Privacy Impact Assessment for the VA IT System

VA Okta Identity as a Service (IDaaS) Assessing -E

VA Central Office (VACO)
Product Engineering Services (PES), Identity Credential and Access Management (ICAM)

eMASS ID #0176

Date PIA submitted for review:

08/28/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Julie Drake	Julie.drake@va.gov OITPrivacy@va.gov	(202) 632-8431
Information System Security Officer (ISSO)	Mary Reifers	Mary.reifers@va.gov	605-254-4367
Information System Owner	Craig W. Davis	Craig.davis1@va.gov	407-840-2475

Abstract

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

VA OKTA -E: Okta Identity as a Service (IDaaS) Assessing -E is a Software as a Service cloud service provider and is an identity management system used to validate identity of users that need to access VA applications.

Overview

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

1 *General Description*

A. *What is the IT system name and the name of the program office that owns the IT system?*

VA Okta Identity as a Service (IDaaS) Assessing -E; Product Engineering Services (PES) Identity Credential and Access Management (ICAM)

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

Okta is a cloud-based SaaS; hosted in AWS Government Cloud East under FedRAMP, Okta supports the VA performing authentication and access management for multiple applications and systems within the VA for both internal/workforce and external/Veteran use cases. The system is an on-demand identity and access management service that enables enterprises to accelerate the secure adoption of the web-based applications, both in the cloud and behind the firewall. The Okta core service is web-based SaaS identity platform. Users interact with Okta via web browser or APIs that have been integrated into 3rd party applications to access VA systems.

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

The system is VA Controlled & non-VA Owned and Operated.

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 Okta WIC feature is presently used by Enterprise Cloud Solutions Office (ECSO) to support Cloud Computerized Patient Record System (CPRS) using MFA and by Office of Chief Technology Officer (OCTO) for authentication to tools supported by DevOps Tools Suite (DOTS) for approximately 32,000 active VA employed Monthly Access Users (aMAU).

VA is currently licensed for 1,100,000 Okta CIS aMAUs for the support of non-VA employee users which primarily supports Veteran & Caregiver facing authentications.

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

Workforce authentication data elements are collected to validate, streamline and enhance security for VA internal workforce users to access VA systems. The general information collected during workforce authentication includes:

- Name
- Work Email Address
- Certificate/License number: VA Provider
- DoD Electronic Data Interchange Personal Identifier (EDIPI)

Customer authentication data elements are collected to validate, streamline and enhance security for external (e.g. Non-VA workforce) users to access VA systems. The general information collected during workforce authentication includes:

- Name
- Personal Email Address

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

Okta Workforce Identity Cloud (WIC) subsystem currently provides a seamless and secure sign-on experience for VA internal workforce users into VA applications. It allows users to authenticate with Personal Identity Verification (PIV) or Authentication Assurance level (AAL) 2/AAL3 compliant authentication factors when accessing applications.

Okta Customer Identity Services (CIS) subsystem, as currently deployed, allows VA to provide a seamless and secure identity experience for external users such as Veterans and caregivers as well as developers that create digital products on behalf of VA. It allows for self-service registration, social login, identity verification, and consent management.

The Okta Application Server subsystem is critical in providing functionality for authentication operations. This system manages user authentications, session handling and API requests to ensure secure access to applications. It enforces security policies like multi-factor authentication and access controls while integrating with other subsystems (e.g. WIC, CIS, Database). This component acts as an intermediary, ensuring that only authorized users can access protected resources and maintaining secure interactions across all internal modules.

The Database subsystem supports the Application subsystem by storing and retrieving critical identity and access information. This includes user profiles, authentication data, session information, access control policies, and application configurations. Then the application server processes authentication requests or enforces security policies, it queries the database to validate user credentials, and check permissions. The database forms the foundation for reporting and compliance.

G. Is the system 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?

Okta has one cloud instance and is used enterprise wide. Data is stored in the FedRAMP cloud service provider (CSP) database. VA OKTA operates under the FedRAMP ATO, OKTA has obligations under this Master Subscription Terms to protect Customer Data and if it breaches the agreement then the VA can seek legal remedies. Okta has strong measures in place to prevent disclosure of privacy related data, in addition the VA is in full control of what data is entered their OKTA tenant. The magnitude of the harm would be determined at the time of incident.

