	To properly identify, adjudicate and pay claims	To support electronic payment of health care claims.
Patient Control Number	To ensure attachment records accuracy	To support electronic payment of health care claims.
Medical Record Identification Number	To properly identify, adjudicate and pay claims	To support electronic payment of health care claims.
Date of Birth (DOB)	To properly identify, adjudicate and pay	To support electronic payment of health care claims.
Date of Death (DOD)	To properly identify, adjudicate and pay	To support electronic payment of health care claims.
Address; Zip Code	To properly identify, adjudicate and pay claims	To support electronic payment of health care claims.
Plan Name	To properly identify, adjudicate and pay claims	To support electronic payment of health care claims.
Email	To properly identify, adjudicate and pay claims	To support electronic payment of health care claims.
Health Insurance Numbers	To properly identify, adjudicate and pay claims	To support electronic payment of health care claims.
Coverage Dates	To provide actual dates for adjudication and pay claims	To support electronic payment of health care claims.
Date of Service (DOS)	To provide actual dates for adjudication and pay claims	To support electronic payment of health care claims.
Place of Service (POS)	To provide actual dates for adjudication and pay claims	To support electronic payment of health care claims.
CPY and International Code Designator (ICD) Coded Billing Information	To properly identify, adjudicate and pay claims	To support electronic payment of health care claims.
Health Information (and other insurance)	To properly identify, adjudicate and pay claims	To support electronic payment of health care claims.
Prescription/NCPDP Codes Information	To properly identify, adjudicate and pay claims	To support electronic payment of health care claims.
Procedure/Treatment/Diagnosis Codes Number/Coded Billing Information (Claim Index)	To properly identify, adjudicate and pay claims	To support electronic payment of health care claims.
Paid Amounts Information (Check/Remittance Numbers)	To properly identify, adjudicate and pay claims	To support electronic payment of health care claims.
Tax Identification Number (TIN)	To properly identify, adjudicate and pay claims	To support electronic payment of health care claims.
Provider Name, Phone, Billing Address, Physical Address	To properly identify, adjudicate and pay claims	To support electronic payment of health care claims.
Provider TIN	To properly identify, adjudicate and pay claims	To support electronic payment of health care claims.

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?

The ClaimXM system will provide to the VA a series of reports on volume processed and frequencies. Claims processed will ultimately reside in the Claims Processing & Eligibility (CP&E) Data Warehouse for analysis.

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.

The ClaimXM system will provide to the VA a series of reports on volume processed and frequencies. Claims processed will ultimately reside in the CP&E Data Warehouse for analysis.

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?

For Data at Rest, the storage device used to collect, process and/or retain information to include Social Security Numbers is an Encrypted Storage Array which is FIPS-140 compliant. For Data in Transit, the Network Encryption protects data in transit. It provides all data network encryption and integrity to ensure that data is secure as it travels across the network.

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

Data in transit is protected by means of industry standard encryption protocols (e.g., HTTPS, VPN, etc.). Data at rest is FIPS 140-3 compliant and fully encrypted at aggregate-level. All data is encrypted while at rest and during transmission. Appropriate security controls are in place to guard against unauthorized access to the data.

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

System data is encrypted at rest and in transit at or above the VA requirements. The Technical Safeguards used to protect PII/PHI data are, two factor authentication (2FA), authorized access through the VA intranet only, the 15-minute timeout/session lock. For elevated

privileges approval is required before an Electronic Permissions Access System (ePAS) can be submitted for approval.

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 Controls- All access requests are submitted and processed internally through the Payer EDI TAS system utilizing only approved VA two factor authentication with PIV and only with an approved Active Directory (AD) account. System uses Active Directory (AD) authentication. (Access denied/granted depending on AD account that initiates a browser session). Access requests are reviewed by Office of Information Technology(OIT) team, who act as system administrators. Enforced with the following criteria: o No user can request access for themselves. The request must identify exact roles required. A request can only be approved if the submitter is a "Tier" or "Role" above the individual gaining access.

