Privacy Impact Assessment for the VA IT System called:

# CLAIMS Assessing

# VETERANS HEALTH ADMINISTRATION (VHA)

# Compensation and Pension Product Line

Date PIA submitted for review:

09/05/2023

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) | Karen McQuaid | Karen.McQuaid@va.gov | 708-724-2761 |
| Information System Owner | Christina Lawyer | Christina.Lawyer@va.gov | 518-210-0581 |

## Abstract

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

The CLAIMS Authentication server, housed at Philadelphia ITC , is essential to the authorization and authentication processes used by applications that require Veterans Health Information Systems and Technology Architecture (VistA) login authentication and credentials. It supports Compensation and Pension Record Interchange (CAPRI) connectivity by users from multiple program offices through the CAPRI system to all VAMCs, allowing the setup and performance of the Compensation and Pension exams. It supports the Joint Legacy Viewer (JLV), a graphical user interface (GUI) that links the Veteran Affairs (VA) electronic medical record (EMR) systems with the Department of Defense (DoD) EMR systems. CLAIMS also supports WebVRAM which facilitates Community of Care office staff, provider and clinician access to multiple remote Veterans Health Information Systems and Technology Architecture (VistA)\ Fee Basis Claims System (FBCS) and related business applications without requiring physician users to establish login authentication and credentials at each VistA where Veteran clinical data is related to the Veteran and includes all data associated with that Veteran that would be required to provide any clinical care.

## 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.*
CLAIMS Assessing [Compensation and Pension C&P]

*B. The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
CLAIMS Assessing, housed at Philadelphia Information Technology Center (PITC), is critical to the functioning of the Compensation and Pension Record Interchange (CAPRI). It supports connectivity by users from multiple program offices through the CAPRI system to all VAMCs, allowing the setup and performance of the Compensation and Pension exams, and to interface with VBA. Current applications include CAPRI, JLV, and Web VRAM.

*C. Indicate the ownership or control of the IT system or project.*
The CLAIMS Assessing system is VA Owned and Operated.

*2. Information Collection and Sharing*

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

CLAIMS is an authentication server. Any information stored in the CLAIMS database is solely for authenticating purposes.

*E. A general description of the information in the IT system and the purpose for collecting this information.*
Name, Social Security number, Date of Birth, IP Address numbers. These are used solely for authenticating purposes

*F. Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
CLAIMS do not share any information. CLAIMS is an authentication server.

*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 CLAIMS Authentication server is operated in one site, Philadelphia ITC

*3. Legal Authority and SORN*

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

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 10 U.S.C. chapters 106a, 510, 1606 and 1607 and title 38, U.S.C. § 501(a) and Chapters 3, 11, 13, 15, 18, 19, 21, 23, 30, 31, 32, 33, 34, 35, 36, 37, 39, 51, 53, 55 and 77. Title 5 U.S.C. 5514.

https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

SORN number, 58VA21/22/28 / 86 FR 61858
SORN Title: Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA
SORN from the OPRM site. 2021-24372.pdf (govinfo.gov)
(https://www.oprm.va.gov/privacy/systems_of_records.aspx)

*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

*4. System Changes*

*J. Whether the completion of this PIA will result in circumstances that require changes to business processes*
No

*K. Whether 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.*

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)

Additional Information Collected but Not Listed Above:
1. Network Username
2. Email address
3. Phone number
4. Identity and Access Management Unique User ID
5. Identity and Access Management Active Directory User Principal Name (AD UPN)

**PII Mapping of Components (Servers/Database)**

CLAIMS consists of no key components servers or databases. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by CLAIMS and the reasons for the collection of the PII are in the table below.

Based on the CLAIMS PTA (section 3.9), there are no internal database connections.

**Note**: Due to the PIA being a public facing document, please do not include the server names in the table.

*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 |
|---|---|---|---|---|---|
| N/A | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

**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?*

This question is N/A to CLAIMS.

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

This question is N/A to CLAIMS.

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

This question is N/A to CLAIMS.

**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?*

CLAIMS is an authentication server and does not collect information directly from individuals, received via electronic transmission from another system.

*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.*

CLAIMS does not collect any forms and is not subject to Paperwork Reduction Act.

**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.*

CLAIMS does not have any information store in the system that is checked for accuracy.

*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.*

CLAIMS does not check for accuracy by accessing a commercial aggregator of information.

