Privacy Impact Assessment for the VA IT System called:

Community Care Electronic Data Interchange Gateway (EDI GW)

Veterans Health Administration

Office of Integrated Veteran Care

Date PIA submitted for review:

3/21/2023

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)	Ashton Botts	Ashton.Botts@va.gov	303-398-7155
Information System Owner	Sale Tunoascanlan	Sale.Tuoascanlan@va.gov	913-485-3793

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 (EDI) Gateway (EDIGW) is part of the Community Care Provider Payment Program. It serves as a broker of electronic data transmissions between Office of Community Care systems and other entities including those internal and external to the Department of Veterans Affairs. This system performs a series of extract transfer load (ETL), data transformation, file transfer, and data archiving procedures based on business rules and documented file format standards to ensure data sets, both created and received, are compliant and are serialized in formats digestible by downstream applications.

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.

Community Care Electronic Data Interchange Gateway (EDI GW). Office of Integrated Veteran Care

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

The Electronic Data Interchange (EDI) Gateway (EDIGW) is part of the Community Care Provider Payment Program. It serves as a broker of electronic data transmissions between Office of Community Care systems and other entities including those internal and external to the Department of Veterans Affairs. This system performs a series of extract transfer load (ETL), data transformation, file transfer, and data archiving procedures based on business rules and documented file format standards to ensure data sets, both created and received, are compliant and are serialized in formats digestible by downstream applications.

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.

EDIGW performs compliance checks on incoming and outgoing EDI messages between the contracted Healthcare Clearinghouse and VA-internal processing systems. There are approximately 200 million records of individuals whose information may be stored in the

systems. EDIGW is owned by the Department of Veterans Affairs, and the typical clients include external Providers, Veterans or dependents. External providers must provide their own level of security controls such as access control, and authentication in the protection of Veterans privacy protected information to include Personally Identifiable Information (PII) and Protected Health Information (PHI).

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

It serves as a broker of electronic data transmissions between Office of Community Care systems and other entities including those internal and external to the Department of Veterans Affairs.

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

This system performs a series of extract transfer load (ETL), data transformation, file transfer, and data archiving procedures based on business rules and documented file format standards to ensure data sets, both created and received, are compliant and are serialized in formats digestible by downstream applications.

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.

This system is hosted in Denver HAC Datacenter (Station 741):

3. Legal Authority and SORN

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

The applicable legal authorities can be found in each SORN listing, located at https://www.oprm.va.gov/privacy/systems_of_records.aspx. The legal authorities can be found in the section titled "AUTHORITY FOR MAINTENANCE OF THE SYSTEM". List each legal authority only once as the same legal authorities may be present in different SORNS.

SORNs for this system are as follows:

23VA10NB3, Non-VA Care (Fee) Records – VA (7/30/2015)

24VA10A7, Patient Medical Records – VA (10/2/2020)

43VA008, Veterans, Dependents of Veterans, and VA Beneficiary Survey Records – VA (1/25/2021)

54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files – VA (3/3/2015)

58VA21/22/28, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA (11/8/2021)

147VA10, Enrollment and Eligibility Records – VA (8/17/2021)

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?

No

D. System Changes

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

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

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

The 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.

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)

- Current Procedural Terminology (CPT) and International Code Designator (ICD) Code
- Billing Information
- Billed Amounts
- Other Health Insurance Information
- Other Health Insurance Paid Amounts
- Provider Name
- Provider Phone Number
- Provider Billing Address
- Provider Physical Address
- Provider Remit to Address

PII Mapping of Components (Servers/Database)

EDI GW consists of 1 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 EDI GW 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
CLAIMS Database	Yes	Yes	Name, Social Security Number, Date of Birth, Address, Zip Code, Health Insurance Beneficiary Numbers/Account Numbers, Current Medications, Provider's TIN and	It serves as a broker of electronic data transmissions between Office of Community Care systems and other entities	The data is encrypted in transit. Only authorized users have access to the database. Remote protection is provided by remote

			Address information.	**including those internal and external to the Department of Veterans Affairs.**	**access control, authenticator management, audit. Both contractors and VA employees are required to take Privacy, HIPAA, and information security training annual.**

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

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

The information collected, maintained, and/or disseminated in EDI GW comes from a few areas depending on the type of information. The information may come directly from VDIF, or the CLAIMS Database. VHA Office of Community Care who owns and manages the EDI GW system on the VA side.

