Privacy Impact Assessment for the VA IT System called:

Workers' Compensation-Occupational Safety Health/Management Information System

(WCP)

Infrastructure Operations Support (IO-AS)

Veterans Affairs Central Office (VACO)

Date PIA submitted for review:

02/20/2024

System Contacts:

	Name	E-mail	Phone Number
Privacy Officer	Gina Siefert	Gina.siefert@va.gov	202-632-8430
Information System Security Officer (ISSO)	Griselda Gallegos	Griselda.gallegos@va.gov	512-326-6037
Information System Owner	Tiffiney Benton	Tiffiney.Benton@va.gov	980-565-7059

Abstract

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

The purpose of Workers' Compensation-Occupational Safety Health/Management Information System is to facilitate the management of workers' compensation claims filed under the Federal Employment Compensation Act (FECA) which is administered by the U.S. Department of Labor, Office of Workers' Compensation Programs (OWCP) the system records and tracks work related injuries and illnesses for the Department of Veteran Affairs employees.

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 Workers' Compensation – Occupational Safety Health\Management Information System (WCOSH\MIS) application is written and owned by the Veterans Health Administration – Office of workers' compensation Program (VHA-OWCP) Fund and funded by the Director, Occupational Safety and Health OOS1.

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 purpose of the program is to record and track injuries and illnesses for the Department of Veteran Affairs employees, which are reported to the Department of Labor (DOL). The Workers' Compensation-Occupational Safety Health/Management Information System (WC-OSH\MIS) tracks work related illnesses and injuries is mandated by DOL, and its reduction by Presidential Order. The purpose of tracking is to reduce the rising costs associated with on-the-job injuries and lost time claims preventing workers from returning to the work force

C. *Who is the owner or control of the IT system or project?*
WC-OSH/MIS is owned by the Office of Occupational Safety and Health/Workers' Compensation, including ownership of the Memorandum of Understanding (MOU) governing the use of DOL data. The Office of Information & Technology (OIT) provides system development and operational support.

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?*

The number of individuals whose information is stored in the system is approximately 275,000 with number increasing daily as new claims are filed. The client/individual information in the system is on Veteran Affairs employees who have filed worker compensation claims with the Department of Labor (DOL).

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

The purpose of the program is to record and track injuries and illnesses for the Department of Veteran Affairs employees which are reported to the Department of Labor (DOL).

The data include the claimant's name, address, Social Security number, date of birth, grade, salary, telephone number, OWCP's case adjudication status (approved or denied, waiting adjudication, file sent to Hearings and Review for decision), medical injury /illness information such as *accepted medical condition(s), compensation paid (amount and time period covered), medical bills paid (name of physician, hospital or health facility, type of treatment, date of treatment, amount paid, amount paid for medical equipment, and rehabilitation expenses*, COP authorized or denied, dates COP is paid, number of days of COP, and total amount paid

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

The WC-OSH/MIS system does not share data with any other system. The WC-OSH/MIS system only receives data from DOL and HR-PAS (payroll data).

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

The WC-OSH/MIS system only operates at one site – the Austin Information Technology Center (AITC).

3. Legal Authority and SORN

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

https://www.govinfo.gov/content/pkg/FR-2023-01-25/pdf/2023-01438.pdf 08VA05/ 88 FR 4885 (https://www.oprm.va.gov/privacy/systems_of_records.aspx)

System of Record Notice (SORN) 86VA00S1 Workers' Compensation-Occupational Safety and Health/Management Information System—VA states the authority for operation/ maintenance of the system: Public Law 91–596; 5 U.S.C. 8101 et seq.; and Federal Regulations 20 CFR part 10, 29 CFR part 1960, and 5 CFR Ch. 1, part 353.

All Federal Employees' Compensation Act (FECA) information (which is what WCOSH/MIS contains) is owned by DOL, even when in the position of VA. FECA information falls under DOL's government-wide SORN, called DOL-GOVT/1, and not any VA privacy regulations. In addition, the MOU between VA and DOL covers the storage and use of FECA data.

The DOL government-wide SORN can be found here DOL/GOVT-1 | U.S. Department of Labor.

