Privacy Impact Assessment for the VA IT System called:

Managed Services – Logistics Health Inc. (LHI) Assessing

Veterans Benefits Administration (VBA)

Medical Disability Examination Office (MDEO)

Date PIA submitted for review:

11/11/2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Lakisha Wright	Lakisha.Wright@va.gov	202-632-7216
Information System Security Officer (ISSO)	Ronald Cox	Ronald.cox@va.gov	414-902-5613
Information System Owner	Jennifer Treger	Jennifer.treger@va.gov	202-461-9497

Abstract

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

Managed Services - Logistics Health Inc. (LHI) Assessing (LHI MedNet) is owned by Optum Serve Health Services (OSHS) and is OSHS's proprietary comprehensive data management information system hosted in the La Crosse WI primary Information Technology Center (PITC), is utilized to capture and store all medical records for examinees. MedNet routes health care encounter data for every member into a single repository that serves as an individualized electronic health record. This record maintains accurate contact information, demographic information, and medical documentation for every member. LHI MedNet is a comprehensive, single-platform solution designed to automate our operational processes, integrate our call centers and other communications and support systems, prioritize operational workload and interface with external systems. MedNet is highly configurable to customer business rules and preferences and adds automation and operational control to nearly every function of our technical approach.

Overview

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

1 General Description

A. The IT system name and the name of the program office that owns the IT system.

Managed Services - Logistics Health Inc. (LHI) Assessing (LHI MedNet), owned by Optum Serve Health Services Incorporated and operated under the Milwaukee region (330), is used to provide services under the VBA MDEO contract.

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

LHI MedNet is a comprehensive, single-platform solution designed to automate our operational processes, integrate our call centers and other communications and support systems, prioritize operational workload and interface with external systems. LHI MedNet is highly configurable to customer business rules and preferences and adds automation and operational control to nearly every function of our technical approach.

C. Indicate the ownership or control of the IT system or project.

LHI MedNet, owned by Optum Serve Health Services Incorporated and operated under the Milwaukee region (330), is used to provide services under the VBA MDE contract.

2. Information Collection and Sharing

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

Data storage will be limited to individuals OSHS is supporting under the Medical Disability Examinations conducted under the VBA MDE contract, with a current count of 437,782 veterans' data stored.

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

This data is only accessible from inside the OSHS network through the LHI MedNet application through use of servers housed in OSHS's datacenters, which utilize Closed Circuit Television (CCTV) among other physical security controls. Limited data is also available through the web portals that provide interfaces for OSHS's providers, VA contract management staff, and Veterans designed specifically for these interactions.

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

Due to its flexible nature, LHI MedNet can respond quickly to evolving requirements based on contract changes that may require technology upgrades or changes in program processing. MedNet has data exchanges established with Virtual Lifetime Electronic Record (VLER) Data Access Services (DAS), allowing for secure encrypted data exchanges between VA and OSHS.

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

The LHI MedNet system is housed in OSHS's two datacenters, all held to the same security and compliance requirements, in line with VA6500/NIST SP 800-53 revision 4. Systems are replicated between sites to ensure all systems are available in the event of loss of a datacenter.

3. Legal Authority and SORN

H. "VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA" 58VA21/22/28.

Legal authorities for this collection are defined under Title 10 U.S.C. chapters 106a, 510, 1606 and 1607 and Title 38, U.S.C., section 501(a) and Chapters 11, 13, 15, 18, 23, 30, 31, 32, 33, 34, 35, 36, 39, 51, 53, and 55.

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

N/A

D. System Changes

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

Completion of this PIA does not result in changes to OSHS's business processes.

K. Whether the completion of this PIA could potentially result in technology changes
Completion of this PIA does not result in changes to OSHS's technology solutions.

Section 1. Characterization of the Information

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

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

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

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

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

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

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

Claimed Conditions, Disability Benefit Questionnaires (DBQs) being requested to be performed by contractor, and Previous Diagnoses along with narrative details. We also have the inclusion of Request ID, Veteran Customer ID, Medical Center, Exam Name, Exam ID, Voucher Number, Veteran Diagnosis, Physician Name, and Physician License Number.