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.

Information from sources other than the individual is not required.

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

EDI GW pass along the information to other VA systems internally.

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 information is provided to EDI GW from VDIF (Change Healthcare). It serves as a broker of electronic data transmissions between Office of Community Care systems and other entities including those internal and external to the Department of Veterans Affairs.

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.

EDI GW does not collect information on a form. Information is passed to EDI GW from VDIF Change Healthcare.

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.

Information is not checked for accuracy. It simply serves as a broker of electronic data transmissions between Office of Community Care systems and other entities including those internal and external to the Department of Veterans Affairs.

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.

It simply serves as a broker of electronic data transmissions between Office of Community Care systems and other entities including those internal and external to the Department of Veterans Affairs.

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

SORNs for this system are as follows:
23VA10NB3, Non-VA Care (Fee) Records – VA (7/30/2015)
24VA10A7, Patient Medical Records – VA (10/2/2020)
43VA008, Veterans, Dependents of Veterans, and VA Beneficiary Survey Records – VA (1/25/2021)
54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files – VA (3/3/2015)
58VA21/22/28, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA (11/8/2021)
147VA10, Enrollment and Eligibility Records – VA (8/17/2021)

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: Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious personal, professional, or financial harm may result for the individuals affected.

Mitigation: The Veterans Health Administration (VHA) employ a variety of security measures designed to ensure that the information is not inappropriately disclosed or released. These measures include access control; awareness and training; audit and accountability; certification,

accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. Our facility employs all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in National Institute of Standards and Technology (NIST) Special Publication 800-37 and specific VA directives.

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 the patient during appointments and in other forms of communication
Social Security Number: Used as a patient identifier and as a resource for verifying income information with the Social Security Administration
Date of Birth: Used to identify age and confirm patient identity
Mailing Address: Used for communication, billing purposes and to calculate travel pay
Zip Code: Used for communication, billing purposes, and to calculate travel pay
Phone Number(s): Used for communication, confirmation of appointments and to conduct telehealth appointments
Health Insurance Beneficiary Account Numbers: Used to communicate and bill third party health care plans
Employment information: Used to determine potential employer's insurance eligibility and for veteran contact, financial verification.
Gender: Used as patient demographic, identity and indicator for type of medical care/provider and medical tests required for individual.
Patient ID: Used to help identify the specific patients outside of SSN, and DOB. This ensures we have the correct patient and eliminated cross or duplicated information.

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 GW simply serves as a broker of electronic data transmissions between Office of Community Care systems and other entities including those internal and external to the Department of Veterans Affairs.

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.

EDI GW simply serves as a broker of electronic data transmissions between Office of Community Care systems and other entities including those internal and external to the Department of Veterans Affairs.

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?

The data is encrypted in transit. Only authorized users have access to the database. Remote protection is provided by remote access control, authenticator management, audit.

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

The data is encrypted in transit. Only authorized users have access to the database. Remote protection is provided by remote access control, authenticator management, audit. Both contractors and VA employees are required to take Privacy, HIPAA, and information security training annual.

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

Controls are in place to ensure data is used and protected in accordance with legal requirements, VA policies, and VA's stated purpose for using the data. Controls include mandatory training completion for all employees, volunteers, and contractors. Additionally, audits are performed to ensure information is accessed and retrieved appropriately. VA has implemented required security and privacy controls for Federal information systems and organizations according to NIST SP 800-53 and VA Handbook 6500, Risk Management Framework for VA Information Systems. VA OIT implements data protection assurances on all databases where patient insurance information is stored.

Limited system access is granted by VA OIT to ensure only those with need to know have access to any patient related data. VA OIT periodically audits user accounts and removes access to those who no longer need access or have not used granted access in the previous audit period. All data collected, generated and stored by ICBWeb is the properly of VA and only used in VA controlled space.