3. Legal Authority and SORN

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

VA OKTA is provided under –Public Law 114-31; Veteran Information: Title 38, United States Code, Section 5107, Title 38, United States Code, Section 5106, and Title 38 United States Code 5701. 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. "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." E-government Act of 2002 (44 U.S.C. §208(b)). 38 United States Code 5706.

The SORN that will cover veterans/dependents is:
138VA005Q / 87 FR 79066 Veterans Affairs/Department of Defense Identify Repository (VADIR)-VA (12/23/2022)
https://www.oprm.va.gov/docs/SORN/Current_SORN_List_09_19_2022.pdf

The SORN that will cover VA Employee and VA Contractor is:
146VA005Q3/73 FR 16093 Department of Veterans Affairs Identity Management System (VAIDMS)-VA (3/26/2008) https://www.govinfo.gov/content/pkg/FR-2008-03-26/pdf/E8-6120.pdf

VA SORN that covers health information is:
168VA005 / 86 FR 6975 SYSTEM NAME: Health Information Exchange-VA (1/25/2021)
https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01516.pdf

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 SORNs listed above are not being modified.

4. System Changes

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

No changes to business processes will result from completion of this PIA.

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

No changes to technology will result from completion of this PIA.

Section 1. Characterization of the Information

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

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

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

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

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

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

☒ Name
☐ Social Security Number
☐ Date of Birth
☐ Mother's Maiden Name
☐ Personal Mailing Address
☐ Personal Phone Number(s)
☐ Personal Fax Number
☒ Personal Email Address
☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
☐ Financial Information
☐ Health Insurance Beneficiary Numbers Account numbers
☒ Certificate/License numbers[1]
☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☐ Medications
☐ Medical Records
☐ Race/Ethnicity
☐ Tax Identification Number
☐ Medical Record Number
☐ Gender
☐ Integrated Control Number (ICN)
☐ Military History/Service Connection
☐ Next of Kin
☒ Other Data Elements (list below)

Other PII/PHI data elements: None

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

- Business Email Address
- DoD Electronic Data Interchange Personal Identifier (EDIPI)

PII Mapping of Components (Servers/Database)

Okta -E 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 Okta -E and the reasons for the collection of the PII are in the table below.

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

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection / Storage of PII	Safeguards
Application Server	No	Yes	Name Email Address (Personal or Business) Certificate/License number: VA Provider DoD Electronic Data Interchange Personal Identifier (EDIPI)	Verify identity	Hosted in the Cloud and managed by Digital transformation Center (DTC). Controlled physical and logical access, only approved and authorized users granted access to application.
Data Database	Yes	Yes	Name Email Address (Personal or Business) Certificate/License number: VA Provider DoD Electronic Data Interchange Personal Identifier (EDIPI)	Verify identity	Hosted in the AWS Cloud, controlled physical and logical access, only approved and authorized users granted access to database.

Okta Workforce Identity Cloud (WIC)	YES	YES	Name Personal Email Address Email Address (Personal or Business) Certificate/License number: VA Provider DoD Electronic Data Interchange Personal Identifier (EDIPI)	Verify identity	Hosted in the AWS Cloud, controlled physical and logical access, only approved and authorized users granted access to database.
Okta Customer Identity Services (CIS)	YES	YES	Name Personal Email Address Email Address (Personal or Business) Certificate/License number: VA Provider DoD Electronic Data Interchange Personal Identifier (EDIPI)	Verify identity	Hosted in the AWS Cloud, controlled physical and logical access, only approved and authorized users granted access to database.

1.2 What are the sources of the information in the system?

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

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

Users will enter information in VA OKTA instance. subjects name, address and email address. VA OKTA will provide all the information to the VA application/system for use with authenticating and allowing access.

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 not required from other sources.

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

This system does not create information.

1.3 How is the information collected?

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

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

The means of data collection will be directly from the individual. User accesses SaaS web application and enters information directly.

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?

Information is not collected on a form. Notice is provided to individual upon entering any information into VA OKTA. It reinforces to the user that any information they enter into form-fields on the SaaS/IDaaS will be collected. Please see Appendix A for an example. Also, notice is provided within this PIA and the governing SORN.

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.

All information will be collected from the individual and is considered accurate. VA OKTA will validate identity using VA Master Person Index or Active Directory Service. The individual user will identify the VA applications/systems to share information with to using MPI or AD as part of the identity management and user authorization process. Information received and displayed from other VA systems is considered accurate.