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

Yes, all employees and contractors with access to Veterans' information are required to complete VA Rules of Behavior and VA Privacy and Security training annually. Disciplinary actions, up to and including termination of employment, are possible for violations of the requirements specified in the training and their positions. These access rights are removed and reassigned for each transferred user, and these access permissions are re-approved annually.

2.4c Does access require manager approval?

Access is processed through the e9957 process. Local approval from supervisors and designated authorization officials are required prior to granting access to the system

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

Access is processed through the e9957 process. Local approval from supervisors and designated authorization officials are required prior to granting access to the system.

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

All users of the system are responsible for assuring safeguards for the PII. The system manager is responsible for assigning users to the appropriate user roles to limit access and assuring PII safeguards as documented in the technical documentation and system design documentation.

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*

Patient Name: to properly identify, adjudicated and pay claims
Social Security Number (SSN): to properly identify, adjudicated and pay claims
Member Identification Number: to properly identify, adjudicated and pay claims
Patient Control Number: to ensure attachment records accuracy
Medical Record Identification Number: to properly identify, adjudicated and pay claims
Plan Name: to properly identify, adjudicated and pay claims
Date of Birth (DOB)/Date of Death (DOD): to properly identify, adjudicated and pay claims
Address; Zip Code: to properly identify, adjudicated and pay claims
Email: to properly identify, adjudicated and pay claims
Health Insurance Numbers: to properly identify, adjudicated and pay claims
Coverage Dates: to provide actual dates for adjudication and pay claims
Date of Service (DOS): to provide actual dates for adjudication and pay claims
Place of Service (POS): to provide actual place for adjudication and pay claims
CPY and International Code Designator (ICD) Coded Billing Information: to properly identify, adjudicated and pay claims
Health Information (and other insurance): to properly identify, adjudicated and pay claims
Prescription/NCPDP Codes Information: to properly identify, adjudicated and pay claims
Procedure/Treatment/Diagnosis Codes Number/Coded Billing Information (Claim Index): to properly identify, adjudicated and pay claims
Paid Amounts Information (Check/Remittance Numbers): to properly identify, adjudicated and pay claims
Tax Identification Number (TIN): to properly identify, adjudicated and pay claims
Provider Name, Phone, Billing Address, Physical Address to properly identify, adjudicated and

pay claims
Provider's TIN: to properly identify, adjudicated and pay claims

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.*

Claims records are to be destroy 6 years after all individuals in the record become ineligible for program benefits.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)?

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner. Please work with the system Privacy Officer and VA Records Officer to answer these questions.
This question is related to privacy control DM-2, Data Retention and Disposal.

3.3a Are all records stored within the system of record indicated on an approved disposition authority?

Yes. The item Number 1260.1, Care in the Community, Disposition Authority N1-15-03-1, Item 2

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

Retention schedule as approved by the VHA Record Control Schedule and the National Archives and Records Administration (NARA) GRS 1.1: Financial Management and Reporting Records General Records 1.1, Item 10: Temporary. Destroy 6 years after final payment or cancellation, but longer retention is authorized if required for business use. VHA RCS 10-1: https://www.va.gov/vhapublications/rcs10/rcs10-1.pdfGRS: https://www.archives.gov/records-mgmt/grs.html. The item Number 1260.1, Care in the Community, Disposition Authority N1-15-03-1, Item 2

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.

Paper documents are destroyed to an unreadable state in accordance with the Department of Veterans' Affairs VA Directive 6371, (April 8, 2014), https://www.va.gov/vapubsElectronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with the Department of Veterans' Affairs Handbook 6500.1, Electronic Media Sanitization (November 3, 2008), https://www.va.gov/vapubs. When required, this data is deleted from their file location and then permanently deleted from the deleted items, or Recycle bin. Magnetic media is sent out for destruction per VA Handbook 6500.1. Digital media is shredded or sent out for destruction per VA Handbook 6500.1. Additionally, this system follows Field Security Service (FSS) Bulletin #176 dated April 9, 2014 for Media Sanitization Program, SOPs - FSS - All Documents as well as FSS Standard Operating Procedures (SOP) MP-6 Electronic Media Sanitization

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.