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?

EDI GW is placed on its own VLAN and behind ACLs. Access to the EDI GW servers are limited to administrators for maintenance.

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

Yes, there are procedures in place regarding access. EDI GW follows standard VA Policy and procedures when granting access to its system. Controls are in place to ensure data is used and protected in accordance with legal requirements, VA policies, and VA's stated purpose for using the data. Controls include mandatory training completion for all employees, volunteers, and contractors. Additionally, audits are performed to ensure information is accessed and retrieved appropriately. VA has implemented required security and privacy controls for Federal information systems and organizations according to NIST SP 800-53 and VA Handbook 6500, Risk Management Framework for VA Information Systems. VA OIT implements data protection assurances on all databases where patient insurance information is stored. Limited system access is granted by VA OIT to ensure only those with need to know have access to any patient related data. VA OIT periodically audits user accounts and removes access to those who no longer need access or have not used granted access in the previous audit period.

2.4c Does access require manager approval?

Manager approval is required through ePAS requests.

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

Access is monitored through logging

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

VA Administrators within the HAC Denver.

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*

Name, Social Security Number, Date of Birth, Address, Zip Code, Health Insurance Beneficiary Numbers/Account Numbers, Current Medications, Provider's TIN and Address information.

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.*

EDI GW follows VA policy regarding retention of records. For Patient medical records are retained for a total of 75 years after the last episode of care. As directed by the Department Veterans Affairs, Veterans Health Administration Record Control Schedule (RCS) 10-1, • RCS 10-1 link for VHA: http://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

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?

Veterans Health Administration Record Control Schedule (RCS) 10-1,• RCS 10-1 link for VHA: http://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

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

Veterans Health Administration Record Control Schedule (RCS) 10-1,• RCS 10-1 link for VHA: http://www.va.gov/vhapublications/rcs10/rcs10-1.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 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 VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and VA Handbook 6500.1 Electronic Media Sanitization. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destruction. https://www.va.gov/vapubs/search_action.cfm?dType=1

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

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

PII and PHI data is not used for research or testing. EDI GW simply serves as a broker of electronic data transmissions between Office of Community Care systems and other entities including those internal and external to the Department of Veterans Affairs.

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: There is a risk that the information maintained by EDI GW 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, breached, or exploited for reasons other than what is described in the privacy documentation associated with the information.

Mitigation: To mitigate the risk posed by information retention, EDI GW adheres to the VA RCS schedules for each category or data it maintains. When the retention data is reached for a record, the medical center will carefully dispose of the data by the determined method as described in question 3.4. The EDI GW ensures that al personnel involved with the collection, use and retention of data are trained in the current process for collecting, using, and retaining this data. A Records Management Officer (RMO), Privacy Officer (PO), and an Information System Security Officer (ISSO) are assigned to the boundary to ensure their respective programs are understood and followed by all to protect sensitive information from the time it is captured by the VA until it is finally disposed of. Each of these in-depth programs have controls that overlap and are assessed annually to ensure requirements are being met and assist staff with questions concerning proper handling of information.

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***
Veterans Health Administration - Claims Database	Veteran healthcare claim data that includes all PII and all related PHI values which support claim adjudication	Name, Social Security Number, Date of Birth, Address, Zip Code, Health Insurance Beneficiary Numbers/Account Numbers, Current Medications, Provider's TIN and Address information.	Java Database Connectivity (JDBC), System in internal to the VA. Only approved employees and contractors have access to the system.