The original SORN 86VA00S1 assumes both Safety and Workers Compensation data, but WC-OSH/MIS only holds Workers Compensation records which are covered under the DOL/GOVT-1 SORN . Note the replacement system for WC-OSH/MIS (S/WIMS) did not need a SORN because the DOL-GOVT/1 one is government-wide and addresses the targeted data.

Federal Information Security Management Act(FISMA), Title III of Public Law 107-347, December 17, 2002(the E-Government Act of 2002) (as amended), 44 USC 3541 et seq. Authority for operation/ maintenance of the system: Pub. L. 91–596, 5 U.S.C. 8101 et seq. and Federal Regulations 20 CFR part 10, 29 CFR part 1960, and 5 CFR ch. 1, part 353. The Secretary of Veterans Affairs established these guidelines pursuant to the authorities in and requirements of Title 38, United States Code, section 81 11 (38 U.S.C. 5811 I), titled "Sharing of Department of Veterans Affairs and Department of Defense Health Care Resources," and the authorities contained under Title 10, United States Code, section 1104 (10 U.S.C.5 1104), titled "Sharing of Resources with the Department of Veterans Affairs," which incorporates Title 31, United States Code, section 1535 (31 U.S.C. 51 535), titled "Agency Agreements," also known as the "Economy Act." These guidelines assist in the implementation of these statutes

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

No, the system is not in the process of being modified.

4. System Changes

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

No

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

No

Section 1. Characterization of the Information

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

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

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

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

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1. 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 (pay grade, pay step)

☐ 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:

- Medical injury/illness information
- Zip code

PII Mapping of Components (Servers/Database)

Workers' Compensation-Occupational Safety Health/Management Information System consists of **2** 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 **Workers' Compensation-Occupational Safety Health/Management Information System** 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	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

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

Program Interface (API) etc.) that contains PII/PHI					
WCP Server 1	**Yes**	**Yes**	SSN, DOB, Personal Phone Numbers, Personal Mailing Address, Name, Pay Grade, Pay Step, Medical Injury/Illness Information	Storing WC claim data	Data is encrypted
WCP Server 2	**Yes**	**Yes**	SSN, DOB, Personal Phone Numbers, Personal Mailing Address, Name, Pay Grade, Pay Step, Medical Injury/Illness Information	Entering and Processing WC Claims	HTTPS

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

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

The information for the claim comes from DOL and the payroll system as determination for eligibility. Sources include data elements from the Personnel and Accounting Integrated Data System-VA, VA COP data, and VA employees.

1.2b Describe why information from sources other than the individual is required? For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question indicate why the system is using this source of data.

Information is needed from other sources to determine entitlements with regard to wages at time of illness or injury and rates of pay

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

The system has a myriad of reports gleaned from the case information in the database and utilized by VA Office of Workers' Compensation Program (OWCP) and Safety Managers to manage their claims, mitigate safety risks, departmental as well as DOL reporting requirements

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?

Once DOL has assigned a case number, captures the case information, receives any bills or determines any compensation, the information related to the case is sent to the VA in the form of the bi-weekly files which include the case master, bill payment and compensation payment files. Updates to the cases are received via the bi-weekly and quarterly chargeback transfer files. In addition, a payroll file is received from HR-PAS after each payroll run. The salary information is used to ensure the compensation amounts received from DOL are accurate.

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 collection forms used in the data received or stored in WC-OSH/MIS.

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.

The information goes through an integrity check at the time it is entered and before it is saved to the database (Automated). Further integrity checks are made once received by DOL. The information is again checked upon receipt from DOL as a case through the bi-weekly and quarterly feeds. Information that does not pass the integrity checks is rejected and returned to the source for correction and resubmitted.

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?

This system does not use a commercial aggregator to check accuracy

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

Federal Information Security Management Act(FISMA), Title III of Public Law 107-347, December 17, 2002(the E-Government Act of 2002) (as amended), 44 USC 3541 et seq. Authority for operation/ maintenance of the system: Pub. L. 91–596, 5 U.S.C. 8101 et seq. and Federal Regulations 20 CFR part 10, 29 CFR part 1960, and 5 CFR ch. 1, part 353. The Secretary of Veterans Affairs established these guidelines pursuant to the authorities in and requirements of Title 38, United States Code, section 81 11 (38 U.S.C. 5811 I), titled "Sharing of Department of Veterans Affairs and Department of Defense Health Care Resources," and the authorities contained under Title 10, United States Code, section 1104 (10 U.S.C.5 1104), titled "Sharing of Resources with the Department of Veterans Affairs," which incorporates Title 31, United States Code, section 1535 (31 U.S.C. 51 535), titled "Agency Agreements," also known as the "Economy Act." These guidelines assist in the implementation of these statutes.

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

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

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

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

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

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

<u>Principle of Data Quality and Integrity:</u> 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: WCP collects Personally Identifiable Information (PII). If this information was breached or accidentally released to inappropriate parties or the public, it could result in financial, personal, and/or emotional harm to the individuals whose information is contained in the system.

Mitigation: The Department of Veterans Affairs is careful to only collect the information necessary to identify the parties involved in an incident, identify potential issues and concerns, and offer assistance to the affected parties so that they may find the help they need to get through their crisis. By only collecting the minimum necessary information, the VA is able to better protect the individual's information.

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	Identification purposes	Not used
Social Security Number	Identification purposes	Not used
Date of Birth	Identification purposes	Not used
Mailing Address	Identification purposes	Not used
Zip code	Identification purposes	Not used
Phone Number	Identification purposes	Not used
Pay Grade	Identification purposes	Not used
Pay Step	Identification purposes	Not used
Medical injury/illness information	Identification purposes	Not used

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?*

There are number of reports available to the OWCP specialist which is used for the management of claims or the management and mitigation of safety risks (WCP has its own report function allowing authorize users the ability to run a variety of reports). The only analysis is the reporting function.

2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

The system does not create or make available new or previously unutilized information about an individual.

2.3 How is the information in the system secured?

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

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

Data is protected in transmit via secure electronic data exchange from mailman messaging in VISTA and also safeguarded by encryption, SFTP and HTTPS.

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

No additional protections for SSNs in the Production environment. In non-production environments, SSNs, along with any other PII/PHI data elements are masked.

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

Individual access is requested via the Agency Administrator who in turn validates that the individual has a legitimate need for access because of their position as documented by the System Security Plan. Once the need is established and verified, the Agency Administrator enters them into the system via the application. All users, regardless of whether they are in the agency or contracted to do case investigation, must be approved by the Agency Administrator. Additionally, all users are required to sign a Rules of Behavior. The different roles are 'read-only', 'data-entry', 'agency-administrator' and 'system-administrator'. 'Read-only' access gives read-only compartmentalized access within the agency or agencies which the user is assigned. 'Data-entry' gives read/write compartmentalized access within the agency or agencies which the user is assigned. ‘Agency administrator’ gives read/write access within the agency or agencies which the user is assigned. ‘System administrator’ gives read/write access.

The control of access is managed by the program owners. Access to and use of the information is covered by the Rules of Behavior and the Government Computer Systems warnings. The System of Records Notice (SORN) for the WCP system is 86VA00S1 -Workers Compensation Occupational Safety and Health Management Information System (Formally known as 86VA058)-VA. The official system of records notice (SORN) for these can be found on-line at: http://www.gpo.gov/fdsys/pkg/FR-2000-09-14/pdf/00-23569.pdf Amended SORN can be found at: http://www.gpo.gov/fdsys/pkg/FR-2008-08-05/pdf/E8-17899.pdf. The SORN defines the information collected from veterans, use of the information, and how the information is accessed and stored.

The minimum-security requirements for WCP’s high impact system cover 17 security-related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. Our facilities employ all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 Rev 4 and specific VA directives. VA Records Management Policy and the VA Rules of Behavior in Talent Management System (TMS) govern how Veterans’ information is used, stored, and protected.

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?

Individual access is requested via the Agency Administrator who in turn validates that the individual has a legitimate need for access because of their position as documented by the System Security Plan. Once the need is established and verified, the Agency Administrator enters them into the system via the application. All users, regardless of whether they are in the agency or contracted to do case investigation, must be approved by the Agency Administrator. Additionally, all users are required to sign a Rules of Behavior. The different roles are 'read-only', 'data-entry', 'agency-administrator' and 'system-administrator'. 'Read-only' access gives read-only compartmentalized access within the agency or agencies which the user is assigned. 'Data-entry' gives read/write compartmentalized access within the agency or agencies which the user is assigned. 'Agency administrator' gives read/write access within the agency or agencies which the user is assigned. 'System administrator' gives read/write access.

The control of access is managed by the program owners. Access to and use of the information is covered by the Rules of Behavior and the Government Computer Systems warnings. The System of Records Notice (SORN) for the WCP system is 86VA00S1 -Workers Compensation Occupational Safety and Health Management Information System (Formally known as 86VA058)-VA. The official system of records notice (SORN) for these can be found on-line at: http://www.gpo.gov/fdsys/pkg/FR-2000-09-14/pdf/00-23569.pdf Amended SORN can be found at: http://www.gpo.gov/fdsys/pkg/FR-2008-08-05/pdf/E8-17899.pdf. The SORN defines the information collected from veterans, use of the information, and how the information is accessed and stored.

The minimum-security requirements for WCP's high impact system cover 17 security-related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. Our facilities employ all security controls in the respective high impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 Rev 4 and specific VA directives. VA Records Management Policy and the VA Rules of Behavior in Talent Management System (TMS) govern how Veterans' information is used, stored, and protected.

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

Yes

2.4c Does access require manager approval?

Yes

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

User login activity is recorded. Access to the PII data is controlled by the role assigned and the case scope assigned.

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

Agency Administrator from the Office of Occupational Safety and Health/Workers' Compensation

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*

The PII/PHI information retained by the system includes the following:

- Name
- Social Security Number (SSN)
- Date of Birth (DOB)
- Mailing address
- Zip code
- Phone Number
- Financial Information (Pay Grade, Pay Step)
- Medical injury/illness information

3.2 How long is information retained?

In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. ***The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.*** *If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

Per the SORN, Records are scheduled to be destroyed 30 years after OWCP closes the claimant's case file.

The official system of records notice (SORN) for these can be found on-line at: http://www.gpo.gov/fdsys/pkg/FR-2000-09-14/pdf/00-23569.pdf

DOL-GOVT/1 covers how DOL treats their data and while they may mark something as "retired" or "deleted", it is not deleted in WC-OSH/MIS because if DOL reactivates the case, it would need the last known state of that case/record. The applicable MOU states the following:

> *DVA will retain FECA data, documents and information provided by DOL pursuant to this MOU in accordance with the appropriate records retention schedule regarding FECA records inthe custody of non-DOL agencies, set forth in General Records Schedule 2.4,Disposition Authorities DAA-GRS-2016-0015-0012 and 00*

The data files received from DOL are deleted after 180 days per the MOU.

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

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

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

Yes, the disposition authority is DAA-GRS 2016-0015 0012.

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

GENERAL RECORDS SCHEDULE 2.4: Employee Compensation and Benefits Records
Item: 100
Workers' Compensation (personnel injury compensation) records.
Disposition Authority: DAA-GRS 2016-0015 0012

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

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

Electronic media sanitization, when the records are authorized for destruction (or upon system decommission) will be carried out in accordance with *VA Directive 6500 Cyber Security Program* . Forms and other types of printed output produced by any computer systems and related peripherals will be evaluated by the responsible staff member for data sensitivity. Printed output containing sensitive data will be stored in locked cabinets or desks and disposed of properly by shredding or similar VA approved methods in accordance with VA Directive 6371. Program listings and documentation relating to the use of or access to a computer system require special handling if the listings or documentation provide information about a system which processes sensitive data. VA personnel are responsible for retrieving/removing all printed outputs they request from printers.

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

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

WCP does not use PII 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 that the information maintained that could be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached.

Mitigation: To mitigate the risk posed by information retention, WCP adheres to the Records Schedule approved by NARA. When the retention date is reached for a record, the individual's information is carefully disposed of by the determined method as described in Records Schedule in accordance with VA media destruction policies.

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*
Human Resources – Payroll Application Services (HR-PAS)	Pay grade information used to check accuracy of the compensation paid amounts	• Name • Social Security Number • (SSN) • Date of Birth (DOB) • Mailing address • Zip Code • Financial Information (Pay Grade, Pay Step) • Phone • Medical injury/illness information	Transmitted via secure electronic data exchange from an Amazon Web Services S3 bucket. This runs automatically following the

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*
			regular payroll run

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:

<u>Privacy Risk:</u> Claims information is available through the application and could be disclosed to an unauthorized user of the system.

<u>Mitigation:</u> Users are required to sign a rules of behavior document which outlines specific uses for the claims data and the penalty which could be imposed as a result of misuse of that data.

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***
Department of Labor Office of Workers' Compensation Programs (OWCP)	Bi-weekly updates on all workers compensations cases	• Name • Social Security Number • (SSN) • Date of Birth (DOB) • Mailing address • Zip Code • Phone • Medical injury/illness information •	DOL ISA/MOU	Transmitted via secure electronic data exchange Batch SFTP. Secure File Transfer Protocol (FTP)

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.

*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: The privacy risk associated with maintaining PII is that sharing data outside of the Department of Veteran's Affairs could increase the risk that data may be disclosed to individuals who do not require access and heightens the threat of the information being misused.

Mitigation: The file that is provided is via SFTP and covered by an ISA/MOU. The principle of need-to-know is strictly adhered to. Only personnel with a clear business purpose are allowed access to the system and the information contained within the 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.

This question does not apply to this system, since it is not the system used to capture information from the employee/client.

As a note, all systems and procedures in this business process are covered by the DOL's government-wide SORN, DOL-GOVT/1 which was cited earlier.

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

This question does not apply to this system, since it is not the system used to capture information from the employee/client. As a note, all systems and procedures in this business process are covered by the DOL's government-wide SORN, DOL-GOVT/1 which was cited earlier.

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.

All systems and procedures in this business process are covered by the DOL's government-wide SORN, DOL-GOVT/1 which was cited earlier.

Additionally, The Department of Veterans Affairs does provide public notice that the system does exist. This notice is provided in 2 ways:

1) The System of record Notice (SORN) is 86VA00S1 -Workers Compensation Occupational Safety and Health Management Information System (Formally known as 86VA058)-VA. The official system of records notice (SORN) for these can be found on-line at: http://www.gpo.gov/fdsys/pkg/FR-2000-09-14/pdf/00-23569.pdf Amended SORN can be found at: http://www.gpo.gov/fdsys/pkg/FR-2008-08-05/pdf/E8-17899.pdf

2) This document - Privacy Impact Assessment (PIA) also serves as notice of the Workers Compensation Occupational Safety and Health Management Information System, as required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means

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.

Claims are submitted on behalf of the claimant or injured employee. Decision to disclose information is the employee's decision and affects whether or not they will be covered by the OWCP program.

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.

The Individual does not have the right to consent to a particular usage of information due to the reporting requirement for workers' compensation.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

Principle of Transparency: *Has sufficient notice been provided to the individual?*

Principle of Use Limitation: *Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?*
This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.
Follow the format below:

Privacy Risk: There is a risk that members of the public may not know that the WCP system exists within the Department of Veterans Affairs. The risk also exists that the information within the system could be used for an unauthorized purpose.

Mitigation: Collection of claimant data is authorized by the Occupational Workers' Compensation Program and has specific uses. There is no other use authorized for this data. As stated in section 4.2, users are required to sign a rules of behavior document which outlines specific uses for the claims data and the penalty which could be imposed as a result of misuse of that data.

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.

Per the DOL's government-wide SORN, DOL-GOVT/1:

Employees seeking information regarding access to and contesting of VA records may write, call, or visit VA's Human Resources Management Office of employment.

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

The system is not exempt from the provisions of the Privacy Act

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

The system is a Privacy Act system.

Per the DOL's government-wide SORN, DOL-GOVT and the RECORD ACCESS PROCEDURES - Employees seeking information regarding access to and contesting of VA records may write, call, or visit VA's Human Resources Management Office of employment.

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.

The information collected by the agency on behalf of the claimant is sent to DOL and becomes DOL data. The WC/OSH-MIS makes no changes to this claimant data. If there is a change that needs to take place it must be changed by DOL, who in turn sends the changes to the VA in the form of the bi-weekly or quarterly file.

In addition, per SORN 86VA00S1 - Workers Compensation Occupational Safety and Health Management Information System (Formally known as 86VA058)-VA states: RECORD ACCESS PROCEDURES: Employees seeking information regarding access to and contesting of VA records may write, call, or visit VA's Human Resources Management Office of Employment

.

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.