1.4b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?

The system does not use a commercial aggregator.

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

VA OKTA is provided under –Public Law 114-31; Veteran Information: Title 38, United States Code, Section 5107, Title 38, United States Code, Section 5106, and Title 38 United States Code 5701. 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. "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." E-government Act of 2002 (44 U.S.C. §208(b)). 38 United States Code 5706.

The SORN that will cover veterans/dependents is:
138VA005Q / 87 FR 79066 Veterans Affairs/Department of Defense Identify Repository (VADIR)-VA (12/23/2022)
https://www.oprm.va.gov/docs/SORN/Current_SORN_List_09_19_2022.pdf

The SORN that will cover VA Employee and VA Contractor is:
146VA005Q3/73 FR 16093 Department of Veterans Affairs Identity Management System (VAIDMS)-VA (3/26/2008) https://www.govinfo.gov/content/pkg/FR-2008-03-26/pdf/E8-6120.pdf

VA SORN that covers health information is:
168VA005 / 86 FR 6975 SYSTEM NAME: Health Information Exchange-VA (1/25/2021) https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01516.pdf

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?

This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

Privacy Risk: Data collected by the OKTA application contains PII, and other sensitive information. The risk is collection of inaccurate data which could lead to denial of system access.

Mitigation: OKTA ensures strict access to information by enforcing thorough access control and requirements for end users. When data is received from the individual and verified through OIT Identity and Access Management (IAM) Active Directory Services (AD) and OIT Identity and Access Management (IAM) Master Person Index (MPI), if that data is incorrect, access is denied. As part of the access management activities, the highest level of assurance for providing identity along with multi-factor authentication will be used. Individuals who suspect inaccurate data can contact the support staff as identified on the error message for assistance to correct data elements.

The collection of logon information for access to VA applications is a critical component of ensuring secure, efficient, and effective delivery of services to veterans. It supports the VA's mission by safeguarding sensitive information, enhancing service quality, preventing fraud, improving user experience, and enabling data-driven decision making.

The VA's mission includes providing high-quality healthcare, benefits, and services to veterans. Ensuring that only authorized individuals can access these services is crucial to maintaining the integrity and confidentiality of veteran data.

The program collects information directly from individuals whenever it is possible and practical. This approach ensures accuracy and relevance, as the data comes straight from the source, allowing for more personalized and accurate outcomes for authentication processing.

The Department of Veterans Affairs (VA) has several policies in place to ensure that personally identifiable information (PII) is accurate, complete, and current:

VA Directive 6502 – which includes 1.) Data Quality Principles to emphasize the importance of maintaining accurate, complete and up to date PII; 2.) Periodic Reviews which mandates regular reviews of PII to ensure its accuracy and relevance.

VA Handbook 6500 – which includes 1.) Data Integrity Controls to validate processes and check the accuracy of data entries and prevent unauthorized modifications. 2.) Auditing and Monitoring policies to detect and correct any discrepancies or inaccurate PII.

These policies and practices collectively ensure that the VA maintains high standards for the accuracy, completeness, and currency of PII.

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.

VA OKTA will be used to gather information in order to verify identity for use with authentication and accessing authorized VA applications/systems.

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	Verify identity	Not used
Email address (Business)	Verify identity	Not used
Email address (Personal)	Verify identity	Not used
Certificate/License #: VA Provider	Verify identity	Not used
Electronic Data Interchange Personal Identifier (EDIPI)	Verify identity	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?

This system does not process or analyze the data submitted. The data provided is used to produce the identity management information needed to verify identity and authenticate users for accessing authorized VA applications/systems.

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 individuals.

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?

Okta uses Transport Layer Security (TLS) to encrypt data transmitted between users and Okta service, as well as between Okta and any integrated applications. This ensures that data in-transit is protected from interception and eavesdropping. In addition, Okta adheres to the Federal Risk and Authorization Management Program (FedRAMP) with a FedRAMP Moderate certification. These standards included stringent security requirements for protection of data both in-transit and at rest. These standards ensure that Okta's data protection practices meet federal guidelines.

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

No SSNs are collected.

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

To safeguard Protected Health Information (PHI) and Personally Identifiable Information (PII) in accordance with OMB Memorandum M-06-15, Okta has implemented the following measures leveraging the protections described above:

Strong Encryption: Okta's use of Transport Layer Security (TLS) for encrypting data in-transit ensures that PHI and PII are protected from interception. This meets the requirement to encrypt data when transmitted over public networks, as outlined in the OMB memorandum.

