Privacy Impact Assessment for the VA IT System called:

VA Recovery Audit Contract System

Veterans Health Administration

Office of Finance

eMASS ID 1253

Date PIA submitted for review:

June 3, 2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Yolanda Thornton	yolanda.thornton@va.gov	202-461-0328
Information System Security Officer (ISSO)	Joseph “JJ” Jarvis	joseph.jarvis@va.gov	469-494-2287
Information System Owner	Akeel Omari	Akeel.omari@va.gov	404-828-5507

Abstract

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

The VA Recovery Audit Contractor (VARAC) system. The Veterans Health Administration (VHA) Office of Finance (OF) is required by law to conduct a series of recovery audits to identify potential overpayments to providers. VHA OF will use VA personnel from supporting offices to pull VA Data containing Sensitive Information (SI) meeting specific parameters established by VHA OF's Payment Operations directorate. When data has been pulled, it will be sent to the VA Recovery Audit Contractor (RAC) system using the secure MOVEit Secure File Transfer Protocol SFTP connection. When Cotiviti GOV Services has received the securely transmitted data in the VA RAC system, they will use their proprietary system data system and auditor personnel to identify overpayments to providers and securely convey this information to VA for collections activities. Reports to other VHA OF personnel may be used for identifying claims processing issues that may need to be addressed. Pushing data to the VA RAC system from the VHA OF Network Storage Device (NSD) and pulling data back from the VA RAC to the VHA OF NSD are ONLY initiated by VA. Cotiviti GOV Services has no MOVEit functionality.

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?

The VA Recovery Audit System (the acronym in eMASS is VA RAC), is a managed service that will be utilized under a contract with VHA Office of Finance – Payment Operations to support the Recovery Audit Program.

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 Recovery Audit Program operates under Public Law 111–204, Improper Payments Elimination and Recovery Act of 2010 (IPERA).

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

Through this contract, Cotiviti GOV Services, a RAC from the Las Vegas, Nevada and Irving, Texas locations manages the service.

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?

Cotiviti GOV Services will review the paid claim data of an estimated 3 million VA Beneficiaries per year.

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

Cotiviti GOV Services processes and stores VA data during execution of the contract.

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

The VA RAC system has been determined to be an Infrastructure-as-a-Service (IaaS). The VA RAC system will use the case management tool, ReSults™ application to support and document all aspects of the audit and recovery process using only the data shared by VHA.

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 VA RAC system is a contractor owned system that will reside in the Microsoft Azure Commercial cloud platform, a commercial cloud environment that will be physically located in Microsoft's South Central and North Central locations.

3. Legal Authority and SORN

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

The Recovery Audit Program operates under Public Law 111–204, Improper Payments Elimination and Recovery Act of 2010 (IPERA).
SORNs:
23VA10NB3 Non-VA Care (Fee) Records-VA (7-30-2015)
24VA10A7/ 85 FR 62406, Patient Medical Records-VA (8-30- 2020)
54VA10NB3; Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files-VA (3-3-2015)
79VA10/85 FR 84114, Veterans Health Information Systems and Technology Architecture (VistA)-VA (12-23-2020)

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?

The System of Record Notice will not require amendment or revision. Cotiviti GOV Services processes and stores VA data during execution of the contract. The VA contract requires the contractor to ensure compliance with all Performance Work Statement and VA system requirements, including Information Technology (IT) systems security policies, procedures, and practices.

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

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

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

Section 1. Characterization of the Information

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

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

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

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

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

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

- ☒ Name
- ☒ Social Security Number
- ☒ Date of Birth
- ☐ Mother's Maiden Name
- ☒ Personal Mailing Address
- ☒ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☐ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☐ Financial Information
- ☒ Health Insurance Beneficiary Numbers Account numbers

☐ Certificate/License numbers[1]
☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☒ 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: Date of Death, Eligibility, Diagnosis Codes, Procedure Codes, Date of Service, Place of Service, Claim Amounts.

PII Mapping of Components (Servers/Database)

VA RAC consists of five key components (servers/databases/instances/applications/software/application programming interfaces (API). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by VA RAC 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

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
Recoup	Yes	Yes	Name, Social Security # (SSN), Date of Birth, Personal Mailing Address, Personal Phone Number, Current Medication,	The Data Elements are used for identifying potential overpayments to providers so those overpayments may be recouped.	Maintenance of the Authority to Operate (ATO), compliance with Federal Information Security Management Act (FISMA) requirements, Least

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

			Tax Identification Number (TIN), Medical Record Number (MRN), Gender, Integration Control Number, Date of Death, Eligibility, Diagnosis Codes, Procedure Codes, Date of Service, Place of Service, Claim Amounts, Health Insurance Beneficiary Numbers and Account Numbers		Privileges applied in Active Directory, Encryption at rest within the storage, Dynamic Data Masking and all the controls outlined in the System Security Plan (SSP).
varac_all	Yes	Yes	Name, Social Security # (SSN), Date of Birth, Personal Mailing Address, Personal Phone Number, Current Medication, Tax Identification Number (TIN), Medical Record Number (MRN), Gender, Integration Control Number, Date of Death,	The Data Elements are used for identifying potential overpayments to providers so those overpayments may be recouped.	Maintenance of the Authority to Operate (ATO), compliance with Federal Information Security Management Act (FISMA) requirements, Least Privileges applied in Active Directory, Encryption at rest within the storage, Dynamic Data

			Eligibility, Diagnosis Codes, Procedure Codes, Date of Service, Place of Service, Claim Amounts, Health Insurance Beneficiary Numbers and Account Numbers		Masking and all the controls outlined in the System Security Plan (SSP).
varac_master	Yes	Yes	Name, Social Security # (SSN), Date of Birth, Personal Mailing Address, Personal Phone Number, Current Medication, Tax Identification Number (TIN), Medical Record Number (MRN), Gender, Integration Control Number, Date of Death, Eligibility, Diagnosis Codes, Procedure Codes, Date of Service, Place of Service, Claim Amounts,	The Data Elements are used for identifying potential overpayments to providers so those overpayments may be recouped.	Maintenance of the Authority to Operate (ATO), compliance with Federal Information Security Management Act (FISMA) requirements, Least Privileges applied in Active Directory, Encryption at rest within the storage, Dynamic Data Masking and all the controls outlined in the System Security Plan (SSP).