Copies of production data are used for Pre-Production testing. Access to the Pre-Production environment and data is restricted to business personnel and less than five Independent Validation & Verification (IV&V) personnel. Established policies and procedures address this matter and each member has training to ensure they understand the risks while testing with the PII data. Training documentation is kept within the Training office. No connections shall be permitted without having an Enterprise Security External Change Council (ESECC) approval.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

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

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

Follow the format below:

Privacy Risk: If data is maintained within the Payer EDI TAS system for a longer time-period than what is needed or required, then the risk that the information will be compromised, breached, or unintentionally released to unauthorized individuals increases.

Mitigation: The Payer EDI TAS system adheres to information security requirements instituted by the VA OI&T to secure data with PII in a FISMA-Moderate environment. A Backup Plan and Restore Plan are in place. At a minimum, the plan includes the requirement to save data for the backup and recovery of information stored on the AWS infrastructure, and the retention of records as required by VA Handbook 6300.1 (Records Management Procedures) and VA Directive 6300 (Records and Information Management).

Business Associate Agreements-For all contracts which may have exposure or access to VA Personal Health Information (PHI)/Personally Identifiable Information (PII) information, Functional Categories are assigned by the supervisor and verified annually.

Talent Management System (TMS) training is required annually.

- VA 10176: VA Privacy and Information Security Awareness and Rules of Behavior
- VA 10203: Privacy and HIPAA Training

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 data element types such as PII/PHI that are shared/received with the Program Office or IT system***	***Describe the method of transmittal***
Veteran Health Administration Claim Processing & Eligibility (CP&E)	Veteran beneficiary healthcare claim data that includes all PII and related PHI values. Data exchanged supports claim adjudication.	Coverage Dates, Plan Name, Current Procedural Terminology, International Code Designator (ICD), Coded Billing Information (Claim Index), Billed Amounts, Other Health Insurance Information, Insurance FMS Document ID, Paid Amounts, Check or Remittance Numbers, Provider Name, Provider Phone Number, Provider Billing Address, Provider Physical Address, Provider Remit to Address), Tax Identification Number, Diagnosis Codes, Treatment Codes, Prescription Numbers, NCPDP Codes, Date of Service (DOS), Place of Service (POS), Patient Name, Social Security Number (SSN), Date of Birth (DOB), Data of Death (DOD), Address, 2nd Address, Email, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Numbers,	Via secure file transfer Protocol (SFTP) within the VA network

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*
		Health Insurance Numbers (Policy Number).	
Veteran Health Administration Financial Management System (FMS)	Veteran and beneficiary healthcare claim data that includes PII and minimal PHI values. Data exchanged supports claim payments and subsequent reconciliation between claim adjudication and claims paid and not paid.	Coverage Dates, Plan Name, Current Procedural Terminology, International Code Designator (ICD), Coded Billing Information (Claim Index), Billed Amounts, Other Health Insurance Information, Insurance FMS Document ID, Paid Amounts, Check or Remittance Numbers, Provider Name, Provider Phone Number, Provider Billing Address, Provider Physical Address, Provider Remit to Address), Tax Identification Number, Diagnosis Codes, Treatment Codes, Prescription Numbers, NCPDP Codes, Date of Service (DOS), Place of Service (POS), Patient Name, Social Security Number (SSN), Date of Birth (DOB), Data of Death (DOD), Address, 2nd Address, Email, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Numbers, Health Insurance Numbers (Policy Number)	Via secure file transfer Protocol (SFTP) within the VA network
Veteran Health Administration	Veteran and beneficiary healthcare claim	Coverage Dates, Plan Name, Current Procedural Terminology,	Via secure file transfer