Data Integrity and Authentication: By employing mutual TLS (mTLS), Okta can authenticate both parties in a data exchange, ensuring that PHI and PII are transmitted between verified entities. This helps prevent unauthorized access and data tampering.

Access Controls and User Authentication: Okta's stringent access controls and multi-factor authentication (MFA) mechanisms help ensure that only authorized users can access PHI and PII. This aligns with OMB M-06-15's emphasis on protecting data from unauthorized access.

FedRAMP Compliance: Okta's adherence to FedRAMP moderate standards means that it complies with rigorous security and privacy controls that are crucial for protecting sensitive information like PHI and PII. These controls include measures for incident response, continuous monitoring, and vulnerability management.

Secure API Communication: By ensuring all API communications are encrypted using TLS, Okta safeguards PHI and PII when interfacing with other services and applications, protecting data integrity and confidentiality.

Continuous Monitoring and Incident Response: Okta's continuous monitoring for security threats and its incident response plan allow for the quick identification and mitigation of any breaches involving PHI and PII. This proactive approach is essential for maintaining data security and compliance with federal guidelines.

Regular Audits and Compliance Checks: Regular audits and compliance checks, as part of Okta's FedRAMP compliance, ensure that security measures are consistently applied and effective in protecting PHI and PII. These audits help identify any potential vulnerabilities and ensure ongoing adherence to OMB M-06-15 requirements.

Endpoint Security: Securing endpoints involved in the transmission of PHI and PII, through encryption and secure configurations, prevents unauthorized access and data breaches at the device level.

By implementing these measures, Okta can effectively safeguard PHI and PII in accordance with OMB Memorandum M-06-15, ensuring the confidentiality, integrity, and security of sensitive information.

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?

Access to the system is governed by a need to know. All those with access have been trained in Privacy and Information Security and have signed Rules of Behavior and are required to comply with VA Directive 6001.

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

VA OKTA operates under the OIT Standard Operating Procedure (SOP), Infrastructure Operations, Network Operations Network Access Control procedures. It also adheres to National Institutes of Standards and Technology (NIST) Special Publication 800-83, and VA 6500 directives in order to protect confidentiality, integrity and availability of the information processed, stored and transmitted. As a FedRAMP Medium SaaS system with approved Authority to Operate (ATO), there are numerous procedure & controls in place inclusive of System Security Plan, Configuration Management Plan, RMF Plan of Action and others relative to access controls. 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; system and information integrity; and privacy.

2.4c Does access require manager approval?

For non-VA users, there is not a requirement for manager approval. Non-VA employees who access VA applications, such as My HealtheVet, face specific restrictions. They are generally limited to certain roles, such as caregivers or family members with the veteran's permission. Their access is restricted to specific functionalities, such as viewing health records, communicating with healthcare providers, or managing appointments. They must comply with VA's privacy and security policies, including protecting sensitive information and only using the system for authorized purposes. Unauthorized access or misuse can result in penalties or revoked access.

VA Employees require manager approval for access to VA information systems per VA policy. VA employees are bound by VA Directive 6500 and other policies that define role-based access to VA systems. These requirements ensure that access is granted based on necessity, security, and adherence to policy, safeguarding government systems and data.

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

Yes, access is tracked through logging. Any administrative user's activities are tracked when accessing the system.

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

The responsibility for PII is ultimately that of the Veterans Administration as defined shared between the Okta Cloud Service Provider (CDP) and the VA. Although Okta Software as a Service (SaaS) platform meets FedRAMP Medium standards the government agency remains responsible for protecting the PII it manages within the platform. The Accountable Official identified in the Authority to Operate (ATO) bears final authority for PII monitoring. Overall, VA Directive 6502 is applicable to all employees and provides guidance for protecting PII and ensuring compliance with privacy laws, regulations, and policies. The directive applies to all VA employees, contractors, and anyone else who handles PII on behalf of the VA.

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
Email address (Personal)
Email address (Business)
Certificate/License Number: VA Provider
DOD Electronic Data Interchange Personal Identifier (EDIPI).

3.2 How long is information retained?

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

VA OKTA information is retained for 60 days.

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

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

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

Yes, **GRS 3.2, Item 030** System access records.