**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*

CLAIMS is an Authentication Server that operates as an instance of VistA. VistA instances operate under the authority of Veterans' Benefits, Title 38, United States Code (U.S.C.), Chapter 5, § 501(b), and Veterans Health Administration – Organization and Functions, Title 38, U.S.C., Chapter 73, § 7301(a)
SORN number, 58VA21/22/28 / 86 FR 61858
SORN Title Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA, and the SORN from the OPRM site. 2021-24372.pdf (govinfo.gov)
https://www.oprm.va.gov/privacy/systems_of_records.aspx

**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:**
CLAIMS is an Authentication Server. PII is used by application users (CAPRI, JLV, Web VRAM) to authenticate and gain access to VistA applications. Due to this, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious harm or even identity theft may result.

**Mitigation:**
CLAIMS deploys security measures to protect the information from inappropriate use and/or disclosure through both access controls and training of all employees and contractors. CLAIMS security measures include access control, configuration management, audit and accountability

measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information integrity, security assessment and authorization, incident response, risk assessment, planning and maintenance.

## 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.*

The records and information (e.g.)
• Name - Application User
• Social Security Number - Application User-Identifier
• Date of Birth - Application User-Identifier
• Internet Protocol (IP) Address Numbers- Used to communicate Network Username – Username on CLAIMS system

CLAIMS is an Authentication Server. PII is used by application users (CAPRI, JLV, Web VRAM) to authenticate and gain access to VistA applications.

**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.*

CLAIMS is an authentication system and does not conduct and analyze data.

*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.*

CLAIMS does not create or make available new or previously unutilized information about an individual or individuals since it is an authentication system.

### 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?*

CLAIMS is an Authentication Server. Encryption at rest. Users never leave the VA network; encryption is across the MPLS WAN.

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

Any users accessing CLAIMS are within the VA network. CLAIMS has controls in place which provides access to only those who have a need to know and those who create and maintain accounts for users. All data is encrypted, at rest and in-transit to VA standards utilizing FIPS 140-2 compliant Advanced Encryption Standard (AES) encryption algorithm.

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

PII is safeguarded within the VA Network. CLAIMS is not a forward-facing system.

### 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?*

CLAIMS is an Authentication Server. PII is used by application users (CAPRI, JLV, Web VRAM) to authenticate and gain access to VistA applications. Access to PII by CLAIMS administrators are determined by their roles and responsibilities which are granted by elevated privileges.

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

All access requires an Electronic Permission Access System (EPAS) request. Any procedures and documentation are in eMASS under artifacts or answered via AC controls.

*2.4c Does access require manager approval?*

Yes, via EPAS. All EPAS requests get routed for manager approval.

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

Only CLAIMS administrators can access the PII. Elevated privileges are required for this access, and it is granted/approved through EPAS.

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

CLAIMS is an Authentication Server. PII is used by application users (CAPRI, JLV, Web VRAM) to authenticate and gain access to VistA applications. CLAIMS PII is strictly for credential/access to VistA Instances.

## Section 3. Retention of Information

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

**3.1 What information is retained?**

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

• Name
• Social Security Number
• Date of Birth
• Internet Protocol (IP) Address Numbers
• Network Username

**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. 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.*

This control is inherited for CLAIMS from T1SOR. The VA defines the time for retaining each collection of PII that is required to fulfill the purpose(s) identified in the published privacy notice or required by law as 'in accordance with National Archives and Records Administration (NARA) approved General Records Schedules and/or Agency Record Control Schedules.' CLAIMS is an instance of VistA and follows their guidance of 75 years.

**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?*

CLAIMS is an Authentication Server. PII is used by application users (CAPRI, JLV, Web VRAM) to authenticate and gain access to VistA applications. CLAIMS PII is strictly for credential/access to VistA Instances. There are no records stored and CLAIMS is not a system of record.

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

Records Control Schedule VB–1, Part 1 Section XIII, Item 13–052.100 as authorized by NARA.

**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.*

There are no records stored and CLAIMS is not a system of record. CLAIMS is housed in PITC and will follow their policy and procedure for any electronic destruction. The VA defines the techniques or methods to be employed to ensure the secure deletion or destruction of PII (including originals, copies, and archived records) as 'Paper Records: Pulping, maceration, shredding and others that ensure that records are not readable or reconstruct able to any degree. Other Records: In accordance with the disposition instructions from approved National Archives and Records Administration (NARA) General Records Schedule and/or Agency Record Control Schedules.'