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*
Program Integrity Tool (PIT)	data that includes all PII and many PHI values.	International Code Designator (ICD), Coded Billing Information (Claim Index), Billed Amounts, Other Health Insurance Information, Insurance FMS Document ID, Paid Amounts, Check or Remittance Numbers, Provider Name, Provider Phone Number, Provider Billing Address, Provider Physical Address, Provider Remit to Address), Tax Identification Number, Diagnosis Codes, Treatment Codes, Prescription Numbers, NCPDP Codes, Date of Service (DOS), Place of Service (POS), Patient Name, Social Security Number (SSN), Date of Birth (DOB), Data of Death (DOD), Address, 2nd Address, Email, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Numbers, Health Insurance Numbers (Policy Number)	protocol (SFTP) within the VA network

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: There is a risk that information may be shared with unauthorized VA programs or systems.

Mitigation: The OI&T develops, disseminates and periodically reviews and updates access control policies and procedures. OI&T has formally developed an access control policy that addresses purpose, scope, roles, responsibilities, management commitment, and coordination among other VA entities. The policies and procedures are reviewed on an annual basis by responsible parties and updated as needed.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

Data Shared with External Organizations

List External Program Office or IT System information is	***List the purpose of information being shared / received / transmitted***	***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***	***List the method of transmission and the measures in***

shared/received with	*with the specified program office or IT system*		*(can be more than one)*	*place to secure data*
Trizetto Facets Claim(CXM) (Signature Performance	Veteran and beneficiary PII and PHI claim related data. Data exchanged supports professional, institutional, dental and pharmacy claim adjudication.	Coverage Dates, Plan Name, Current Procedural Terminology, International Code Designator (ICD), Coded Billing Information (Claim Index), Billed Amounts, Other Health Insurance Information, Insurance FMS Document ID, Paid Amounts, Check or Remittance Numbers, Provider Name, Provider Phone Number, Provider Billing Address, Provider Physical Address, Provider Remit to Address), Tax Identification Number, Diagnosis Codes, Treatment Codes, Prescription Numbers, NCPDP Codes, Date of Service (DOS), Place of Service (POS), Patient Name, Social Security Number (SSN), Date of Birth (DOB), Data of Death (DOD), Address, 2nd Address, Email, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Numbers, Health Insurance Numbers (Policy Number).	ISA/MOU	Site to Site (S2S) VPN Tunnel Files are exchanged via SFTP
Globalscape (Change Healthcare Operations)	Veteran and beneficiary PII and PHI claim related data. Data exchanged supports initial receipt of healthcare claims from an industry	Coverage Dates, Plan Name, Current Procedural Terminology, International Code Designator (ICD), Coded Billing Information (Claim Index), Billed Amounts, Other Health Insurance Information, Insurance FMS Document ID, Paid Amounts, Check or Remittance Numbers, Provider Name, Provider	ISA/MOU	Site to Site (S2S) VPN Tunnel Files are exchanged via SFTP

	clearing house through final disposition of processed payments to an industry clearing house. Claims include professional, institutional and dental.	Phone Number, Provider Billing Address, Provider Physical Address, Provider Remit to Address), Tax Identification Number, Diagnosis Codes, Treatment Codes, Prescription Numbers, NCPDP Codes, Date of Service (DOS), Place of Service (POS), Patient Name, Social Security Number (SSN), Date of Birth (DOB), Data of Death (DOD), Address, 2nd Address, Email, Member Identification Number, Patient Control Number, Medical Record Identification Number, Medical Record Numbers, Health Insurance Numbers (Policy Number).		
Department of Defense Optum	Veteran and beneficiary PII and PHI claim related data. Data exchanged supports Pharmacy claim initial receipt of pharmacy claims from Optum through final disposition of payments to Optum.	Coverage Dates, Plan Name, Current Procedural Terminology, International Code Designator (ICD), Coded Billing Information (Claim Index), Billed Amounts, Other Health Insurance Information, Insurance FMS Document ID, Paid Amounts, Check or Remittance Numbers, Provider Name, Provider Phone Number, Provider Billing Address, Provider Physical Address, Provider Remit to Address), Tax Identification Number, Diagnosis Codes, Treatment Codes, Prescription Numbers, NCPDP Codes, Date of Service (DOS), Place of Service (POS), Patient Name, Social Security Number (SSN), Date of Birth (DOB), Data of Death (DOD), Address, 2nd Address, Email, Member Identification Number, Patient Control Number, Medical Record	ISA/MOU	Site to Site (S2S) VPN Tunnel Files are exchanged via SFTP

		Identification Number, Medical Record Numbers, Heath Insurance Numbers (Policy Numbers).		