			Health Insurance Beneficiary Numbers and Account Numbers		
Folder on shared drive in VA network: Z:\HMS RAC (\\vhahachsm200.vha.med.va.gov\ HAC_Services$\ BIC_10D1E1) Z\HMS RAC:	Yes	Yes	Name, Social Security # (SSN), Date of Birth, Personal Mailing Address, Personal Phone Number, Current Medication, Tax Identification Number (TIN), Medical Record Number (MRN), Gender, Integration Control Number, Date of Death, Eligibility, Diagnosis Codes, Procedure Codes, Date of Service, Place of Service, Claim Amounts, Health Insurance Beneficiary Numbers and Account Numbers	The Data Elements are used for identifying potential overpayments to providers so those overpayments may be recouped.	Maintenance of the Authority to Operate (ATO), compliance with Federal Information Security Management Act (FISMA) requirements, Least Privileges applied in Active Directory, Encryption at rest within the storage, Dynamic Data Masking and all the controls outlined in the System Security Plan (SSP).
• VA Corporate Data Warehouse (CDW) – Server: CDWA06 – Database: VHA_HOC_Tier2.dflt	Yes	Yes	Name, Social Security # (SSN), Date of Birth,	The Data Elements are used for identifying potential	Maintenance of the Authority to Operate (ATO),

			Personal Mailing Address, Personal Phone Number, Current Medication, Tax Identification Number (TIN), Medical Record Number (MRN), Gender, Integration Control Number, Date of Death, Eligibility, Diagnosis Codes, Procedure Codes, Date of Service, Place of Service, Claim Amounts, Health Insurance Beneficiary Numbers and Account Numbers	overpayments to providers so those overpayments may be recouped.	compliance with Federal Information Security Management Act (FISMA) requirements, Least Privileges applied in Active Directory, Encryption at rest within the storage, Dynamic Data Masking and all the controls outlined in the System Security Plan (SSP).

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?

VA Paid Claim data is maintained in VA systems and is extracted and is provided to the contractor. VHA Finance – Payment Operations develops the criteria for defining the data needed for the RAC. Data Analysts in the Informatics and Data Analytics (IDA) office use these criteria to gather copies of the data for use by the contractor.

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.

It would be extremely difficult, complicated and expensive to attempt to collect the paid claim data from the estimated 3 million individuals represented by the data. Additionally, the data Cotiviti GOV Services requires for an audit may not exist with those individuals.

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

The purpose of the Recovery Audit contract is to have Cotiviti GOV Services perform an audit on paid claim data to identify potential overpayments to providers. That paid claim data resides in several national VA systems. Copies of this claim data will be generated by IDA by drawing from these VA systems:

- VA Corporate Data Warehouse (CDW) and,
- Claims Processing and Eligibility (CP&E) and,
- The CDW Program Integrity Tool (PIT).

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 paid claim data/information for the Recovery Audit contractor is extracted from these VA systems:

- VA Corporate Data Warehouse (CDW),
- Claims Processing and Eligibility (CP&E) and,
- The CDW Program Integrity Tool (PIT)

VA Informatics and Data Analytics (IDA) analysts will use SQL or Software as a Service (SaaS) Enterprise guide to pull data from the sources above and in accordance with criteria established by VHA Finance. The results of those queries will create individual files saved to Excel spreadsheets located within the VA network on the HMS RAC shared drive and in the IDA Data Drop folder.

On an Ad Hoc basis, VA will use MOVEit, a program using a Standard File Transfer Protocol (SFTP) connection to transmit the Fiscal Year (FY) data from the IDA Data Drop folder in the VA network to a location in the Cotiviti GOV Services network. Cotiviti GOV Services will then retrieve that data into their case management tool for processing.

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?

There are no forms used in this process.

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.

Medical records as well as provider and claim information is provided to Cotiviti GOV Services by the VA and is assumed to accurately reflect patient, provider, medical treatment, and payment information. The information will be checked at the source end prior to sending to Cotiviti GOV Services.

Upon transfer of the VA data to Cotiviti GOV Services, Cotiviti GOV Services has put in place a mechanism that whenever a threshold of unacceptable data in the source is reached during transmission from the source, it gets rejected, which will then prompt the VA to resend corrected data.

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?

The Cotiviti GOV Services process includes a combination of reviews from seasoned auditors and near real-time monitoring from some internal security tools such as QRadar and McAfee. These tools monitor and ensure data remains intact and a secure FIPS 140-2 approved tool will be used to preserve data integrity while in transit.

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

The Cotiviti GOV Services Recovery Audit Contractor is charged with identifying overpayments and providing information to VA for recoupment of those overpayments under a contractual obligation with the Veterans Health Administration in addition to applicable laws such as:

- Public Law 116-117, Payment Integrity Information Act of 2019 (PIIA),
- 28 CFR 16.53 for use and collection of social security numbers.
- Claims payments fall under the system of records notices:
  - 23VA10NB3, Non-VA Care (Fee) Records - VA (7/30/2015)
  - 24VA10A7, Patient Medical Records - VA (10/2/2020),
  - 54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files - VA (3/3/2015)
  - 79VA10, Veterans Health Information Systems and Technology Architecture (VistA) - VA (12/23/2020)

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: If VA shares inaccurate data with Cotiviti GOV Services, there is a risk of VA sending inaccurate collection notices to providers.

Mitigation: Medical records as well as provider and claim information provided to Cotiviti GOV Services by the VA are assumed to accurately reflect patient, provider, medical treatment and payment information. On the Cotiviti GOV Services side, Cotiviti GOV Services developers create a Data Manipulation Language (DML) script that will be reviewed and executed to correct data inaccuracies. If errors are detected from the source data, these are communicated to VA for retransmission of accurate data.

Section 2. Uses of the Information

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

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

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

PII/PHI Data Element	Internal Use	External Use
Name	To identify the Veteran	To identify the Veteran
SSN	To identify the Veteran	To identify the Veteran
Date of Birth	To determine the Veteran's age, to inform community care providers, and to support medical treatment and decision-making	To determine the Veteran's age, to inform community care providers, and to support medical treatment and decision-making
Personal Mailing Address	For communication	For communication
Personal Phone Number	For communication	For communication
Current Medication	To inform community care providers and to support medical treatment and decision-making	To inform community care providers and to support medical treatment and decision-making
Tax Identification Number (TIN)	To identify the Veteran	To identify the Veteran
Medical Record Number (MRN)	To identify the Veteran	To identify the Veteran
Gender	To identify the Veteran	To identify the Veteran
Integration Control Number	To identify the Veteran	To identify the Veteran
Date of Death	Eligibility dates of service	Eligibility dates of service
Eligibility	Payment eligibility	Payment eligibility
Diagnosis Codes	To inform community care providers and to support medical treatment and decision-making	To inform community care providers and to support medical treatment and decision-making
Procedure Codes	To inform community care providers and to support medical treatment and decision-making	To inform community care providers and to support medical treatment and decision-making

Date of Service **Place of Service** **Claim Amounts** **Health Insurance Beneficiary Numbers and Account Numbers**	Verify medical services Verify medical services Eligibility payment Payment eligibility	Verify medical services Verify medical services Eligibility payment Payment eligibility

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 VA RAC system will generate Weekly Batch Transmission (WBT) reports that will be made available to VA weekly. These reports will be used by VA to prepare documentation for collecting overpayments. While the reports do have claim information, they are geared towards collecting overpayments from providers more than anything to do specifically with Veterans or Beneficiaries. Veterans or Beneficiaries are never involved in the actions performed under this contract. By manipulating the original data VA provides Cotiviti GOV Services and by using their assessments of that data, Cotiviti GOV Services creates the WBT reports and provides them to VA for initiating collection actions. The reports are claim specific and they never involve either Veterans or Beneficiaries.