All notifications on claimant data occurs either by direct contact from DOL to the individual or through the OWCP Manager to the individual claimant. (SORN) is 86VA00S1 -Workers Compensation Occupational Safety and Health Management Information System (Formally known as 86VA058)-VA which states: CONTESTING RECORD PROCEDURES: See record access procedures above. The SORN states: Employees seeking information regarding access to and contesting of VA records may write, call, or visit VA's Human Resources Management Office of employment.

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 process is provided.

..

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

Privacy Risk: Privacy Risk: There is a risk that individuals may seek to access or redress records about them held by the VA Office and become frustrated with the results of their attempt.

Mitigation: Changes are reported to and made by DOL only. Mitigation: By publishing this PIA, and the applicable SORN, the VA makes the public aware of the unique status of applications and evidence files, such as those stored on the Virtual VA platform. Furthermore, this document and the SORN provide the point of contact for members of the public who have questions or concerns about applications and evidence files. Section 8. Technical Access and Security

.

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?

Individual access is requested via the Agency Administrator who in turn validates that the individual has a legitimate need for access because of their position as documented by the System Security Plan. Once the need is established and verified, the Agency Administrator enters them into the system via the application. All users, regardless of whether they are in the agency or contracted to do case investigation, must be approved by the Agency Administrator. Additionally, all users are required to sign a Rules of Behavior.

8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

Users from other agencies do not have access to the system

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

‘Read-only’ access gives read-only compartmentalized access within the agency or agencies which the user is assigned. ‘Data-entry’ gives read/write compartmentalized access within the agency or agencies which the user is assigned. ‘Agency administrator’ gives read/write access within the agency or agencies which the user is assigned. ‘System administrator’ gives read/write access. Per VA Directive and Handbook 6330, every 5 years the Office of Information Technology (OIT) develops, disseminates, and reviews/updates a formal, documented policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; along with formal, documented procedures to facilitate the implementation of the control policy and associated controls

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.

Access to contractors is limited to development/system administration and public trust is required. VA contract employee access is verified through the Contracting Officer’s Representative (COR) and other VA supervisory/administrative personnel before access is granted to any VA system. Contractor access is reviewed annually at a minimum. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of behavior training via the VA Talent Management System (TMS). All contractors are vetted using the VA background investigation process and must obtain the appropriate level background investigation for their role. Contractors with systems administrative access are required to complete additional role-based training prior to gaining system administrator access. Generally, contracts are reviewed at the start of the initiation phase of acquisitions and again during procurement of option years by the Contracting Officer, Information Security Officer, Privacy Officer, COR, Procurement Requestor/Program Manager and any other stakeholders required for approval of the acquisition. Contracts generally have an average duration of 1-3 years and may have option years stipulated in the original contract.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately. This question is related to privacy control AR-5, Privacy Awareness and Training.

Personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the VA Privacy and Security Awareness training which all personnel must complete via the VA's Talent Management System (TMS). The TMS courses are *TMS 10176 VA Privacy and Information Security Awareness and Rules of Behavior* and *TMS 10203 Privacy and HIPAA Training.*

After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the privacy and security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system. 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. System administrators are required to complete additional role-based training. Users with access to PHI are required to complete HIPAA privacy training annually

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Current
2. *The System Security Plan Status Date:* Security Plan Status is current on May 10, 2023
3. *The Authorization Status*: Yes, Authority To Operate was granted
4. *The Authorization Date:* July 16, 2023
5. *The Authorization Termination Date* July 15, 2025
6. *The Risk Review Completion Date:* December 29, 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.***

Not applicable

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)*

This system does not use cloud technology.

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.*

This system does not use cloud technology.

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.

This system 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.

This system 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).

This system does not utilize Robotics Process Automation (RPA).

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

ID	Privacy Controls
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.

GINA SIEFERT Digitally signed by GINA SIEFERT
Date: 2024.07.23 10:29:18 -05'00'

Privacy Officer, Gina Siefert

GRISELDA GALLEGOS Digitally signed by GRISELDA GALLEGOS
Date: 2024.07.24 14:22:13 -05'00'

Information System Security Officer, Griselda Gallegos

TIFFINEY BENTON Digitally signed by TIFFINEY BENTON
Date: 2024.07.23 09:13:01 -04'00'

Information System Owner, Tiffiney Benton

APPENDIX A-6.1

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

This is not applicable since the system does not collect information directly from the individual.

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