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

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

Follow the format below:

Privacy Risk: There is a risk that PII may be accidently released to unauthorized individuals.

Mitigation: The external agreements are in place ensuring the proper processes are in place to prevent disclosure of PII. The entity must provide the minimum necessary policies and procedures, or a secure alternative to the extent consistent with the VA policies and procedures. Must comply with the HIPAA Privacy rules.

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.

This Privacy Impact Assessment (PIA) also serves as notice of the Payer EDI TAS 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." Disclosure of Social Security numbers of those for whom benefits are claimed is requested under the authority of 38 USC and is voluntary. Social Security numbers will be used in the administration of Veterans' benefits and in the identification of Veterans or persons claiming or receiving VA benefits and their records, and may be used for other purposes where authorized by 38 USC and the Privacy Act of 1974 (5 USC 552a) or where required by other statutes.

1. Beneficiaries are provided notice of privacy practices upon enrollment. A form of this notice is provided in the ChampVA Guide.
2. Privacy notices are provided at the point of service at the medical center where the Veteran and beneficiary receive care, in accordance with VHA Handbook 1605.4, Notice of Privacy Practices.
3. Notice of privacy practices are available on the VA Privacy website. https://www.oprm.va.gov/privacy/systems_of_records.aspx

Each of the above notices includes information on how to report any use of information that is not in accordance with the collection. See Appendix A for the notice of privacy practices provided at all VA medical centers

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

Payer EDI TAS does not collect information from the Veteran/Beneficiary. The sources collecting the information provide this notice.

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 PAYER EDI TAS 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." Disclosure of Social Security numbers of those for whom benefits are claimed is requested under the authority of 38 USC and is voluntary. Social Security numbers will be used in the administration of Veterans' benefits and in the identification of Veterans or persons claiming or receiving VA benefits and their records, and may be used for other purposes where authorized by 38 USC and the Privacy Act of 1974 (5 USC 552a) or where required by other statutes.

1. Beneficiaries are provided notice of privacy practices upon enrollment. A form of this notice is provided in the ChampVA Guide.
2. Privacy notices are provided at the point of service at the medical center where the Veteran and beneficiary receive care, in accordance with VHA Handbook 1605.4, Notice of Privacy Practices.

3. Notice of privacy practices are available on the VA Privacy website. https://www.oprm.va.gov/privacy/systems_of_records.aspxEach of the above notices includes information on how to report any use of information that is not in accordance with the collection. See Appendix A for the notice of privacy practices provided at all VA medical centers.

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.

Payer EDI TAS does not collect information from the Veteran/Beneficiary, and does not provide the individuals the NOPP, this is conducted by the point of service.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

This question is directed at whether an individual may provide consent for specific uses, or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent.

Individuals including the Veterans and Beneficiary do have the right to request restrictions that their information is not used or disclose all or part of their health care. Disclosures and use of information or disclosure restrictions are under the provisions of the 45 CFR and the VA Notices of Privacy Practices that provide the necessary details for requesting or releasing information of their records. Veterans must submit a written request that identifies information they want restricted and the extend of the restriction being requested. Individuals do have the right to refuse to provide information but doing so may result in denial of the claim and/or inappropriate care to be provided. See Appendix A for additional details regarding the consent and practices.

6.4 <u>PRIVACY IMPACT ASSESSMENT: Notice</u>

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:

<u>Principle of Transparency:</u> Has sufficient notice been provided to the individual?