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*
Office of Veteran Integrated Care - MOVEit	Pass through vehicle. Transfers transactions from clearinghouse for 275 transactions include all types of PII and PHI	Name, Social Security Number (SSN), Date of Birth (DOB), Address, Phone Numbers, Email Addresses, Health Insurance Beneficiary Numbers, Account Numbers, Current Medications, Previous Medical Records.	Via Secure File Transfer Protocol (SFTP), System in internal to the VA. Only approved employees and contractors have access to the system.
Veterans Health Administration - Fee Payment Processing System (FPPS)	Veteran healthcare claim data that includes all PII and all related PHI values which support claim adjudication	Name, Social Security Number, Date of Birth, Address, Zip Code, Health Insurance Beneficiary Numbers/Account Numbers, Current Medications, Provider's TIN and Address information.	JDBC, System in internal to the VA. Only approved employees and contractors have access to the system.
Veterans Health Administration - Attachment Retrieval System EDI Web Viewer (EWV)	Veteran healthcare claim data that includes all PII and all related PHI values which support claim adjudication	Name, Social Security Number, Date of Birth, Address, Zip Code, Health Insurance Beneficiary Numbers/Account Numbers, Current Medications, Provider's TIN and Address information	JDBC, System in internal to the VA. Only approved employees and contractors have access to the system.

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 internal sharing of data is necessary individuals to receive benefits at the EDI GW. However, there is a risk that the data could be shared with an inappropriate VA organization or institution which could result in a breach of privacy and disclosure of PII/PHI to unintended parties or recipients.

Mitigation: Safeguards implemented to ensure data is not sent to the wrong VA organization are employee security and privacy training and awareness are required reporting of suspicious activity. Use of secure passwords, access for need-to-know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized within the facilities. Access to sensitive information and the systems where the information is stored is controlled by the VA using a "least privilege/need to know" policy. Access must be requested and only the access required by VA persons or processes acting on behalf of VA persons is to be requested or granted.

Section 5. External Sharing/Receiving and Disclosure

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

5.1 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 shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
N/A	N/A	N/A	N/A	N/A

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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: N/A

Mitigation: N/A

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 GW does not collect information from the individual. Data is provided to EDI GW from VDIF Change Healthcare

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

EDI GW does not collect information from the individual. Data is provided to EDI GW from VDIF Change Healthcare

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.

EDI GW does not collect information from the individual. Data is provided to EDI GW from VDIF Change Healthcare

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.

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. Yes, see appendix A.

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

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

Veterans 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 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 veterans and other members of the public will not know that the EDI GW exists or that it collects, maintains, and/or disseminates PII, PHI, or PII/PHI about them.

Mitigation: This risk is mitigated by the common practice of providing the Notice of Privacy Practice (NOPP) when Veterans are enrolled for healthcare. Employees and contractors are required to review, sign, and abide by the National Rules of Behavior on a yearly basis as required by VA Handbook 6500 as well as complete the annual mandatory Information Security and Privacy Awareness training. Additional mitigation is provided by making the System of Record Notices (SOR) and Privacy Impact Assessment (PIA) available to review online, as discussed in question 6.1 and the Overview section of this PIA.

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.***

An individual wanting notification or access, including contesting the record, should mail or deliver a request to the office identified in the SOR. If an individual does not know the "office concerned," the request may be addressed to the PO of any VA field station VHA facility where the person is receiving care or the Department of Veterans Affairs Central Office, 810 Vermont Avenue, NW, Washington, DC 20420. The receiving office must promptly forward the mail request received to the office of jurisdiction clearly identifying it as "Privacy Act Request" and notify the requester of the referral.

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 answer from 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 answer from 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.

Individuals are required to provide a written request to amend or correct their records to the appropriate Privacy Officer or System Manager as outlined in the Privacy Act SOR. Every Privacy Act SOR contains information on Contesting Record Procedure which informs the individual who to contact for readdress. Further information regarding access and correction procedures can be found in the notices listed in Appendix A.

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

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

Veterans are informed of the amendment process by many resources to include the VHA Notice of Privacy Practice (NOPP) which states, 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 wanted corrected, and provide a reason to support your request amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA healthcare facility that maintains your information. If your request for amendment is denied, you will be notified of this decision in writing and provided appeals rights. In response, you may do any of the following: file an appeal, file a "Statement of Disagreement", and ask that your initial request for amendment accompany all future disclosures of the disputed health information. Individuals seeking information regarding access to and contesting of VA benefits records may write, call, or visit the nearest VA regional office. Additional notice is provided through the SORS listed in 6.1 of this PIA and through the Release of Information Office where care is received.