3.3b Please indicate each records retention schedule, series, and disposition authority?
NARA-General Record Schedule: https://www.archives.gov/records-mgmt/grs.html

GRS 3.2, Item 030 System access records. These records are created as part of the user identification and authorization process to gain access to systems. Records are used to monitor inappropriate systems access by users.
Systems not requiring special accountability for access. These are user identification records generated according to preset requirements, typically system generated.
NOTE VA OKTA information is retained for 60 days
Disposition Instruction: Temporary. Destroy when business use ceases.
Disposition Authority: DAA-GRS 2013-0006 0003

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.

VA OKTA utilizing the OKTA ATO. The information is based on the OKTA environment. All data cached/stored by OKTA is deleted upon reaching the deletion timeframes.

OKTA operates on time-based deletion rules that programmatically triggers a clean-up script. This is in accordance with VA Handbook 6500, Data Minimization and Retention, which states VA will retain PII for only as long as necessary to fulfill the specified purpose(s).

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.

OKTA does NOT use PII/PHI for testing information systems or pre-production prior to deploying to production nor does it utilize PII/PHI for 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: The risk to maintaining data within VA OKTA for a longer time period than what is needed or required is that the longer information is kept, the greater the risk that information will be compromised, unintentionally released or breached.

Mitigation: The system only retains information long enough to process authentication requests. OKTA is housed in a secure Amazon AWS Cloud utilizing the OKTA ATO. The information is based on the OKTA ATO FISMA High environment. All data cached/stored by OKTA is deleted upon reaching the deletion timeframes.

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?

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***
OIT Identity and Access Management (IAM) Master Person Index (MPI)	Purpose is to validate user authentication attributes.	- Name -Email address (Business) -Certificate/License number: VA Provider -DoD Electronic Data Interchange -Personal Identifier (EDIPI)	Simple Object Access Protocol (SOAP) over Hypertext Transfer Protocol Secure (HTTPS) using Secure Socket Layer (SSL) encryption and Certificate exchange
OIT Identity and Access Management (IAM) Active Directory Services (AD)	Purpose is to validate user authentication attributes.	-Name -Email address (Business) -Certificate/License number: VA Provider -DoD Electronic Data Interchange -Personal Identifier (EDIPI)	Simple Object Access Protocol (SOAP) over Hypertext Transfer Protocol Secure (HTTPS) using Secure Socket Layer (SSL) encryption.

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: All parties who have access to the VA system may inappropriately access and misuse the data.

Mitigation: Existing mitigation techniques used to protect privacy from internal sharing and disclosure risks, such as training, system log monitoring and adherence to VA Directive 6500 will suffice as mitigation, since there is no increased risk. Risk increases with the number of people having access to protected information.

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.

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***	***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***	***List the method of transmission and the measures in place to secure data***

	office or IT system		***be more than one)***	
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.

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: No external sharing

Mitigation: N/A

Section 6. Notice

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

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an Appendix-A 6.1 on the last page of the document. Also provide notice given to individuals by the source system (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

6.1a This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the

Federal Register, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

Yes. Notice is provided to Veteran upon entering any information into VA OKTA. It reinforces to the user that any information they enter into form-fields on the SaaS/IDaaS will be collected. Please see Appendix A for an example. Also, notice is provided within this PIA and the governing SORN.

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

A privacy notice is provided. Please see Appendix A for an example.

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.

Privacy notice is provided in appendix A in accordance with the following System of Records Notices (SORN).

The SORN that will cover veterans/dependents is:
138VA005Q / 87 FR 79066 Veterans Affairs/Department of Defense Identify Repository (VADIR)-VA (12/23/2022)
https://www.oprm.va.gov/docs/SORN/Current_SORN_List_09_19_2022.pdf

The SORN that will cover VA Employee and VA Contractor is:
146VA005Q3/73 FR 16093 Department of Veterans Affairs Identity Management System (VAIDMS)-VA (3/26/2008) https://www.govinfo.gov/content/pkg/FR-2008-03-26/pdf/E8-6120.pdf

VA SORN that covers health information is:
168VA005 / 86 FR 6975 SYSTEM NAME: Health Information Exchange-VA (1/25/2021) https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01516.pdf

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress.