<u>Principle of Use Limitation:</u> 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 Veterans will not know that Payer EDI TAS collects, maintains and disseminates Personally Identifiable Information and Sensitive Personal Information.

Mitigation: Privacy practice notices are provided to the veteran at the time of service. This is in accordance with (IAW) VHA Handbook 1605.04 NOTICE OF PRIVACY PRACTICES. Per the VHA Handbook 1605.04 Notice of Privacy Practices. All Programs that are administered by the Office of Community Care (OCC) are provided these notices at least every 3 years. The Privacy Office retains a copy of the notices and how often they are provided to the beneficiary

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.***

See Appendix A for the notice of privacy practices provided at all VA medical centers, which includes the following: Right to Review and Obtain a Copy of Health Information. You have the right to review and obtain a copy of your health information in our records. You must submit a written request to the facility Privacy Officer at the VHA health care facility that provided or paid for your care. NOTE: Please send a written request, to your VHA health care facility Privacy Officer. The VHA Privacy Office at Central Office in Washington, D.C. does not maintain VHA health records, nor past military service health records. For a copy of your military service health records, please contact the National Personnel Records Center at (314)801-0800. The Web site is Veteran's Service Records

7.1b If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR)?

The system does not collect information from individuals. The Sources collecting the information provide this notice. Individuals have the rights to request access to review their records by submitting the VHA-10-5345 provides the process to Request for and Authorization to Release Medical Records or Health Information.

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

The system does not collect information from individuals. The Sources collecting the information provide this notice. Individuals have the rights to request access to review their records by submitting the VHA-10-5345 provides the process to Request for and Authorization to Release Medical Records or Health Information

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.

See Appendix A for the notice of privacy practices provided at all VA medical centers, which includes the following: Right to Request Amendment of Health Information. You have the right to request an amendment (correction) to your health information in our records if you believe it is incomplete, inaccurate, untimely, or unrelated to your care. You must submit your request in writing, specify the information that you want corrected, and provide a reason to support your request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains your information. If your request for amendment is denied, you will be notified of this decision in writing and provided appeal rights. In response, you may do any of the following:

• File an appeal

• File a "Statement of Disagreement"

• Ask that your initial request for amendment accompany all future disclosures of the disputed health information

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.

See Appendix A for the notice of privacy practices provided at all VA medical centers, which includes the following: Right to Request Receipt of Communications in a Confidential Manner. You have the right to request that we provide your health information to you by alternative means or at an alternative location. We will accommodate reasonable requests, as determined by VA/VHA policy, from you to receive communications containing your health information:

• At a mailing address (e.g., confidential communications address) other than your permanent address

• In person, under certain circumstance

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.

Individuals have a right to contact the VHA call center to gain access to their information. Disclosure of Social Security numbers of those for whom benefits are claimed is requested under the authority of 38 USC and is voluntary. Social Security numbers will be used in the administration of Veterans' benefits and in the identification of Veterans or persons claiming or receiving VA benefits and their records and may be used for other purposes where authorized by 38 USC and the Privacy Act of 1974 (5 USC 552a) or where required by other statutes.

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: Privacy risks are with end users approved for access to specific information misusing such information being the most predominant risk. All systems are susceptible to hackers and a risk exists.

Mitigation: Users are restricted by role-based assignments access to only that data needed to process the claim. Hacking attempts are thwarted through a multifaceted approach of NSOC manned firewalls and gateways, AD account requirements, role-based assignments and login credentials.

Section 8. Technical Access and Security

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

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

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

8.1a Describe the process by which an individual receives access to the system?

Access to the Payer EDI TAS system is limited to authorized users – VA staff who have completed the required training and agreed to rule of behavior will have view only access on a need-to-know basis. All user accounts allow read only access to data. All users must be VA cleared.

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?

No other agencies have access to the system.

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 is requested per VA policies utilizing Electronic Permission Access System (ePAS). Users submit access requests based on need to know and job duties. Supervisor and OI&T approval must be obtained prior to access granted. These requests are submitted for VA employees, contractors and all outside agency requests and are processed through the appropriate approval processes.