**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.*

There is no research, testing, or training done. CLAIMS is an Authentication Server only.

**3.6 <u>PRIVACY IMPACT ASSESSMENT: Retention of information</u>**

*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:*

*<u>Principle of Minimization:</u> 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?*

*<u>Principle of Data Quality and Integrity:</u> 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:

**<u>Privacy Risk:</u>**

There is a risk that PII contained in the CLAIMS will be retained for longer than is necessary to fulfill the VA mission. PII held longer than required are at greater risk of being unintentionally released or breached**.**

**Mitigation:**
The VA defines the techniques or methods to be employed to ensure the secure deletion or destruction of PII (including originals, copies, and archived records) as 'Paper Records: Pulping, maceration, shredding and others that ensure that records are not readable or reconstruct able to any degree. Other Records: In accordance with the disposition instructions from approved National Archives and Records Administration (NARA) General Records Schedule and/or Agency Record Control Schedules.'

## 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*** |
|---|---|---|---|
| N/A | | | |

**4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure**

*Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).*

*This question is related to privacy control UL-1, Internal Use.*

Follow the format below: N/A

**Privacy Risk:**
Based on the CLAIMS PTA (section 3.9), there are no Data Shared with internal organizations.
This question is N/A to CLAIMS

**Mitigation:**
Based on the CLAIMS PTA (section 3.9), there are no Data Shared with internal organizations.
This question is N/A to CLAIMS

## Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

*Data Shared with External Organizations*

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

## 5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

Follow the format below: n/a

**Privacy Risk:**
Based on the CLAIMS PTA (section 3.10), CLAIMS does not connect, receive, or share PII/PHI with any other external (outside of VA) organization, IT system, third-party website, or application.
This question is N/A to CLAIMS

**Mitigation:**
Based on the CLAIMS PTA (section 3.10), CLAIMS does not connect, receive, or share PII/PHI with any other external (outside of VA) organization, IT system, third-party website, or application.
This question is N/A to CLAIMS

## 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.*

The Notice of Privacy Practice (NOPP) is a document which explains the collection and use of protected information to individuals applying for VHA benefits. The NOPP is giving out when the Veteran enrolls or when updates are made to the NOPP copies are mailed to all VHA beneficiaries. Employees and contractors are required to review, sign, and abide by the National Rules of Behavior on an annual basis. https://www.va.gov/VHAPublications/ViewPublication.asp?pub_ID=1090

The Department of Veterans Affairs provides additional notice of this system by publishing 2 System of Record Notices (SORNs):

1) The VHA System of Record Notice (VHA SORN) Patient Medical Records-VA, SORN 24VA10P2 (Feb. 11, 2014), in the Federal Register and online. An online copy of the SORN can be found at: https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

2) The VHA System of Record Notice (VHA SORN) Veterans Health Information System and Technology Architecture (VISTA) - VA, SORN 79VA10 in the Federal Register and online. An online copy of the SORN can be found at: https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf

This Privacy Impact Assessment (PIA) also serves as notice of the CLAIMS 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."

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

CLAIMS is an authentication server and does not store any records.

*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.*

Notice is done through publishing 2 System of Record Notices (SORNs) and the PIA for CLAIMS. See 6.1a for the links.

**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.*

Any information provided to CLAIMS is to support authentication. A user provides their credentials for authentication. If a user does not authenticate, then access is denied.

**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.*

CLAIMS is an Authentication Server. PII is used by application users (CAPRI, JLV, Web VRAM) to authenticate and gain access to VistA applications. CLAIMS PII strictly for credential/access to VistA Instances. There is no information use, just identifiers.

**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:**
CLAIMS is an Authentication Server. PII is used by application users (CAPRI, JLV, Web VRAM) to authenticate and gain access to VistA applications.

**Mitigation:**
Users of CLAIMS are internal to the VA network. We rely on VA Policy and training to ensure any user has proper credentials and is current in any training.

## 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.***

There is no information to gain access to. There are no patient data/records in CLAIMS. CLAIMS is an Authentication Server. PII is used by application users (CAPRI, JLV, Web VRAM) to authenticate and gain access to VistA applications.

*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).*

CLAIMS is exempt because it is an authentication server and does not have patients' data or records.

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

CLAIMS is not a Privacy Act system and does not have any procedures or regulations in place that covers an individual gaining access to their information.