Yes, the individual has the right to decline. To verify identity and authentication for access authorized VA applications/systems, the Veteran must use VA OKTA or another approved VA system. There is no penalty for a Veterans refusal; however, we will be unable to verify identity without the information. Information is required to verify identity. Providing information is a basic assumption and requirement of VA OKTA.

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 has the right to consent as outlined within the System of Records Notice (138VA005Q for veterans/dependents and 146VA005Q3 for employees). All requests must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA address outlined in the respective SORN https://department.va.gov/privacy/system-of-records-notices/

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 the Veterans' who provide information to OKTA will not know how their information is being stored in VA OKTA.

Mitigation: A disclaimer will be placed on the VA OKTA landing page outlining the scope of information usage and retention. Notice is published within the Privacy Act, PIA and applicable SORN. Please see Appendix A for an example.

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.***

Individuals may request access to Privacy Act records maintained by requesting a copy using the procedures defined at https://department.va.gov/foia/. All requests to review must be received by direct mail, fax, in person, or by mail referral from another agency or VA office. All requests for access must be delivered to and reviewed by the System Manager for the concerned VA system of records, the facility Privacy Officer, or their designee. Each request must be date stamped and reviewed to determine whether the request for access should be granted.

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.

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

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

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

Individuals have the right to amend their records by submitting their request in writing. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA organization that maintains the record. Information about VA records and contact information can be found at https://www.va.gov/records/ A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VA system of records, and the facility Privacy Officer, or designee, and needs to be date stamped; and filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579.

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.

If an individual has questions pertaining to data submitted to the VA to obtain services, they will follow standard Amendment processes listed within the SORN and this PIA.

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. ***<u>Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.</u>***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

The system will allow user to enter correct information and request access to authorized VA applications/systems.

7.5 <u>PRIVACY IMPACT ASSESSMENT: Access, redress, and correction</u>

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:
<u>Principle of Individual Participation:</u> Is the individual provided with the ability to find out whether a project maintains a record relating to him?

<u>Principle of Individual Participation:</u> 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?

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

Follow the format below:

Privacy Risk: There is risk of inaccurate information being sent to authorized VA credential providers as a result of a Veteran entering incorrect data into VA OKTA.

Mitigation: Individuals are provided notice of how to access, redress and correct information maintained in a VA system of record within the applicable SORN and the PIA. We will monitor user feedback, as well as analyze system data for error rates. Any inaccuracies will be addressed immediately by Veteran either making changes to the information that was entered or by contacting the Veteran via letter sent using the United States Postal Service informing that the request could not be completed because erroneous information was submitted.

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?

VA OKTA uses 2 Factor Authentication mechanism to allow users internal to the VA to access VA systems (e.g., using Personal Identity Verification PIV).

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 government 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.

Server-level access will be managed and granted to developers on an as-needed basis through approved processes using established VA OIT Systems. We will be limiting access to only a small set of trusted developers approved to work with and diagnose production issues. Secure Shell (SSH) access will be logged and monitored.

8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and

Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII. This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.

Contractors will be given access to hosting environment and complete their contractual obligations for ensuring the architecture, and hardware are available; and complies with VA OI&T policy. Contractors will have access to PII or data contained in the system in order to support authentication workflows. Contractors are required to sign VA National Rules of Behavior (ROB) and/or Non-Disclosure Agreements (NDA) as required under contract stipulations.

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.

No additional privacy or security training would be offered specific to the OKTA application. Existing VA privacy and PII trainings are deemed to be sufficient.
VA awareness training program commences with the VA OIT TMS training, *VA Privacy and Information Security Awareness and Rules of Behavior (ROB), number 10176.* Following the training, all information system users will be able to identify the types of information that must be carefully handled to protect privacy; recognize the required information security practices, legal requirements, and consequences and penalties for non-compliance; and explain how to report incidents. The awareness program is consistent, updated and deployed for all employees regularly.

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

8.4a If Yes, provide:

1. *The Security Plan Status: Approved 6/21/2023*
2. *The System Security Plan Status Date: 6/22/2023*
3. *The Authorization Status: Authorization to Operate (ATO)*
4. *The Authorization Date:* 8/18/2023
5. *The Authorization Termination Date: 8/17/2025*
6. *The Risk Review Completion Date:* 8/8/2023
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)*

SaaS through Amazon Web Services (AWS) Government East under FedRAMP

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.*

Okta Government Community Cloud Contract # VA118-16-D-1009
36C10B19N10090016

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.

No, data collected is used solely for the purposes of providing Okta services and is protected though strict security measures.

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.

For information systems that are hosted, operated, maintained, or used on behalf of VA at non-VA facilities, Contractors/Subcontractors are fully responsible and accountable for ensuring compliance with all HIPAA, Privacy Act, FISMA, NIST, FIPS, and VA security and privacy directives and handbooks. This includes conducting compliant risk assessments, routine vulnerability scanning, system patching and change management procedures, and the completion of an acceptable contingency plan for each system. The Contractor's security control procedures must be equivalent to those procedures used to secure VA systems. A Privacy Impact Assessment (PIA) must also be provided to the COR and approved by VA Privacy Service prior to operational approval. All external Internet connections to VA network involving VA information must be in accordance with the TIC Reference Architecture and reviewed and approved by VA prior to implementation. For Cloud Services hosting, the Contractor shall also ensure compliance with the Federal Risk and Authorization Management Program (FedRAMP).

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**
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.

JULIE DRAKE Digitally signed by JULIE DRAKE
Date: 2024.09.09 15:28:40 -04'00'

Privacy Officer, Julie Drake

MARY REIFERS Digitally signed by MARY REIFERS
Date: 2024.09.09 14:44:10 -05'00'

Information Systems Security Officer, Mary Reifers

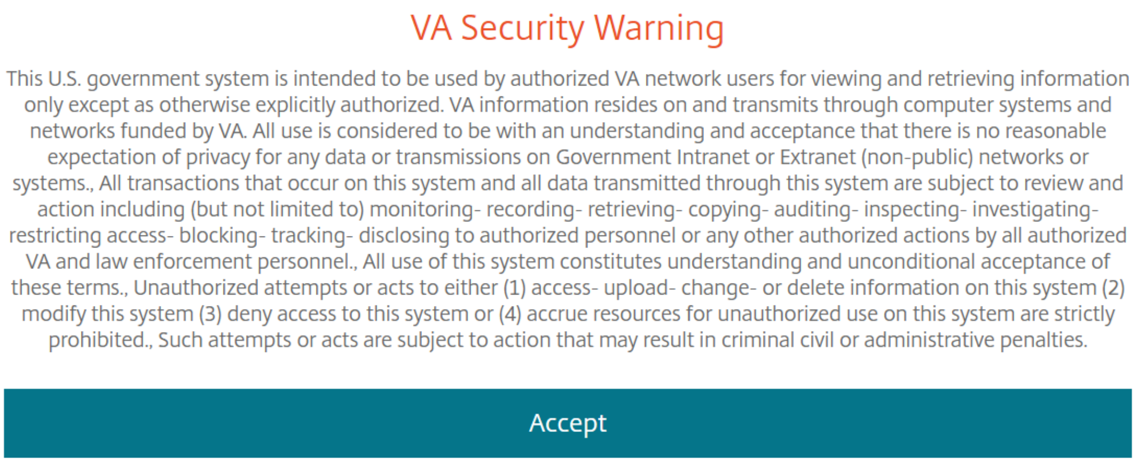
CRAIG DAVIS Digitally signed by CRAIG DAVIS
Date: 2024.09.09 15:51:18 -04'00'

Information Systems Owner, Craig W. Davis

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).

Privacy Act System of Records Notices (SORNs) - Privacy



VA Security Warning

This U.S. government system is intended to be used by authorized VA network users for viewing and retrieving information only except as otherwise explicitly authorized. VA information resides on and transmits through computer systems and networks funded by VA. All use is considered to be with an understanding and acceptance that there is no reasonable expectation of privacy for any data or transmissions on Government Intranet or Extranet (non-public) networks or systems., All transactions that occur on this system and all data transmitted through this system are subject to review and action including (but not limited to) monitoring- recording- retrieving- copying- auditing- inspecting- investigating- restricting access- blocking- tracking- disclosing to authorized personnel or any other authorized actions by all authorized VA and law enforcement personnel., All use of this system constitutes understanding and unconditional acceptance of these terms., Unauthorized attempts or acts to either (1) access- upload- change- or delete information on this system (2) modify this system (3) deny access to this system or (4) accrue resources for unauthorized use on this system are strictly prohibited., Such attempts or acts are subject to action that may result in criminal civil or administrative penalties.

Figure 1. VA Privacy Notification

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 and VHA Handbook 1605.04: Notice of Privacy Practices