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.

Cotiviti GOV Services will use a proven, effective, comprehensive case management tool, ReSults™, to support and document all aspects of Cotiviti GOV Services audit and recovery process using only data shared by VHA. The automated, detailed process flows support timely medical record review monitoring and reporting. The tool has built-in, continual time checks to help us meet established time requirements to ensure that the claims review process is completed within the designated timelines to fulfill our contractual Service Level Agreements. The tool

makes use of letters and reports templates to generate reports that will be submitted to VA for review and approval prior to implementation.

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?

VA RAC is hosted in a FedRAMP High certified cloud platform with comprehensive technical and administrative security policies that account for all necessary safeguards to protect VA data from external and internal threats. The system maintains Federal Information Processing Standards (FIPS) 140-2 compliant encryption for data both in transit and at rest and industry best security solutions are used to protect and monitor data throughout its lifecycle within the authorized system boundary.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs?
In addition to the technical and logical security controls in place to protect all sensitive data in the VA RAC, Social Security Numbers are protected using obfuscation when not bring used in the production environment.

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

The Company performs a regular review of policies and processes to prevent the intentional or unintentional misuse or unauthorized access and removal of personally identifiable information. Adequate safeguards are in place and any deviances are identified and tracked to remediation through use of Plans of Actions and Milestones (POA&Ms) within the VA Enterprise Mission Assurance Support Service (eMASS) system.

2.4 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u>

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:

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

<u>Principle of Use Limitation:</u> 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?

The Risk Determination for non-IT personnel on this contract is Tier 1 (Low) and the risk designation for IT personnel is higher at a Tier 2 (Moderate). All contractor personnel must have at least a Tier 1 Background Investigation (BI) which includes requirements to take both:

1. The Privacy and HIPAA training, and
2. The VA Privacy and Information Security Awareness and Rules of Behavior training

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

Once personnel have received their training and if they will be accessing the VA RAC system, they must request access in accordance with the Cotiviti GOV Services developed and VA approved Access Tracking Plan (ATP). The ATP is a contract requirement, and it establishes how Cotiviti GOV Services will:

- Manage Access Rights
- Monitor and track Background Investigation and Systems Access
- Monitor and track all accesses granted to an Cotiviti GOV Services employee working on this contract.

2.4c Does access require manager approval?

To access the VA RAC system and data, Cotiviti GOV Services will require that personnel go through an approval process. Managers will determine the access requirement for their employees and submit the request internally via Cotiviti's Identity Management (IDM) to the Cotiviti GOV Services RAC Program Director. The Cotiviti GOV Services RAC Program Director will then work with the VA COR to validate the approval. Requests will be assessed based on their roles, the support they will provide to the program and the result of their background investigations.

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

Monitoring and logging will be available and enabled in VA RAC to track access to the different resources and the data as well as ensure that events are being saved and reviewed. Also, the ATP establishes the framework for tracking contractor access to Sensitive Personal Information (SPI).

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

Anyone who will view PII will have taken the required training, therefore everyone is responsible for their own actions. However, if Cotiviti GOV Services or VA were to discover an issue, we would expect the contract Program Manager to become involved and resolve the issue. The contract Program Manager must approve all access requests based on their need. The COR will also assess the need for access prior to processing requests for access to VA systems.

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 # (SSN),
- Date of Birth,
- Personal Mailing Address,
- Personal Phone Number,
- Current Medication,
- Tax Identification Number (TIN),
- Medical Record Number (MRN),
- Gender,
- Integration Control Number,
- Date of Death,
- Eligibility,
- Diagnosis Codes,
- Procedure Codes,
- Date of Service,
- Place of Service,
- Claim Amounts,
- Health Insurance Beneficiary Numbers and Account Numbers

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.*

VA only provides Cotiviti GOV Services with a **copy** of the paid claim data for them to audit. Cotiviti GOV Services retains this copy of the data in accordance with contract requirements. Cotiviti GOV Services will only destroy data per VA written guidance and approval and in accordance National Archives and Records Administration (NARA) requirements as outlined in

VA Directive 6300, Records and Information Management and its Handbook 6300.1 Records Management Procedures, applicable VHA Records Control Schedule 10-1, and VA Handbook 6500.1, Electronic Media Sanitization or the Cotiviti GOV Services Retention Schedule if specific requirements are absent.

Records are maintained in accordance with the VHA Records Control Schedule 10-1 under:

4000.1.b – Financial Transaction Records Related to Procuring Goods and Services, Paying Bills, Collecting Debts, and Accounting.

Collecting debts includes the collection of income from all sources (excluding taxation). Collection records document the collection of monies from all sources excluding administrative claims, taxation – not covered under the General Records Schedule (GRS), and Congressional appropriation, such as:

Records documenting administration, receipt, and deposit of user fees for entry into and/or use of public facilities; for recovering costs of providing government services; and receipt of donations, bequests, and other collections from the public, including:

- cash register transaction records
- credit card and charge cards receipts
- records documenting deposits
- records documenting allocation of fees to funds/accounts
- deposit lists and logs
- customer orders
- revolving fund records
- fee and fine collection records
- garnishments
- sale of excess and surplus personal property
- fee or rate schedules and supporting documentation

Prior to termination or completion of this contract, Cotiviti GOV Services must receive written approval from the VA before any VA provided information is destroyed. Any data destruction done on behalf of the VA must be done in accordance with National Archives and Records Administration (NARA) requirements as outlined in VA Directive 6300, Records and Information Management and its Handbook 6300.1 Records Management Procedures, applicable VA Records Control Schedules, and VA Handbook 6500.1, Electronic Media Sanitization.

All documents are destroyed/deleted when system is no longer operational. Electronic images are preserved until the end of the contract, and then destroyed after obtaining VA approval and according to the approved VA records disposition schedule.

Temporary; destroy when business use ceases (GRS 1.1 item 011) (DAA-GRS-2013-0003-0002) Information is retained as long as the contract is active.

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?

VHA Finance provides Cotiviti GOV Services with a copy of VA paid claim data housed within VA. Cotiviti GOV Services will process and store VA data in accordance with VA contract requirements as described in the Statement of Work and based on VA directives (VA Directive 6300, Records and Information Management and its Handbook 6300.1 Records Management Procedures Applicable VA Records Control Schedules, and VA Handbook 6500.1, Electronic Media Sanitization).