PII Mapping of Components (Servers/Database)

MedNet consists of one key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by MedNet and the reasons for the collection of the PII are in the table below.

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

Internal Database Connections

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
VBMS	**Yes**	**Yes**	**SSN**	The information collected directly identifies specific	SSN Numbers are masked

				individuals, or the information can be used to trace an individual's identity (i.e., it is linked or linkable to specific individuals).	within the application and database. SSNs are not visible in the application and are hashed within the database.

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?

Information is collected from a VA data exchange such as DAS, through interaction with the VA beneficiary themselves through an appointment or contact center contact, or details attained from VBMS.

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.

N/A

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

MedNet

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

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

The information is collected either through the DAS data exchange with VA, through claims file documents obtained from Veterans Benefits Management System (VBMS) and through completion of documentation or interaction with disability examination providers at appointments, or through interaction with contact center personnel.

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

N/A

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

These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

Data accuracy for data received from VA data exchanges are verified with the Veteran during calls or office visits, in addition to field validation for data fields within MedNet.

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

N/A

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

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in

addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders. This question is related to privacy control AP-1, Authority to Collect

Legal authorities for this collection are defined under Title 10 U.S.C. chapters 106a, 510, 1606 and 1607 and Title 38, U.S.C., section 501(a) and Chapters 11, 13, 15, 18, 23, 30, 31, 32, 33, 34, 35, 36, 39, 51, 53, and 55. SORN 58VA21/22/28 (November 8, 2021). Link:

https://www.gpo.gov/fdsys/pkg/FR-2012-07-19/pdf/2012-17507.pdf

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: Sensitive Personal Information and Protected Health Information are stored within the system and could be improperly disclosed.

Mitigation: Security and Privacy Controls, in line with VA Directive 6500 and NIST 800-53 Revision 4, are in place to protect the confidentiality, integrity, and availability of the data within the system. All employees with access to Veterans' information are required to complete VA Rules of behavior and VA Privacy and Security Awareness training annually. Additionally, all data exchanged between OSHS and VA are encrypted in transit, in addition to being encrypted at rest.

Section 2. Uses of the Information

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

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

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

All VA beneficiary data is used only as required in the act of performing VA Compensation and Pension Examinations as required under the VBA MDE contract. The information is used to identify and contact the veteran, conduct the disability exams, and to report back to VA to support benefits determination.

Name: Identification & Communication
SSN: Identification
Email Address: Communication
Mailing Address: Communication
Zip Code: Communication (part of Mailing Address)
Phone Number: Communication
Current Medications: Data required for examination
Previous Medical Records: Data required for examination
Claimed Conditions: Data required for examination
Disability Benefit Questionnaires (DBQs): Data required for examination
Previous Diagnoses along with narrative details: Data required for examination
Request ID: Identification
Veteran Customer ID: Identification
Medical Center: Data required for examination
Exam Name, Exam ID: Identification
Voucher Number: Data required for examination
Veteran Diagnosis: Data required for examination
Physician Name: Identification
Physician License Number: Identification

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.

Data produced would be limited to data gathered in speaking with the Veteran, or through an examination performed as a part of the VA Compensation and Pension Examinations under the VBA MDE contract. The data is put into the individuals records and is uploaded to their VA data record through electronic data exchanges established with VA.

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.

There are no further analysis tools used on the data that is gathered in MedNet.

2.3 How is the information in the system secured?

These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

2.3a What measures are in place to protect data in transit and at rest?

The information that is collected and used in MedNet is stored internally under FIPS 140-2 or higher encryption on both the storage area network (SAN) and on any other physical servers that may store process or transmit data. Data in transit is encrypted at the same level. Portal access for Providers and Veterans is encrypted with SSL.

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

Social Security Numbers are hashed in the Mednet database and are not directly available. SSN Numbers are masked within the application and database. SSN's are not visible in the application and are hashed within the database.

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

All information is encrypted per FIPS 140.2 modules both in-transit and at rest. MedNet uses a defense-in-depth approach to security based on NIST SP 800-53 revision 4.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. ***Example: Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or system***

controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.

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

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

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?
This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

2.4a How is access to the PII determined?