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

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

Mitigation: EDI GW mitigates the risk of incorrect information in an individual's records by authenticating information when possible, using the resources discussed in question 1.5. Additionally, staff verifies information in medical records and corrects information identified as incorrect during each patient's medical appointments.

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.

Individuals receive access to the EDI GW by gainful employment in the VA or upon being awarded a contract that requires access to the boundary systems. Upon employment, the Office of Information & Technology (OI&T) creates computer and network access accounts as determined by employment positions assigned. Access is requested utilizing the Electronic Permission Access Boundary (ePAS). Users submit access requests based on need to know and job duties. Supervisor, ISSO, 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.

8.1b 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?

Users from other agencies do not have access to EDI GW.

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.

Admin Access is granted to EDI GW system to maintain the system. There are no changes to the actual data that is being processed or stored by the system.

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.

Contractors will have access to the Boundary after completing the VA Privacy and Information Security Awareness training and Rules of Behavior annually, and after the initiation of a background investigation. Contractors are only allowed access for the duration of the contract this is reviewed by the privacy officer and the designated Contracting Officer Representative (COR). Per the National Contractor Access Program (NCAP) guidelines, contractors can have access to the Boundary only after completing mandatory information security and privacy training, Privacy and HIPAA Focused Training as well as having completed a Special Agency Check, finger printing and having the appropriate background investigation scheduled with Office of Personnel Management. Certification that training has been completed by all contractors must be provided to the employee who is responsible for the contract in question. In addition, all contracts by which contractors might access sensitive patient information must be include a Business Associated Agreement which clarifies the mandatory nature of the training and the potential penalties for violating patient privacy. Contracts with VA EDI GW access must have an approved computer access request on file. The area manager, or designee, in conjunction with the ISSO and the applicable COR reviews accounts for compliance with account management requirements. User accounts are reviewed periodically in accordance with National schedules.

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.

All EDI GW personnel and contractors are required to complete the initial and annual Privacy and Security Awareness and Rules of Behavior (RoB) training, during New Employee Orientation (NEO) or via TMS. In addition, all employees who interact with patient sensitive medical information must complete the Privacy and HIPAA focused mandated privacy training. Finally, all new employees receive face-to-face training by the Boundary Privacy Officer and Information Security Officer during new employee orientation. The Privacy and Information Security Officers also perform subject specific trainings on an as needed basis.

8.4 Has Authorization and Accreditation (A&A) been completed for the system? No

8.4a If Yes, provide:

1. *The Security Plan Status:* Please provide response here
2. *The System Security Plan Status Date:* Please provide response here
3. *The Authorization Status:* Please provide response here
4. *The Authorization Date:* Please provide response here
5. *The Authorization Termination Date:* Please provide response here
6. *The Risk Review Completion Date:* Please provide response here
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Please provide response here

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.***

Currently In Process. 3/15/2023

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.*

N/A

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.

N/A

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).

N/A

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

ID	Privacy Controls
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 D Hartmann 1612370

Digitally signed by Michael D Hartmann 1612370
Date: 2023.04.03 08:52:27 -06'00'

Privacy Officer, Michael Hartmann

ASHTON BOTTS

Digitally signed by ASHTON BOTTS
Date: 2023.04.06 13:49:38 -06'00'

Information Systems Security Officer, Ashton Botts

SALE TUNOASCANLAN

Digitally signed by SALE TUNOASCANLAN
Date: 2023.04.06 15:11:15 -04'00'

Information System Owner, Sale Tunoascanlan

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).

- Department of Veterans Affairs Veterans Health Administration NOTICE OF PRIVACY PRACTICES
- 23VA10NB3, Non-VA Care (Fee) Records – VA (7/30/2015)
- 24VA10A7, Patient Medical Records – VA (10/2/2020)
- 43VA008, Veterans, Dependents of Veterans, and VA Beneficiary Survey Records – VA (1/25/2021)
- 54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files – VA (3/3/2015)
- 58VA21/22/28, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA (11/8/2021)
- 147VA10, Enrollment and Eligibility Records – VA (8/17/2021)

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