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

VHA Record Control Schedule 10-1: https://vaww.va.gov/vhapublications/rcs10/rcs10-1.pdf

VHA Record Control Schedule 10-1, Section 4000.1.b – Financial Transaction Records Related to Procuring Goods and Services, Paying Bills, Collecting Debts, and Accounting.

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)** https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=1254&FType=2**.** 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.

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.

No PHI or PII is being used for Testing, Training or Research.

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 of the data being breached the longer that data is retained.

Mitigation:
For records retention, Cotiviti GOV Services will comply with VA's Records Control Schedule 10-1 dated November 2017, **SORN 4000.1b-Financial transaction records related to procuring goods and services, paying bills, collecting debts, and accounting.**

VA will always retain the original data. In the event of data corruption, VA data may be used for rebuilding data within the VA RAC system. Cotiviti GOV Services will only be receiving copies of the data therefore retention times are:

- Temporary; destroy when business use ceases (GRS 1.1 item 011) (DAA-GRS-2013-0003-0002)

For destruction of data: The COR will ensure all data is processed in accordance with the contract and VA directives. Specifically, VA Directive 6300, Records and Information Management and its Handbook 6300.1 Records Management Procedures, applicable VHA Records Control Schedule 10-1, and VA Handbook 6500.1, Electronic Media Sanitization.

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***
Veteran Health Administration (VHA), Claims Processing and Eligibility (CP&E)	Claim payment information is pulled from the CP&E system and shared with the contractor for auditing the data for overpayments and for recoupment.	Name, Social Security # (SSN), Date of Birth, Personal Mailing Address, Personal Phone Number, Current Medication, Tax Identification Number (TIN), Medical Record Number (MRN), Gender, Integration Control Number,	Secure File Transfer Protocol

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*
		Date of Death, Eligibility, Diagnosis Codes, Procedure Codes, Date of Service, Place of Service, Claim Amounts, Health Insurance Beneficiary Numbers and Account Numbers	
Veteran Health Administration (VHA), Corporate Data Warehouse (CDW)	Claim payment information is pulled from the CDW system and shared with the contractor for auditing for overpayments and for recoupment.	Name, Social Security # (SSN), Date of Birth, Personal Mailing Address, Personal Phone Number, Current Medication, Tax Identification Number (TIN), Medical Record Number (MRN), Gender, Integration Control Number, Date of Death, Eligibility, Diagnosis Codes, Procedure Codes, Date of Service, Place of Service, Claim Amounts, Health Insurance Beneficiary Numbers and Account Numbers	Secure File Transfer Protocol
Veteran Health Administration (VHA), Program Integrity Tool (PIT)	Claim payment information is pulled from the PIT system and shared with the contractor for auditing for overpayments and for recoupment.	Name, Social Security # (SSN), Date of Birth, Personal Mailing Address, Personal Phone Number, Current Medication, Tax Identification Number (TIN), Medical Record Number (MRN),	Secure File Transfer Protocol

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*
		Gender, Integration Control Number, Date of Death, Eligibility, Diagnosis Codes, Procedure Codes, Date of Service, Place of Service, Claim Amounts, Health Insurance Beneficiary Numbers and Account Numbers	
Veteran Affairs Financial Service Center (FSC), Debt Management Center (DMC)	Claim payment information is pulled from the WBT and DMC manipulates that data for recoupment. This information is shared with the contractor for auditing for overpayments and for recoupment.	Name, Social Security # (SSN), Date of Birth, Personal Mailing Address, Personal Phone Number, Current Medication, Tax Identification Number (TIN), Medical Record Number (MRN), Gender, Integration Control Number, Date of Death, Eligibility, Diagnosis Codes, Procedure Codes, Date of Service, Place of Service, Claim Amounts, Health Insurance Beneficiary Numbers and Account Numbers	Secure File Transfer Protocol

4.2 <u>PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure</u>

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:
Data shared internally is comprised of data that can be inappropriately accessed.

Mitigation:
Cotiviti GOV Services will use Microsoft Azure, a FedRAMP High certified cloud platform, to host the VA RAC system which will have all the necessary safeguards to protect VA data from external and internal threats. The Cotiviti GOV Services ReSults application will also obtain its FISMA authorization applying required security controls based on NIST 800-53 to ensure the same level of protection is afforded to the data even if it's residing outside the VA network. In the event of data disclosure/breach, Cotiviti GOV Services will conduct an incident response and report the incident and mitigations to appropriate Cotiviti GOV Services key personnel, the VA COR, the VA ISSO and VHA Privacy Office as outlined in the Business Associates Agreement (BAA).

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***
In-Sync: Subcontractor to Cotiviti GOV Services	VA data is used to audit claims in support of the Recovery Audit Contract	Name, Social Security # (SSN), Date of Birth, Personal Mailing Address, Personal Phone Number, Current Medication, Tax Identification Number (TIN), Medical Record Number (MRN), Gender, Integration Control Number, Date of Death, Eligibility, Diagnosis Codes, Procedure Codes, Date of Service, Place of Service, Claim Amounts, Health Insurance Beneficiary Numbers and Account Numbers	Subcontract clauses	Contractor Virtual Private Network

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:
Contractor employees inappropriately accessing VA data within the Cotiviti GOV Services system.

Mitigation:
Cotiviti GOV Services was required to submit an Access Tracking Plan (ATP) which will control access through a VA approved process that includes monitoring user's access to the VA RAC system.

Section 6. Notice

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

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an Appendix-A 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.

VA provides a notice to Veterans via the VHA Notice of Privacy Practices. A copy is provided in appendix A. Link: https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=1090

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

A copy is provided in appendix A.

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.

VA provides the data that Cotiviti GOV Services is required to audit using parameters listed in the contract. This data is transferred securely to the Cotiviti GOV Services network using MOVEitR SFTP connection. No data is required from Veterans or Beneficiaries, and they are never contacted regarding efforts performed under this contract with VA

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.

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. 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: http://www.archives.gov/veterans/military-service-records/medical-records.html.

VA provides the data Cotiviti GOV Services is required to audit using parameters listed in the contract. This data is transferred securely to Cotiviti GOV Services using MOVEit^{R} SFTP connection. No data is required from Veterans or Beneficiaries, and they are never contacted regarding efforts performed under this contract with VA.

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.

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 or health records.

If your request for amendment is denied, you will be notified of this decision in writing and given information about your right to appeal the decision. In response, you may do any of the following:

- File an appeal
- File a "Statement of Disagreement" which will be included in your health record

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

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 circumstances.

Right to Request Restriction. You may request that we not use or disclose all or part of your health information to carry out treatment, payment or health care operations, or that we not use or disclose all or part of your health information with individuals such as your relatives or friends involved in your care, including use or disclosure for a particular purpose or to a particular person.