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

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

Yes, VA is highly dependent on contract augmentation of its workforce. However, contractors must go through background checks, sign the rules of behavior and have the same restrictions as VA staff. The Office of Community Care (OCC) is responsible for ensuring that all contractors who are working on OCC projects have signed Non-Disclosure Agreements and met any necessary contractual requirements governing access and handling of Veteran data.

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.

VA privacy and security training is mandatory. Personnel who will be accessing information systems must read and acknowledge their receipt and acceptance of the VA Information Security Rules of Behavior (RoB) prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training that all personnel must complete via the VA's TMS. After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training.

Acceptance obtained through electronic acknowledgment is tracked through the TMS system. All VA employees must complete annual Privacy and Security training. This training includes, but is not limited to, the following TMS Courses:

• VA 10176: VA Privacy and Information Security Awareness and Rules of Behavior

• VA 10203: Privacy and HIPAA Training

• VA 3812493: Annual Government Ethics

Role-based Training is based on the role of the user and includes, but is not limited to:

- VA 1016925: Information Assurance for Software Developers IT Software Developers
- VA 3193: Information Security for CIOs Executives, Senior Managers, CIOs and CFOs
- VA 1357084: Information Security Role-Based Training for Data Managers
- VA 64899: Information Security Role-Based Training for IT Project Managers
- VA 3197: Information Security Role-Based Training for IT Specialists
- VA 1357083: Information Security Role-Based Training for Network Administrators
- VA 1357076: Information Security Role-Based Training for System Administrators
- VA 3867207: Information Security Role-Based Training for System Owners

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

8.4a If Yes, provide:

1. *The Security Plan Status: approved.*
2. *The System Security Plan Status Date: 10/12/92021 with additional annual reviews*
3. *The Authorization Status: Authorization to Operate (ATO)*
4. *The Authorization Date: 19-Jan-2022*
5. *The Authorization Termination Date: 19-Jan-2025*
6. *The Risk Review Completion Date: 12/15/2021*
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.***
<<ADD ANSWER HERE>>

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)*

Payer EDI TAS utilizes cloud technology as an Infrastructure as a Service (IaaS) and is hosted within the VA Enterprise Cloud (VAEC), AWS GovCloud, which is a FedRAMP approved environment.

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.*
<<ADD ANSWER HERE>>

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

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.
This question is related to privacy control DI-1, Data Quality.
<<ADD ANSWER HERE>>

9.4 NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?
What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.
<<ADD ANSWER HERE>>

9.5 If the system is utilizing Robotics Process Automation (RPA), please describe the role of the bots.
Robotic Process Automation is the use of software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. For example, will the automation move or touch PII/PHI information. RPA may also be referred to as "Bots" or Artificial Intelligence (AI).
<<ADD ANSWER HERE>>

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

MICHAEL HARTMANN

Digitally signed by MICHAEL HARTMANN
Date: 2024.02.01 11:17:58 -07'00'

Privacy Officer, Michael Hartmann

Information Systems Security Officer, Richard Alomar-Loubriel

Information Systems Owner, Dena Liston

APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy; a Privacy Act notice on forms; screen shot of a website collection privacy notice).

Veterans' Health Administration NOTICE OF PRIVACY PRACTICES Effective Date September 23, 2013 *https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=1090*[

23VA10NB3, Non-VA Care (Fee) Records - VA (7/30/2015): 2015-18646.pdf (govinfo.gov)
24VA10A7, Patient Medical Records - VA (10/2/2020): 2020-21426.pdf (govinfo.gov)
54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files - VA (3/3/2015): 2015-04312.pdf (govinfo.gov)
58VA21, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records - VA (11/8/2021): 2021-24372.pdf (govinfo.gov)
79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records – VA: 2020-28340.pdf (govinfo.gov)
147VA10, Enrollment and Eligibility Records - VA (8/17/2021): 2021-17528.pdf (govinfo.gov)

HELPFUL LINKS:

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

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

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

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

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