The information that is collected and used in MedNet is the minimum necessary information needed to provide the services under the VBA MDE contract

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

All employees with access to Veterans' information are required to complete VA Rules of Behavior and VA Privacy and Security training annually. All access to the information requires either a Personal Identity Verification (PIV) card for VA-side access, or OSHS domain authentication including use of RSA multifactor authentication to access MedNet.

2.4c Does access require manager approval?

Access to PII is assigned based on the role of the individual and is detailed by the manager in the user provisioning process. This PIA and the VA SORN Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA, SORN 58VA21/22/28 (last published 11/8/2021) also enumerate the purposes for which information can be used.

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

Access rights are removed and reassigned for each transferred user, and these access permissions are re-approved annually through entitlement reviews of the MedNet application. Additionally, prior to the entitlement reviews, all access assigned to roles are reviewed and approved by the application owner. All modifications, creations, and deletes are monitored and recorded to an audit table.

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

Disciplinary actions, up to and including termination of employment, are possible for violations of the requirements specified in the training and their positions as OSHS employees.

Section 3. Retention of Information

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

*Identify and list all information collected from question 1.1 that is **retained** by the system.*
This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal

Name, Social Security Number, Mailing Address, Zip Code, Phone Numbers, Email Addresses, Current Medications, Previous Medical Records, Claimed Conditions, DBQs, Veteran Customer ID, Medical Center, Exam Name, Exam ID, Voucher Number, Veteran Diagnosis, Physician Name, Request ID, Physician License Number and Previous Diagnoses are retained within the MedNet system.

3.2 How long is information retained?

*In some cases VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. **For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods**. The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented. 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.*

Per contractual requirements, the examination data (case data & PHI) will be kept for 3 years plus the lifetime of the case and will be appropriately destroyed at the end of the contract in accordance with NIST SP 800-88 and VA Directive 6500. Lifetime of the case would typically be less than 30 days, meaning a typical retention period would be approximately 1,125 days.

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

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

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

Yes

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

Records Control Schedule VB-1 Part 1, Section, XIII, Veterans Benefits Administration Records Management, Records Control Schedule VB–1, Part 1, Section VII located at https://www.benefits.va.gov/WARMS/docs/regs/RCS_I.doc

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.

Any paper records are shredded at OSHS using Iron Mountain for its secure disposal method. Non-paper records are stored on magnetic media, such as Hard Drives, and are destroyed by erasing the data through an overwrite process (in accordance with NIST SP 800-88 "Guidelines for Media Sanitization) before being shredded on site by a third party; with a certificate of destruction issued for the media. This is in line with VA Directive 6500; and meets the requirements of PWS Section 19.9.12 specifying the contractor is required to self-certify that the media has been disposed of per VA Directive 6500 requirements. The VA Record Officer is aware of and approves of this disposal method.

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.

All PII is kept solely in the production environment, and all data in training/release candidates/development instances would be non-production data. OSHS does not share data with researchers.

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: The risk is that the information may be stored longer than necessary or be used outside of its intended purpose.

Mitigation: Mitigations in place include the placement of locked, blue Iron Mountain shred bins that are shredded on a weekly basis by Iron Mountain and retaining of only necessary information for performance within the VBA contract. OSHS follows RCS VB-1 and records are retained in accordance with RCS VB-1 and then disposed based on the procedures listed in 3.4. All individuals with access to Veterans' Information in MedNet have completed VA Rules of Behavior and VA Privacy and Security training and have a valid need to access the data. Finally, OSHS has security and privacy controls in place to meet the requirements of VA Directive 6500 and NIST SP 800-53 Revision 4.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Veterans Benefits Management System (VBMS) Exam Management System (EMS) via Data Access Service (DAS)	Exam Requests are sent to the VES from VBMS via DAS. Results are sent back to VBMS via DAS.	Request ID, Veteran Name, Veteran SSN, Veteran Customer ID, Medical Center, Exam Name, Exam ID, Voucher Number, Veteran Diagnosis, Physician Name, Physician License Number	SOAP over HTTPS using SSL encryption and Certificate exchange

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: Private information could be released to unauthorized individuals, or through unauthorized channels.

Mitigation: Interconnection Security Agreements/Memorandums of Understanding have been completed for DAS data exchanges between VA and OSHS. Additionally, data shares are configured through VA-established data exchanges such as DAS, in line with the requirements of VA Directive 6500 and NIST SP 800-53 Rev 4. These interconnections are automated with certificate-based authentication. There's no user involvement.

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***
OptumHealth VA Eligibility	Used for providing Behavioral Health services.	Personally Identifiable Information (PII), Individually Identifiable Information (III), SSN, Name, Address	Provider Network Agreements and MOU.	Secure File Transfer Protocol (SFTP)

5.2 <u>PRIVACY IMPACT ASSESSMENT: External sharing and disclosure</u>
Discuss the privacy risks associated with the sharing of information outside the Department and what steps, if any, are currently being taken to mitigate those identified risks.

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

Follow the format below:

<u>Privacy Risk:</u> Privacy information could be improperly disclosed

Mitigation: Data provided is the minimum amount needed to coordinate any services or examinations needed. Data is sent via encrypted channels to ensure confidentiality and integrity of data in transit via FIPS 140-2 compliant algorithms. ISA/MOUs are in place for interconnections between OSHS and VA. Furthermore, access to all VA systems require the completion of a VA-managed background check, and issue of a PIV card and Citrix use for access to VA systems.

Further controls on this include the controls of VA6500, including the Access Control (AC), Media Protection (MP), Awareness and Training (AT), Physical and Environmental Protection (PE), Audit and Accountability (AU), Planning (PL), Security Assessment and Authorization (CA), Personnel Security (PS), Configuration Management (CM), Risk Assessment (RA), Contingency Planning (CP), System and Services Acquisition (SA), Identification and Authentication (IA), System and Communications Protection (SC), Incident Response (IR), System and Information Integrity (SI), Maintenance (MA), Program Management (PM), Authority and Purpose (AP), Accountability, Audit, and Risk Management (AR), Data Quality and Integrity (DI), Data Minimization and Retention (DM), Individual Participation and Redress (IP), Security (SE), Transparency (TR), and Use Limitation (UL) families.

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.

Optum Serve Health Services identifies its affiliation to the VA as a contractor performing VA Compensation and Pension Examinations and this is communicated to the Veteran during contact center outreach and in written communication, in form of securely delivered appointment kits. These kits include appointment location, date and time of the exam, any examination requirements (i.e. resting prior, items needed for Veteran verification), as well as the required practitioner details as contractually dictated.

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

Notice can be found in the SORN – "VA Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records – VA" 58VA21/22/28.This SORN can be found online at http://www.gpo.gov/fdsys/pkg/FR-2012-07-19/pdf/2012-17507.pdf

Enter Major Application name here.
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.

Additionally, the VA has published a System of Records Notice is published in the Federal Register for VA SORN Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA, SORN 58VA21/22/28 (last amended November 8, 2021) at 77 Federal Register 42594.

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.

Yes. Either via telephonic outreach or in person attendance to appointments, the Veteran can choose to decline to provide information. Over the phone the refusal is captured via call recording and notes from those in OSHS's contact center. When attending an appointment the Veteran verbalizes with the examiner and a declination of services form is filled and signed by the Veteran.

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.

Yes. Optum Serve Health Services only uses the data and information collected for the sole purpose of processing and performing services for VA Compensation and Pension Exams requested by the VA. However, the individual has the right to consent to use of data. To opt out of certain usage, the individual will need to express his concerns in writing to the designated VBA Regional office.

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: The individual may be unaware of his Privacy rights.

Mitigation: This is mitigated through several avenues including the notice of information collection, retention, and processing through the systems OSHS exchanges with DAS in addition to the System of Record Notice and the publishing of this Privacy Impact Assessment. OSHS is required by its contract with the VA to only use the information it receives from individuals for the purposes necessary to accomplish the services being provided by OSHS.

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.***

In order for OSHS to communicate orally with the Veteran about services being performed or other details the Veteran must: Verify their identity with First and Last name as well as other identifying criteria that meets the minimum needed to validate the identity of the individual.

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).

N/A

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.

To gain access to the medical records or documentation processed by OSHS for the Compensation and Pension Examinations, in accordance with contract requirements the Veteran must contact the VA Regional Office for any documentation as it is related to the examination.

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.

OSHS will correct inaccuracies in contact details as a result of outreach with the Veteran. Within OSHS's process, address and contact details provided by the VA are verified with the Veteran. When these are incorrect, the details are updated in our business system for further support in processing for the examination. In the event the Veteran communicates that the services are erroneous, or they had been provided for their claim already, these contentions are requested for cancelation and sent back to the VA Regional Office for their oversight and review.

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.

In the event the Veteran's information is inaccurate, they are told to contact their VA Regional Office and ensure the VA's systems are up to date, as OSHS receives those details from the VA. Individuals can learn about Privacy Act processes in VA SORN Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA, SORN 58VA21/22/28(last amended 11/8/2021).

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.

Formal redress is provided as described in Sections 7.1-7.3.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

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

Mitigation: This privacy risk is mitigated by information provided in this PIA and the VA SORN Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA, SORN 58VA21/22/28(last amended 11/8/2021). This states that individuals should contact their local VA regional office for additional information about accessing and contesting their records at the VA.

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 within MedNet is determined based on the role of the employee, based on job title. Access is provisioned during the user's onboarding and is based on the role they are filling on hire. Each role has specific access defined based on minimum access needed to fulfill their duties, and these are reviewed annually and updated as needed, on top of annual entitlement reviews.. If a user transfers or changes roles, all permissions are removed, and the new permissions are applied.

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?

Only OSHS employees have access to MedNet. MedNet is not externally accessible.

8.1c Describe the different roles in general terms that have been created to provide access to the system. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

Access is defined in a very granular manner, with over 100 different functions being defined in write/read/no access for each role for MedNet. OSHS has a documented access control policy.

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.

As a VA contractor, OSHS employees providing services under the VBA MDE contract will access OSHS's MedNet system as a part of their duties in executing the VBA MDE contract. As part OSHS's employment practices new employees are required to read and sign a non-disclosure agreement (NDA) as part of their employment process. There are no other VA contractors accessing 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.

All OSHS employees providing services under the VBA MDE contract must read and acknowledge their receipt and acceptance of the VA Information Security Rules of Behavior (RoB) prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training that all personnel must complete via the VA's TMS; this also includes HIPAA training. This is completed both on hire and annually thereafter.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 06-Sep-2022
3. *The Authorization Status:* Authorization to Operate (ATO)
4. *The Authorization Date:* 08-Nov-2022
5. *The Authorization Termination Date:* 08-Nov-2023
6. *The Risk Review Completion Date:* 20-Oct-2022
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

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

N/A.

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)*

N/A

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.*

OSHS MedNet currently does not have a FedRAMP provisional or agency authorization.

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

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

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

N/A. OSHS MedNet currently does not use cloud technology.

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

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

N/A. OSHS MedNet currently does not use cloud technology.

9.5 If the system is utilizing Robotics Process Automation (RPA), please describe the role of the bots.

Robotic Process Automation is the use of software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. For example, will the automation move or touch PII/PHI information. RPA may also be referred to as "Bots" or Artificial Intelligence (AI).

N/A. OSHS MedNet currently does not use cloud technology.

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

ID	Privacy Controls
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.

LAKISHA V WRIGHT 111646

Digitally signed by LAKISHA V WRIGHT 111646
Date: 2022.12.02 14:03:57 -05'00'

Privacy Officer, Lakisha Wright

Ronald S Cox 655952

Digitally signed by Ronald S Cox 655952
Date: 2022.12.05 15:26:37 -06'00'

Information System Security Officer, Ronald Cox

Jennifer L. Treger 105837

Digitally signed by Jennifer L. Treger 105837
Date: 2022.12.05 16:32:46 -05'00'

Information System Owner, Jennifer Treger

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).

Notice of Privacy Practice (NOPP):

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices

HELPFUL LINKS:

Record Control Schedules:

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

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

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

National Archives (Federal Records Management):

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

VHA Publications:

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

VA Privacy Service Privacy Hub:

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