Please be aware, that because VHA, and other health care organizations are "covered entities" under the law, VHA is not required to agree to such restriction, except in the case of a disclosure restricted under 45 CFR § 164.522(a)(1)(vi). This provision applies only if the disclosure of your health information is to a health plan for the purpose of payment or health care operations and your health information pertains solely to a health care service or visit which you paid out of pocket in full. However, VHA is not legally able to accept an out-of-pocket payment from a Veteran for the full cost of a health care service or visit. We are only able to accept payment from a Veteran for co- payments. Therefore, this provision does not apply to VHA and VHA is not required or able to agree to a restriction on the disclosure of your health information to a health plan for the purpose of receiving payment for health care services VA provided to you.

To request a restriction, you must submit a written request that identifies the information you want restricted, when you want it to be restricted, and the extent of the restrictions. All requests to restrict use or disclosure should be submitted to the facility Privacy Officer at the VHA health care facility that provided or paid for your care. If we agree to your request, we will honor the restriction until you revoke it unless the information covered by the restriction is needed to provide you with emergency treatment or the restriction is terminated by VHA upon notification to you.

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:
Subject of the data are not made aware of their privacy rights.

Mitigation:
VHA provides notification to Veterans through the mail "Notice of Privacy Practices" and at the point of service. Beneficiaries/family members are provided Privacy notice through Veteran Benefit Administration and the CHAMPVA guide.

VHA Notice of Privacy Practices:
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=1090
VA Privacy links on websites: https://www.oprm.va.gov/privacy/
Privacy impact Assessments: https://www.oprm.va.gov/privacy/pia.aspx

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.***

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.

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)?

All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains your information or health records.

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?

VA provides the data Cotiviti GOV Services is required to audit using parameters listed in the contract. This data is transferred securely to Cotiviti GOV Services using MOVEit^{R} SFTP connection. No data is required from Veterans or Beneficiaries, and they are never contacted regarding efforts performed under this contract with VA.

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.

Cotiviti GOV Services developers create a Data Manipulation Language (DML) script that will be reviewed and executed to correct data inaccuracies. Errors detected from the source data are communicated to VA for retransmission. VA is expected to relay accurate data for processing.

Veterans or Beneficiaries are never contacted regarding efforts performed under this contract they would contact the VA directly at:

Veteran Customer service telephone line: 1-877-881-7618
Beneficiary Customer service telephone line: 1-800-733-8387

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.

VA provides the data Cotiviti GOV Services is required to audit using parameters listed in the contract. This data is transferred securely to Cotiviti GOV Services using MOVEitR SFTP connection. No data is required from Veterans or Beneficiaries, and they are never contacted regarding efforts performed under this contract with VA.

VHA Notice of Privacy Practices:
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=1090
VA Privacy links on websites: https://www.oprm.va.gov/privacy/
Privacy impact Assessments: https://www.oprm.va.gov/privacy/pia.aspx

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.

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. 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:

http://www.archives.gov/veterans/military-service-records/medical-records.html

VA provides the data Cotiviti GOV Services is required to audit using parameters listed in the contract. This data is transferred securely to Cotiviti GOV Services using MOVEit^{R} SFTP connection. No data is required from Veterans or Beneficiaries, and they are never contacted regarding efforts performed under this contract with VA.

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:
Veterans and Beneficiaries are not aware collections of information are being maintained or shared with a contractor (Cotiviti GOV Services).

Mitigation:
This PIA serves as a notification of the collection. The system of record notices also provides the authority to collect and share.

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 PII information by system users is determined utilizing role-based access based on Least Privileges. Role-based training is covered in the Cotiviti GOV Services Privileged Access Training and is provided to anyone obtaining privileged access to any system. Privilege access is also covered in the Annual Security Awareness Training mandatory to all users. User accesses are submitted and approved through Cotiviti GOV Services Identity Management (IDM) – an enterprise access control solution used to track and document the approval process. Access is requested by virtue of their position or role in support of the contract after a successful VA background investigation. Staff managers, security, and program owners are notified for each request prompting for actions such as approval, denial, or request for additional information from the requester.

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?

VA RAC has created the following roles:
System Administrators containing full access to the systems to which they are assigned for system maintenance and support
Application Administrators have limited access to the operating system functions, but full access to assigned application components for application maintenance enhancement and future releases

Security auditors and analysts have access to auditing and security monitoring for security control audits and reporting in addition to monitoring environmental activity
Medical Record Reviewers and Provider Services are provided access to PII as needed to determine the correct identification of the beneficiary for the claim they are reviewing or assisting providers with.

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.

These roles are given the least privileges to perform their duties and will have to request approval before being granted escalated privileges. Users from other agencies will not have direct access to Cotiviti GOV Services internal systems.

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.

The system is maintained using the security concept of least privilege. Only Cotiviti GOV Services employees and InSync subcontractors with the need to work in the VA RAC system and access PII and have had VA background investigations are provided access to the system and PII data. Application and database developers have full access to data. End users such as medical reviewers and provider service representatives are provided access using applications controlling their access to just the PII within the scope of their review and to meet their job requirements. Software is used to track and log events.

Users are granted a specific level of access to the operating system on which they are working. This access is only granted after an approval process is performed via IDM. After approval, access is granted for specific named role access to a system. Users with certain access can only perform specific actions on that system, such as Windows server administrators cannot perform administrator functions on a Linux system. Each role has a minimum privilege need to accomplish the assigned work. Users are assigned to roles based on the concept of least privileges. Administrator roles are granted so that they can perform only the tasks which they need to while blocking them out from all other tasks. Employees must be authorized by their manager as well as their Information System Security Officer (ISSO) to perform privileged functions. Active Directory is used to enforce least privilege in conjunction with our ticketing

system and audit log reviews for escalated privileges. All contractors will sign a Rules of Behavior (ROB) and Non-Disclosure Agreement (NDA) before granted access to the system.

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.

Cotiviti GOV Services institutes a Security Awareness and Training (SAT) program providing all government programs personnel with general security awareness training upon hire (before accessing the VA RAC system) and an annual refresher training thereafter.

All employees also undergo annual Compliance, Code of Conduct and HIPAA training as well as Mandatory Annual Security & Privacy Awareness Computer Based Training (CBT), Annual Social Networking Training, Annual Phishing Awareness Training, Annual IT Security and Awareness Training. In addition, there is a notification posted prior to accessing VA data stating responsibilities for protecting the information collected.

VA also requires Tier 1 and 2 users to complete HIPAA training and Information Security Training in the VA Talent Management System (TMS) before being granted access to any systems.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
1. *The System Security Plan Status Date:* 13-Dec-2021
2. *The Authorization Status:* Authorization to Operate (ATO)
3. *The Authorization Date:* 10-Mar-2022
4. *The Authorization Termination Date:* 09-Mar-2025
5. *The Risk Review Completion Date:* 02-Mar-2022
6. *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.***

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)*

Cotiviti GOV Services utilizes the Microsoft Commercial Cloud platform, which is FedRAMP authorized, and their cloud model is Infrastructure as a Service (IaaS)

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

Cotiviti's contract with the CSP provides that Cotiviti retains all right, title and interest in and to any data including PII. Ownership of data including PHI/PII as between Cotiviti and VA is governed by the party's contract GS00F277CA 36C10X20F00010.

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.

The CSP does not collect any ancillary data other than as required for business operations related to the services being provided for: (1) billing and account management; (2) compensation (e.g., calculating employee commissions and partner incentives); (3) internal reporting and business modeling (e.g., forecasting, revenue, capacity planning, product strategy); (4) combatting fraud, cybercrime, or cyber-attacks that may affect the CSP or CSP products; (5) improving the core functionality of accessibility, privacy or energy-efficiency; and (6) financial reporting and compliance with legal obligations.

When processing for these business operations, the CSP is required to apply principles of data minimization and will not use or otherwise process data for: (a) user profiling, (b) advertising or similar commercial purposes, or (c) any other purpose, other than for the purposes described above.

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.

Yes, the principle is described in Cotiviti's customer contracts. Cotiviti's contracts require that Cotiviti is responsible for all security and privacy of data, whether stored in a cloud, in its physical data centers or elsewhere.

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).

The system does not utilize robotic process automation at this time.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

YOLANDA THORNTON

Digitally signed by YOLANDA THORNTON
Date: 2024.07.09 20:35:18 -04'00'

Privacy Officer, Yolanda Thornton

JOSEPH JARVIS

Digitally signed by JOSEPH JARVIS
Date: 2024.07.10 07:08:41 -05'00'

Information System Security Officer, Joseph "JJ" Jarvis

AKEEL OMARI

Digitally signed by AKEEL OMARI
Date: 2024.07.10 07:55:10 -04'00'

Information System Owner, Akeel Omari

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):
(https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=1090)

Department of Veterans
Affairs Veterans Health
Administration NOTICE OF
PRIVACY PRACTICES
Effective Date September 30, 2019

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED OR DISCLOSED AND HOW YOU CAN GET ACCESS TO YOUR INFORMATION.
PLEASE REVIEW IT CAREFULLY

The Department of Veterans Affairs (VA), Veterans Health Administration (VHA) is required by law to maintain the privacy of your protected health information and to provide you with notice of its legal duties and privacy practices. VHA may use or disclose your health information without your permission for treatment, payment and health care operations, and when otherwise required or permitted by law. This Notice outlines the ways in which VHA may use and disclose your health information without your permission as required or permitted by law. For VHA to use or disclose your information for any other purposes, we are required to get your permission in the form of a signed, written authorization. VHA is required to maintain the privacy of your health information as outlined in this Notice and its privacy policies. Please read through this Notice carefully to understand your privacy rights and VHA's obligations.

YOUR PRIVACY RIGHTS

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. 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 https://www.archives.gov/veterans/military-service-records/medical-records.html.

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 or health records.

If your request for amendment is denied, you will be notified of this decision in writing and given information about your right to appeal the decision. In response, you may do any of the following:

- File an appeal.
- File a "Statement of Disagreement" which will be included in your health record
- Ask that your initial request for amendment accompany all future disclosures of the disputed health information

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 circumstances.

Right to Request Restriction. You may request that we not use or disclose all or part of your health information to carry out treatment, payment or health care operations, or that we not use or disclose all or part of your health information with individuals such as your relatives or friends involved in your care, including use or disclosure for a particular purpose or to a particular person.

Please be aware, that because VHA, and other health care organizations are "covered entities" under the law, VHA is not required to agree to such restriction, except in the case of a disclosure restricted under 45 CFR § 164.522(a)(1)(vi). This provision applies only if the disclosure of your health information is to a health plan for the purpose of payment or health care operations and your health information pertains solely to a health care service or visit which you paid out of pocket in full. However, VHA is not legally able to accept an out-of-pocket payment from a Veteran for the full cost of a health care service or visit. We are only able to accept payment from a Veteran for co- payments. Therefore, this provision does not apply to VHA and VHA is not required or able to agree to a restriction on the disclosure of your health information to a health plan for the purpose of receiving payment for health care services VA provided to you.

To request a restriction, you must submit a written request that identifies the information you want restricted, when you want it to be restricted, and the extent of the restrictions. All requests to restrict use or disclosure should be submitted to the facility Privacy Officer at the VHA health care facility that provided or paid for your care. If we agree to your request, we will honor the restriction until you revoke it unless the information covered by the restriction is needed to provide you with emergencytreatment or the restriction is terminated by VHA upon notification to you.

NOTE: *We are not able to honor requests to remove all or part of your health information from the electronic database of health information that is shared between VHA and DoD, or to restrict access to your health information by DoD providers with whom you have* a *treatment relationship.*

Right to Receive an Accounting of Disclosures. You have the right to know and request a copy of what disclosures of your health information have been made to you and to other

individuals outside of VHA. To exercise this right, you must submit a written request to the facility Privacy Officer at the VHA health care facility that provides your care.

Right to a Printed Copy of the Privacy Notice. You have the right to obtain an additional paper copy of this Notice from your VHA health care facility. You can obtain this Notice from the facilityPrivacy Officer at your local VHA health care facility. You may also obtain a copy of this Notice at the following website: http://www.va.gov/vhapublications.

Notification of a Breach of your Health Information. If a breach of any of your protected health information occurs, we will notify you and provide instruction for further actions you may take, if any.

Complaints. If you are concerned that your privacy rights have been violated, you may file a complaint with:

- The Privacy Officer at your local VHA health care facility. Visit this Web site for VHA facilities and telephone numbers http://www.va.gov/directory/guide/home.asp?isflash=1
- VA via the Internet through "Contact the VA" at http://www.va.gov or by dialing 1-800-983-0936 or by writing the VHA Privacy Office (10A7) at 810 Vermont Avenue NW, Washington, DC 20420.
- The U.S. Department of Health and Human Services, Office for Civil Rights at http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html
- The Office of the Inspector General at https://www.va.gov/oig/hotline/
- Complaints do not have to be in writing, though it is recommended. An individual filing a complaint will not face retaliation by any VA/VHA organization or VA/VHA employee.

When We May Use or Disclose Your Health Information without Your Authorization

Treatment. We may use and disclose your health information without your authorization for treatment or to provide health care services. This includes using and disclosing your information for:

• Emergency and routine health care or services, but not limited to labs and x-rays, clinic visits, inpatient admissions
• Contacting you to provide appointment reminders about treatment alternatives
• Seeking placement in community living centers or skilled nursing homes
• Providing or obtaining home-based services or including hospice services
• Filling and submitting prescriptions for medications, supplies, and equipment
• Coordination of care, including care from non-VHA providers
• Communicating with non-VHA providers regarding your care through health information exchanges
• Coordination of care with DoD, including electronic information exchange

NOTE: *If you are an active-duty service member, Reservist or National Guard member, your health information is available to DoD providers with whom you have a treatment relationship. Your protected health information is on an electronic database that is shared between VHA and DoD. VHA does not have the ability to restrict DoD's access to your information in this database, even if you ask us to do so.*

Examples:

1) A Veteran sees a VHA doctor who prescribes medication based on the Veteran's health information. The VHA pharmacy uses this information to fill the prescription.
2) A Veteran is taken to a community hospital emergency room. Upon request from the emergency room, VHA discloses health information to the non-VHA hospital staff that needs the information to treat this Veteran.
3) A National Guard member seeks mental health care from VHA. VHA discloses this information to DoD by entering the information into a database that may be accessed by DoD providers at some future date.
4) A Veteran is seen by his community health care provider, who wants to review the Veteran's last blood work results from his VHA Primary Care visit for comparison. The community health care provider uses a local health information exchange to request and receive the results from VHA to better care for the Veteran.

Payment. We may use and disclose your health information without your authorization for payment purposes or to receive reimbursement for care provided. This includes using and disclosing your information for:

- Determining eligibility for health care services benefits
- Paying for non-VHA care and services, including services but not limited to, CHAMPVA, Choice and fee basis
- Coordinating benefits with other insurance payers agencies
- Finding or verifying coverage under a health insurance plan or policy
- Pre-certifying insurance
- Billing and collecting for health care provided by VHA
- Reporting to consumer reporting regarding delinquent debt owed to VHA.

Examples:

1) A Veteran is seeking care at a VHA health care facility. VA uses the Veteran's health information to determine eligibility for health care services.
2) The VHA health care facility discloses a Veteran's health information to a private health insurance company to seek and receive payment for the care and services provided to the Veteran.
3) A Veteran owes VA $5000 in copayments for Non-Service Connected care over two years. The Veteran has not responded to reasonable administrative efforts to collect the debt. VA releases information concerning the debt, including the Veteran's name and address, to a consumer reporting agency for the purpose of making the information available for third-party decisions regarding such things as the Veteran's credit, insurance, housing, banking services, utilities.

Health Care Operations. We may use or disclose your health information without your authorization to support the activities related to health care. This includes using and disclosing your information for:

- Improving quality of care or services
- Conducting accreditation
- Conducting Veteran and beneficiary satisfaction surveys
- Reviewing competence or qualifications of health care professionals
- Conducting health care training programs
- Managing, budgeting and planning activities and reports
- Improving health care processes, reducing health care costs and assessing organizational performance
- Legal services
- Certifying, licensing, or credentialing of health care

professionals

- Providing information about treatment alternatives or other programs, including health-related benefits and services
- Performing process reviews and root cause analyses
- Developing, maintaining and supporting computer systems
- Addressing patient complaints
- Conducting audits and compliance fraud, waste and abuse investigations

Examples:

1) Medical Service, within a VHA health care facility, uses the health information of diabetic Veterans as part of a quality-of-care review process to determine if the care was provided in accordance with the established clinical practices.
2) A VHA health care facility discloses a Veteran's health information to the Department of Justice (DOJ) attorneys assigned to VA for defense of VHA in litigation.
3) The VHA health care facility Utilization Review Committee reviews care data, patient demographics, and diagnosis to determine that the appropriate length of stay is provided per Utilization Review Standards.

Eligibility and Enrollment for Federal Benefits. We may use or disclose your health information without your authorization to other programs within VA or other Federal agencies, such as the Veterans Benefits Administration, Internal Revenue Service, or Social Security Administration, to determine your eligibility for Federal benefits.

Abuse Reporting. We may use or disclose your health information without your authorization to report suspected child abuse, including child pornography; elder abuse or neglect; or domestic violence to appropriate Federal, State, local, or tribal authorities. This reporting is for the health and safety of the suspected victim.

Serious and Imminent Threat to Health and Safety. We may use or disclose your health information without your authorization when necessary to prevent or lessen a serious and imminent threat to the health and safety of the public, yourself, or another person. Any disclosure would only be to someone able to help prevent or lessen the harm, such as a law enforcement agency or the person threatened. You will be notified in writing if any such disclosure has been made by a VHA health care facility.

Public Health Activities. We may disclose your health information without your authorization to public health and regulatory authorities, including the Food and Drug Administration (FDA) and Centers for Disease Control (CDC), for public health activities. This includes disclosing your information for:

- Controlling and preventing Disease, injury, or disability
- Reporting vital events such as births and deaths
- Reporting communicable diseases, such as hepatitis, tuberculosis, sexually transmitted diseases & HIV
- Tracking FDA-regulated products
- Reporting adverse events and product defects or problems
- Enabling product recalls, repairs or replacements

Judicial or Administrative Proceedings. We may disclose your health information without your authorization for judicial or administrative proceedings, such as when we receive an order of a court, such as a subpoena signed by a judge, or administrative tribunal, requiring the disclosure.

Law Enforcement. We may disclose your health information without your authorization to law enforcement agencies for law enforcement purposes when applicable legal requirements are met. This includes disclosing your information for:

- Identifying or apprehending an individual who has admitted to participating in a violent crime
- Reporting a death where there is a suspicion that identify or death has occurred as a result of a crime
- Reporting Fugitive Felons
- Investigating a specific criminal act
- Routine reporting to law enforcement agencies, such as gunshot wounds
- Providing certain information to locate a suspect, fugitive, material witness, or missing person

Health Care Oversight. We may disclose your health information without your authorization to a governmental health care oversight agency (e.g., Inspector General; House Veterans Affairs Committee) for activities authorized by law, such as audits, investigations, and inspections. Health care oversight agencies include government agencies that oversee the health care system,

government benefit programs, other government regulatory programs, and agencies that enforce civil rights laws.

Cadaveric Organ, Eye, or Tissue Donation. When you are an organ donor and death is imminent,we may use or disclose your relevant health information without your authorization to an Organ Procurement Organization (OPO), or other entity designated by the OPO, for determining suitabilityof your organs or tissues for organ donation. If you have not specified your donation preferences and can no longer do so, your family may make the determination regarding organ donation on yourbehalf.

Coroner or Funeral Services. Upon your death, we may disclose your health information to a funeraldirector for burial purposes, as authorized by law. We may also disclose your health information to a coroner or medical examiner for identification purposes, determining cause of death, or performing other duties authorized by law.

Services. We may provide your health information without your authorization to individuals, companies and others who need to see your information to perform a function or service for or on behalf of VHA. An appropriately executed contractual document, if applicable, and business associate agreement must be in place to ensure the contractor will appropriately secure and protectyour information.

National Security Matters. We may use and disclose your health information without your authorization to authorized Federal officials for conducting national security and intelligence activities. These activities may include protective services for the President and others.

Workers' Compensation. We may use or disclose your health information without your authorization to comply with workers' compensation laws and other similar programs.

Correctional Facilities. We may disclose your health information without your authorization to a correctional facility if you are an inmate and disclosure is necessary to provide you with health care; toprotect the health and safety of you or others; or for the safety of the correctional facility.

Required by Law. We may use or disclose your health information without your authorization forother purposes to the extent required or mandated by Federal law (e.g., to comply with the Americans with Disabilities Act; to comply with the Freedom of Information Act (FOIA); to comply with a Health Insurance Portability and Accountability Act (HIPAA) privacy or security rule complaint investigation or review by the Department of Health and Human Services).

Activities Related to Research. Before we may use health information for research, all research projects must go through a special VHA approval process. This process requires an Institutional Review Board (IRB) to evaluate the project and its use of health information based on, among other things, the level of risk to you and to your privacy. For many research projects, including any in which you are physically examined or provided care as part of the research, you will be asked to sign a consent form to participate in the project and a separate authorization form for use and possibly disclosure of your information. However, there are times when we may use your health information without an authorization, such as, when:

- A researcher is preparing a plan for a research project. For example, a researcher needs to examine patient medical records to identify patients with specific medical needs. The researcher must agree to use this information only to prepare a plan for a research study; the researcher may not use it to contact you or actually conduct the study. The researcher also must agree not to remove that information from the VHA health care facility. These activities are considered preparatory to research.
- The IRB approves a waiver of authorization to use or disclose health information for the researchbecause privacy and confidentiality risks are minimal and other regulatory criteria are satisfied.
- A Limited Data Set containing only indirectly identifiable health information (such as dates, unique characteristics, unique numbers or zip codes) is used or disclosed, with a data use agreement (DUA) in place.

Military Activities. We may use or disclose your health information without your authorization if you are a member of the Armed Forces, for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission, when applicable legal requirements are met. Members of the Armed Forces include Active-Duty Service members and in some cases Reservist and National Guard members.

Example:
Your Base Commander requests your health information to determine your fitness for duty or deployment.

Academic Affiliates. We may use or disclose your health information without your authorization to support our education and training program for students and residents to enhance the quality of care provided to you.

State Prescription Drug Monitoring Program (SPDMP). We may use or disclose your health information without your authorization to a SPDMP in an effort to promote the sharing of prescription information to ensure safe medical care.

General Information Disclosures. We may disclose general information about you without your

authorization to your family and friends. These disclosures will be made only as necessary and on a need-to-know basis consistent with good medical and ethical practices, unless otherwise directed by you or your personal representative. General information is limited to:

- Verification of identity
- Your condition described in general terms (e.g., critical, stable, good, prognosis poor)
- Your location in a VHA health care facility (e.g., building, floor, or room number)

Verbal Disclosures to Others While You Are Present. When you are present, or otherwise available, we may disclose your health information to your next-of-kin, family or to other individuals that you identify. Your doctor may talk to your spouse about your condition while at your bedside or in the exam room. Before we make such a disclosure, we will ask you if you object or if it is acceptable for the person to remain in the room. We will not make the disclosure if you object.

Verbal Disclosures to Others When You Are Not Present. When you are not present, or are unavailable, VHA health care providers may discuss your health care or payment for your health care with your next-of-kin, family, or others with a significant relationship to you without your authorization. This will only be done if it is determined that it is in your best interests. We will limit the disclosure to information that is directly relevant to the other person's involvement with your health care or payment for your health care.

Examples of this type of disclosure may include questions or discussions concerning your in-patient medical care, home-based care, medical supplies such as a wheelchair, and filled prescriptions.

IMPORTANT NOTE: *A copy of your medical records can be provided to family, next-of-kin, or other individuals involved in your care* ***only*** *if we have your signed, written authorization* ***or*** *if the individual is your authorized personal representative.*

Other Uses and Disclosures with Your Authorization. We may use or disclose your health information for any purpose you specify in a signed, written authorization you provide us. Your signed, written authorization is always required to disclose your psychotherapy notes, if they exist. If we were to use or disclose your health information for marketing purposes, we would require your signed written authorization. In all other cases, we will not use or make a disclosure of your health information without your signed, written authorization, unless the use or disclosure falls under one of the exceptions described in this Notice. When we receive your signed, written authorization we will review the authorization to determine if it is valid, and then disclose your health information as requested by you in the authorization.

Revocation of Authorization. If you provide us a signed, written authorization to use or disclose your health information, you may revoke that authorization, in writing, at any time. If you revoke your authorization, we will no longer use or disclose your health information unless the use or disclosure falls under one of the exceptions described in this Notice or as otherwise permitted by other laws. Please understand that we are unable to take back any uses or disclosures we have already made based on your signed, written authorization.

When We Offer You the Opportunity to Decline the Use or Disclosure of Your Health Information

Patient Directories. Unless you opt-out of the VHA medical center patient directory when being admitted to a VHA health care facility, we may list your general condition, religious affiliation and the location where you are receiving care. This information may be disclosed to people who

ask foryou by name. Your religious affiliation will only be disclosed to members of the clergy who ask for you by name.

Patient Directories. Unless you opt-out of the VHA medical center patient directory when being admitted to a VHA health care facility, we may list your general condition, religious affiliation and the location where you are receiving care. This information may be disclosed to people who ask foryou by name. Your religious affiliation will only be disclosed to members of the clergy who ask for you by name.

NOTE: *If you do object to being listed in the Patient Directory, no information will be given out about you unless there is other legal authority. This means your family and friends will not be able to find what room you are in while you are in the hospital. It also means you will not be able to receive flowers or mail, including Federal benefits checks, while you are an inpatient in the hospital or nursing home. All flowers and mail will be returned to the sender.*

When We Will Not Use or Disclose Your Health Information

Sale of Health Information. We will not sell your health information. Receipt by VA of a fee expressly permitted by law, such as Privacy Act copying fees or FOIA copying fees is not a "sale of health information."

Genetic Information. We will not use or disclose genetic information to determine youreligibility for or enrollment in VA health care benefits.

Changes to This Notice: We reserve the right to change this Notice. The revised privacy practices will pertain to all existing health information, as well as health information we receive in the future. Should there be any changes to this Notice we will make a copy of the revised Notice available to you within 60 days of any change. The Notice will contain the effective date on the first page.

Contact Information: You may the Privacy Officer at your local VHA health care facility if you have questions regarding the privacy of your health information or if you would like further explanation of this Notice. The VHA Privacy Office may be reached by mail at VHA Privacy Office, Office of Health Informatics (10A7), 810 Vermont Avenue NW, Washington, DC 20420 or by telephone at 1-877-461-5038 (toll free).

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