**7.2 What are the procedures for correcting inaccurate or erroneous information?**

*Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed. If the correction procedures are the same as those given in question 7.1, state as much. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.*

CLAIMS is an authentication server and does not provide procedures for correcting inaccurate or erroneous information.

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

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

CLAIMS is an authenticator and does not inform individuals of the procedures for correcting their information.

**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.*

CLAIMS is a pass-through system, an authentication server and does not perform these specific processes or programs.

**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 considering 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: n/a

**Privacy Risk:**
CLAIMS is an Authentication Server. PII is used by application users (CAPRI, JLV, Web VRAM) to authenticate and gain access to VistA applications.

**Mitigation:**
CLAIMS is an authentication server and does not provide individuals ability to find out whether a project maintains a record relating to them.

## Section 8. Technical Access and Security

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

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

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

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

Access to the system for operational purposes is requested via ePAS submission of the VHA NDS Access Form for Health Operations form along with supervisory approval, NDS approval, and

completion of required TMS training. Access to the system for research purposes is requested via DART along with a research request memo, IRB approval, Real SSN Access Request approval, and completion of required TMS training.

*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?*

CLAIMS does not provide access to other government agencies. CAPRI/JLV which utilizes the CLAIMS system for authentication, does not have the ability to limit access to time or content within the Electronic Health Record (EHR). Access is granted on the criteria that the user will have access to the complete EHR. We do limit access to certain user groups to only individuals that have the authority to view a specific EHR. For example, Veteran Service Officers are assigned restricted lists to only view the EHR of the Veterans they have power of attorney for.

*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.*

CAPRI/JLV provides read-only access to the EHR and does not provide access to write to the EHR.

**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.*

Contracts are reviewed based on the contract guidelines by the appropriate contract authority (i.e., COR, Contracting Officer, Contract Review Committee). Contractors will sign BAA and NDA's when required.
Per specific contract guidelines, contractors can have access to the system only after completing mandatory information security and privacy training, VHA HIPAA training as well as the appropriate background investigation to include fingerprinting. Certification that this training has been completed by all contractors must be provided to the VHA employee who is responsible for the contract in question. In addition, all contracts by which contractors might access sensitive patient information must include a Business Associate Agreement which clarifies the mandatory nature of the training and the potential penalties for violating patient privacy.
Contractors with CLAIMS access must have an approved electronic request on file and access reviewed with the same requirements as VHA employees.

**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 VA employees/Contractors who have access to VA computers must complete the onboarding and annual mandatory privacy and information security training. In addition, all employees/contractors with access to VHA computer systems must complete the VHA mandated Privacy and HIPAA Focused raining. Finally, all new employees receive face-to-face/virtual training by the facility Privacy Officer and Information Security Officer during new employee orientation. The Privacy and Information Security Officer also perform subject specific trainings on an as needed basis.

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

*8.4a If Yes, provide: pull from eMASS*

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 02-Jun-2023
3. *The Authorization Status:* 2-year ATO
4. *The Authorization Date:* 12-Aug-2023
5. *The Authorization Termination Date:* 14-Aug-2025
6. *The Risk Review Completion Date:* 21-Nov-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)*

No

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

N/A

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

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

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

N/A

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

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

N/A

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

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

N/A

## Section 10. References

Summary of Privacy Controls by Family

*Summary of Privacy Controls by Family*

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

| ID | Privacy Controls |
|---|---|
| UL-1 | Internal Use |
| UL-2 | Information Sharing with Third Parties |

**Signature of Responsible Officials**

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

LAKISHA V WRIGHT 111646

Digitally signed by LAKISHA V WRIGHT 111646
Date: 2023.09.22 13:24:57 -04'00'

**Privacy Officer, Lakisha Wright**

KAREN MCQUAID

Digitally signed by KAREN MCQUAID
Date: 2023.09.20 08:12:01 -05'00'

**Information Systems Security Officer, Karen McQuaid**

Christina O. Lawyer 141790

Digitally signed by Christina O. Lawyer 141790
Date: 2023.09.20 07:48:30 -04'00'

**Information Systems Owner, Christina Lawyer**

## 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).

SORN number, 58VA21/22/28 / 86 FR 61858
SORN Title: Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA
SORN from the OPRM site. 2021-24372.pdf (govinfo.gov)
(https://www.oprm.va.gov/privacy/systems_of_records.aspx)

**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

**Notice of Privacy Practice (NOPP):**

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices