Privacy Impact Assessment for the VA IT System called:

Office of Academic Affiliations - Support Center (OAA-SC)

Office of Academic Affiliations

Veteran’s Health Administration

eMASS ID: 1813

Date PIA submitted for review:

03 December 2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Nancy Katz-Johnson	nancy.katz-johnson@va.gov	203-535-7280
Information System Security Officer (ISSO)	Wesley Brown	wesley.brown6@va.gov	314-894-6468
Information System Owner	John Parise	john.parise@va.gov	314-894-5760

Abstract

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

The Office of Academic Affiliations Support Center (OAA-SC) system is responsible for accepting obligatory facility and VISN data related to the mission of the National Program Office, Office of Academic Affiliations (OAA). Field input of requested/filled resident positions, associated health requested/filled positions, quarterly adjustments of allocated funds, submission of Standards of Excellence Forms, Advanced Fellow tracking, Health Services Training headcounts, Veterans Access, Choice, and Accountability Act (VACAA) positions requests are included in this data collecting system. In addition, over 50 reports are available. Additional sub-sites are included for various stakeholders which collect data pertaining to Nursing evaluation programs, site visit tracking, and health profession trainee educational activity tracking calculations. Most of the system does not contain PII except for two sub-components which are the Advanced Fellowship Nomination Portal and Needs and Excess Validation tool.

The Advanced Fellowship Nomination Portal allows program office staff to upload nomination materials for review and certification by the Program Director, Coordinating Center, Designated Education Officer (DEO) and OAA for nomination approval. The system provides a way to collect the required documents and track the fellow through the approved program. It also provides a way to generate an approval memo that can be sent to local VAMC HR and fiscal staff with the required information to onboard the fellow for their approved fellowship.

The Needs and Excess Validation tool reconciles funds sent by OAA to VA Medical Centers for trainee salary. The system helps to ensure that funds sent match the salary and hours worked by each trainee.

Overview

The overview is the most important section of the Privacy Impact Assessment (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 business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?

The Office of Academic Affiliations Support Center System (OAA-SC) #2239 is responsible for accepting obligatory facility and VISN data related to the mission of the National Program Office, Office of Academic Affiliations (OAA). Field input of requested/filled resident positions, associated health requested/filled positions, quarterly adjustments of allocated funds, submission of Standards of Excellence Forms, Advanced Fellow tracking, Health Services Training headcounts, Veterans Access, Choice, and Accountability Act (VACAA) positions requests are included in this data collecting system. In addition, over 50 reports are available. Additional sub-sites are included for various stakeholders which collect data pertaining to Nursing evaluation programs, site visit tracking, and health profession trainee educational activity tracking calculations. Most of the system does not contain PII except for the Advanced Fellowship Nomination Application and Needs and Excess Validation Tool.

B. Who is the owner or has control of the IT system or project? If the system has an eMASS entry, ensure this information matches with the eMASS entry.

Owning Organization: VA Owned and Operated

2. Information Collection and Sharing

C. Indicate the expected number of individuals whose information is stored in the system and include a brief description of the typical client or affected individual?

There are approximately 500 current and 4,000 previously appointed Advanced Fellows in the system.

Check if Applicable	Demographic of individuals
☐	Veterans or Dependents
☐	VA Employees
☒	Clinical Trainees
☐	VA Contractors
☐	Members of the Public/Individuals
☐	Volunteers

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

The Office of Academic Affiliations – Support Center (OAA-SC) application system is responsible for accepting obligatory facility and Veterans Integrated Services Network (VISN) data related to the mission of the National Program Office, Office of Academic Affiliations (OAA). Field input of requested/filled resident positions, associated health requested/filled positions, quarterly adjustments of allocated funds, submission of Standards of Excellence Forms, Advanced Fellow tracking, Health Services Training headcounts, Veterans Access, Choice, and Accountability Act (VACAA) positions requests are included in this data collecting system. In addition, over 50 reports are available. Additional sub-sites are included for various stakeholders which collect data pertaining to Nursing evaluation programs, site visit tracking, and health profession trainee educational activity tracking calculations. Veteran Affairs (VA) employees first register for access and then if approved, are added as a user to the system. After that, they are verified using their Active Directory credentials.

E. *What information sharing is conducted by the IT system? A general description of the modules and components, where relevant, and their functions.*

The OAA-SC is an internal system and does not share information with entities outside of the government. The system encompasses several sub-components as outlined below.

- GME Allocation Verification Report (0145) – VISN Prioritization: This database application within OAA allows VISN leadership to review facility Graduate Medical Education / Dental Medical Education (GME/DME) allocations for accuracy and reallocations as necessary.
- GME Disbursement Agreements Uploads: This application provides access to all GME disbursement agreements with academic affiliates throughout the United States. It validates that OAA forms are utilized, unaltered, and signed prior to upload.
- Associated Health and Nursing Program Director Reassignment of Unfilled positions: This application allows Associated Health (AH) and Nursing national program directors to recommend temporary or permanent reassignements of unfilled positions to another VA medical center, which then are reviewed and approved by OAA.
- AH National Program Directors Review: This application allows AH national program directors to recommend the distribution of allocations to OAA. It is used in Q1 annually after each medical center has submitted allocation requests to OAA.
- Trainee Support for Associated Health and Nursing Professions and Standards of Excellence (SoE) Uploads: This application allows Designated Education Officers (DEO) to request stipends for funded Nursing and AH professions for the

upcoming academic year. Additionally, it allows DEOs to upload required profession specific SoE forms.

- GME Allocation Verification Report (Match 0145): This application allows facilities stakeholders to accurately reflect their funding allocations and Post Graduate Year (PGY) levels for the upcoming academic year. In addition, facilities can request additional positions while verifying initial Base position planning from the Fall to upcoming Academic Year.
- Health Services Training (HST) Report: This Database application within OAA allows Facilities to provide a count of all health profession trainees who were fully on-boarded and participated in 40 or more hours of training during the previous academic year. These reported activities directly support VAs statutory mission to educate health care professionals for VA and the Nation. Information extracted from this database is used to support VHAs education mission in the annual Presidents Budget Submission to Congress.
- Needs and Excess Quarterly Submissions: This application allows facilities to view funding disbursement and adjustments. Facilities are required to use the database to report Needs & Excess of funds to OAA quarterly. Expenditures or need requests are approved or denied by Central Office and then processed with national fiscal office.
- Need and Excess Validation Tool: The Needs and Excess Validation tool reconciles funds sent by OAA to VA Medical Centers for trainee salary. The system helps to ensure that funds sent match the salary and hours worked by each trainee.
- AH and Nursing Field Filled Positions: This application allows the Designated Education Officers (DEO) for each medical center to return unused associated health and nursing training positions to OAA. Once the position has been returned, national program directors are notified and can recommend temporary or permanent reallocations to OAA.
- Extended Educational Level Report: This application allows the filing of post-activity reports required by VHA Handbook 1400.11, that addresses procedures for Extended Educational Leave. The database is used to maintain individual application and tracking information for VA Extended Leave requests.
- GME VISN Prioritization for Additional Resident Allocations: This application allows VISN leadership to review the planning allocations of its facilities and make reallocations as necessary.
- GME Medical and Dental Resident Allocations – Facility: This application provides facilities stakeholders with complete long-range planning of academic positions for the upcoming Academic Year. It allows for permanent or temporary changes to allocations while allowing users to request for additional positions within facilities.
- Advanced Fellowship Nomination Application: A system used to complete information and upload documentation on all Advanced Fellows. The system gives the field the ability to appoint Fellows based on criteria set by OAA. The

application approval process includes the applicant being certified at different stages by first the Coordinating Center (if applicable), the Program Director and then the DEO. Additionally, the system generates approval memos for use by each VAMCs human resources department to onboard advanced fellows. OAA staff monitors the progress and process using automated and manual reporting. Report generation and downloading functionality allows for aggregate data analysis in support of program administration.

- Psychology Internship Match Portal: This application notifies OAA of the home schools for incoming internship classes, limited to psychology internship match results and affiliation agreements. OAA RFP Upload Portal: This central location allows VACO administrators to create new RFP data collecting sites and distribute a dynamically generated link to the field specific for that RFP. The module allows for field registration and allows for required supporting document file uploads along with a module to create contact lists of awarded results. Reviewers and administrators can view and score submissions, along with uploading 1 or more associated score sheets.
- OAA Web Manager Application: This web-based application is used internally by OAA staff to manage all programs managed by OAA. It gives staff the ability to manage the various portals within the OAA-SC umbrella.
- OAA Travel Portal: This web-based application routes travel requests via email through the appropriately assigned approval chains on a per person basis where approvers can approve or set another status. Numerous reports and graphs are available to track travel budgets and the associated traveler calendar displays all approved travel and destinations.
- VA Enterprise-Wide Psychology Training Accreditation Application: VA Enterprise-wide Psychology Training Accreditation (VEPTA) is an electronic Portal (Intranet Web Application). A centralized process developed to address the significant challenges facilities and VISNs face establishing contracts and making timely payments for accreditation activities. Each year, one quarter of psychology programs were threatened with having APA accreditation withdrawn due to non-payment of fees. An analysis of the required processes found that it was taking up to 40 hours locally to execute the payment for a site visit, in some cases payments were not executed due to confusion over sole source contracting regulations as they applied to APA as a sole source provider. OAA has worked with the VHA Strategic Acquisitions Center to develop a streamlined national sole source Blanket Purchase Agreement (BPA), associated business processes as well as data portal to allow field entry of APA accreditation activities. The Portal is used to allow each facility to register and notify the Office of Academic Affiliations (OAA) of their funded Psychology training program's existing accreditation status. Use of the VEPTA Portal allows psychology Directors of Training (DoT) to update OAA when an accreditation status has changed, a newly funded program submits an initial application, and/or when a site visit is coordinated and confirmed. The Portal is continuously open to allow updates as accreditation status changes and ask that DoTs review the portal annually to verify the status of each separately accredited program to verify for accuracy.

F. Are the modules/subsystems only applicable if information is shared?

The OAA-SC is an internal system and does not share information with entities outside of the government.

G. *Is the system operated in more than one site to include primary and secondary 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 application and all sub-components are hosted out of one location located at Jefferson Barracks, MO.

3. Legal Authority and System of Record Notices (SORN)

H. *What is the citation of the legal authority?*

38 U.S.C. 501(a)

I. *What is the SORN?*

The SORN is 161VA10 / 88 FR 42005 - published June 28, 2023 Veterans Health Administration Human Capital Management-VA https://www.govinfo.gov/content/pkg/FR-2023-06-28/pdf/2023-13681.pdf

J. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval.

No.

4. System Changes

K. Will the business processes change due to the information collection and sharing?

☐ Yes
☒ No
if yes, <<ADD ANSWER HERE>>

I. *Will the technology changes impact information collection and sharing?*

☐ Yes
☒ No
if yes, <<ADD ANSWER HERE>>

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 Information 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
☐ **Full** Social Security Number
☐ **Partial** 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/Sex
☐ Integrated Control Number (ICN)
☒ Military History/Service Connection
☐ Next of Kin
☐ Date of Death
☐ Business Email Address
☐ Electronic Data Interchange Personal Identifier (EDIPI)
☒ Other Data Elements (List Below)

Other PII/PHI data elements: Veteran Status, Employment History, Education History, Initial Pay.

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

1.2 List the sources of the information in the system

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

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

The applicant must submit their CV to the local VAMC HR department which is uploaded to the system. Some information from the CV is entered into the Advanced Fellow Nomination application which includes name, personal email, and whether they severed in the military or not.

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.

OAA-SC does not collect information from any other sources. Only the individual.

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

OAA-SC does not create information.

1.3 Methods of information collection

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?

No.

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 collected by local VA Medical Center Program Director and HR staff and then uploaded to the system through the Advanced Fellowship portal.
- Applicant information (i.e. Name, personal email address, Veteran status, and program information) is manually entered by VAMC staff into the portal.
- Documents are uploaded by VAMC staff to the OAA-SC.

1.4 Information checks for accuracy, and 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.

Each sub-component is managed by OAA program managers who verify data accuracy through manual and reporting processes. Additionally, field staff users who typically enter the information have a battery of reports at their level to ensure data accuracy. Lastly, for most sub-components, OAA program managers are notified via automated email when VAMC field staff enter or update information.

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?

Information is not checked for accuracy since the information contains employment information. Local HR staff as well as OAA administration must verify employment and education information.

1.5 Identify the specific legal authorities, arrangements, and agreements that 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

- VHA Handbook 1400.07 (Education of Advanced Fellows) lists submission and approval requirements for Advanced Fellows.
- OF 306 - Declaration for Federal Employment Declaration for Federal Employment, Optional Form 306 (opm.gov)
- SORN - Veterans Health Administration Human Capital Management-VA (161VA10A2) https://www.govinfo.gov/content/pkg/FR-2018-03-14/pdf/2018-05087.pdf
- RU 4. Disclosure may be made to individuals, organizations, private or public agencies, or other entities or individuals with whom VA has a contract or agreement to perform such services as VA may deem practicable for the purposes of laws administered by VA, in order for the contractor, subcontractor, public or private agency, or other entity or individual with whom VA has an agreement or contract to perform the services of the contract or agreement. This routine use includes disclosures by the individual or entity performing the service for VA to any secondary entity or individual to perform an

activity that is necessary for individuals, organizations, private or public agencies, or other entities or individuals with whom VA has a contract or agreement to provide the service to VA.re to enter the description.

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.

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

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

Principle of Minimization: The information is directly relevant and necessary to accomplish the specific purposes of the program.

Principle of Individual Participation: The program, to the extent possible and practical, collects information directly from the individual.

Principle of Data Quality and Integrity: VA policies and procedures must ensure that personally identifiable information is accurate, complete, and current.
This 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: Due to the sensitive nature of this data, there is a risk that, if data were compromised by unauthorized personnel, personal or professional harm may result for the affected individuals.

Mitigation: OAA-SC uses several security measures designed to ensure that the information is not inappropriately disclosed or released. Use of encryption to secure data in transit and at rest; user information security and privacy education and training; restricted use of removable media as well as static code analysis conducted by OAA support staff.

OAA-SC applications are built using VA active directory authentication as well as additional custom roles tailored to each sub-component. Additionally, OAA-SC applications are only accessible within the VA network. The OAA-SC helpdesk as procedures to assist users with system access. Security baselines are in place on the SQL and Web server.

Section 2. Uses of the Information

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

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

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

PII/PHI Data Element	Internal Use	External Use
Name	Used for verification in employment.	Not used
Personal Mailing Address	Used in verification as well as to receive employment information from the VA.	Not used
Personal Email	Used to contact the individual during the employment process.	Not used
Personal Phone	Used to contact the individual during the employment process as well as after the fellow is employed.	Not used
Military Service	Used to establish veterans' preference as well as reporting on number of veterans hired.	Not used
Employment History	This is used to verify that the applicant has the necessary experience for the fellowship as well as reference checks	Not used
Education History	Used to ensure that the applicant has the necessary education requirements a fellowship in the VA	Not used
Salary Information	Used to reconcile VA paid trainees against funds dispersed to VA Medical Centers.	Not Used

2.2 Describe the types of tools 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?

System does not 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.

System does not create or make available new or previously utilized information about an individual.

2.3 How the information in the system is secured.

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

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

Data in transit:

- Web application uses SSL

Data at Rest:

- The SQL Server uses Transparent Data Encryption (TDE) using AES-256 encryption.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs? (refer to PTA question 3.8).

Social Security Numbers are not collected, processed, or retained.

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

Data is encrypted both in transit and at rest using SSL and SQL AES-256 bit Transparent Data Encryption (TDE)

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

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. Example: Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.

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

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

2.4a How is access to the PII determined?

Access to the system is controlled by OAA staff on a case-by-case basis and is documented in the Advanced Fellowship yearly conference before each academic year. A prospective user is only granted access after they are vetted by OAA Advanced Fellowship staff. User roles are limited to their position at the local VAMC with only Designated Education Officers being allowed to appoint fellows.

Once a user logs in to the system, their access is recorded with a date time stamp when the logged on and off the system.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented? How are the documented, i.e. Policy, SOP, other. And where is this documentation located?

Yes. The OAA team follows all VA Access Control (AC) policies and has documented their procedures in the OAA-SC Access Control (AC) SOP.

2.4c Does access require manager approval?

Access requires approval from both the VA Medical Center Designated Education Officer and OAA staff.

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

The system uses temporal tables to track all changes. Additionally, the web server is under constant monitoring with App Dynamics.

2.4e Who is responsible for assuring safeguards for the PII as identified in eMASS?

The Information System Owner.

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
Personal Mailing Address

Personal Email
Military History/Service
Employment History
Education History
Salary Information

3.2 How long is information retained?

In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. If the system is using cloud technology, will it be following the NARA approved retention length and schedule https://www.archives.gov/records-mgmt/grs? This question is related to privacy control DM-2, Data Retention and Disposal.

The OAA-SC removes any records used for credentialing 3 years after the fellow separates from the VA. This in accordance with Records Control Schedule 10-1 (Healthcare Provider Credentialing and Privileging Records).

3.3 The retention schedule 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. Please work with the system 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?

The OAA-SC does not use personal identifiers for record retrieval (i.e. SSN is not used to retrieve a record) however, it abides by Records Control Schedule 10-1 for record retention purposes.

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

OAA-SC records are disposed of in accordance with GRS 5.2, item 020, and disposition authority: 44 USC 3501.

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

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

Electronic data and files of any type, including PHI, SPI, Human Resources records, and more are destroyed in accordance with the Media Sanitization section of the VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and are compliant with NIST SP 800-88. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle Bin. Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destruction. https://www.va.gov/vapubs/search_action.cfm?dType=1

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.

For the development \ training environments, PII such as personal email address is changed to a generic format to protect the data. Documents containing PII are not uploaded to the test \ training systems as they are needed for that purpose.

Baseline security requirements and safeguards implemented on our servers cover a large number of security-related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored and transmitted to those systems.

The OAA-SC uses role-specific permissions custom tailored to each sub-component ensuring that only authorized personnel have access to those components. Applications are tested using static code analyzers and servers are subject to recurring PIN scans. Users complete recurring training in handling PII to include the yearly VA rules of behavior as well as more detailed instruction as needed for each sub-component. Lastly, the OAA Helpdesk manages access to all roles requested for access and if requested by supervisors can remove access.

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 Privacy Officer (PO) to complete all Privacy Risk questions inside the document in 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: *The project retains only the information necessary for its purpose, additionally, the PII is retained only for as long as necessary and relevant to fulfill the specified purposes.*

Principle of Data Quality and Integrity: *The PIA should describe 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 OAA-SC team has made every effort to minimize the PII collected from an individual by only collecting essential information required for employment decisions. All of the information collected and stored in the database is encrypted during transport and while at rest in the database. However, because some PII is collected and stored for employment reasons, as identified in Section 2 of this document, a moderate risk based on the length of time the data is retained does exist should this information be accessed by an unauthorized malicious person, or accidentally communicated either verbally or electronically. Unauthorized access or disclosure to unauthorized parties may result in professional harm for the affected induvial(s).

Mitigation: Procedures will be enforced using technical and managerial control mechanisms in accordance with Records Control Schedule 10-1. The baseline security requirements and safeguards cover a large number of security-related areas with regard to protecting the confidentiality, integrity, and availability of the OAA-SC and the information processed therein. Security-related areas include access control, security awareness and training, security assessments, configuration management, contingency planning, incident response, physical and environmental protection and risk assessments.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

PII Mapping of Components

4.1a Office of Academic Affiliations – Support Center (OAA-SC) consists of two 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 OAA-SC 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 3.9a 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
Server 100	Yes	Yes	Name, Personal Email, Military History/service connection, Home Address, Education History, Employment History, Initial Pay	The collected information is used to verify that VA Advanced Fellows are qualified for their appointments.	OAA-SC uses SSL, role-based permissions, Active Directory Authentication, and database encryption. Additionally, only authorized personnel approved at two levels (the Designated Education Officer and OAA staff) can access the information.
Web Application	Yes	No	Name, Personal Email, Military History/service connection, Home Address, Education History, Employment History, Initial Pay	The collected information is used to verify that VA Advanced Fellows are qualified for their appointments.	OAA-SC uses SSL, role-based permissions, Active Directory Authentication, and database encryption. Additionally, only authorized personnel

					approved at two levels (the Designated Education Officer and OAA staff) can access the information.

4.1b List internal organizations information is shared/received/transmitted, the information shared/received/transmitted, and the purpose, and how the information is transmitted.

NOTE: Question 3.9b (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

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
N/A	N/A	N/A	N/A

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

Discuss the privacy risks associated with the sharing of information within the VA network 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 in this section.).

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

Follow the format below:

Privacy Risk: N/A

Mitigation: N/A

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 List the external organizations (outside VA) that information shared/received. and information shared/received, and the purpose, and how the information transmitted and what measures are taken to ensure it is secure.

The sharing of information outside the agency must be compatible with the original collection. The sharing must be covered by an appropriate routine use in a SORN. If not covered, 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 IT System or External Program Office information is	*List the purpose of information being shared /*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted)*	*List agreements such as: Contracts, MOU/ISA,*	*List the method of transmission and the measures in*

shared/received with	***received / transmitted***		***BAA, SORN. etc. that permit external sharing (can be more than one)***	***place to secure data***
N/A	N/A	N/A	N/A	N/A

5.2 <u>PRIVACY IMPACT ASSESSMENT: External sharing and disclosure</u>

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

If no External Sharing listed on the table above, ***(State there is no external sharing in both the risk and mitigation fields).***

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

Follow the format below:

<u>Privacy Risk:</u> N/A

<u>Mitigation:</u> 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 The notice provided to the individual before collection of the information. Please provide a copy and/or screen shot of a web notice of the notice as an Appendix-A 6.1 on the last page of the document. (A notice may include a posted privacy policy, a Privacy Act notice on forms, notice given to individuals by the sources system, or a system of records notice published in the Federal Register.) If notice was not provided, explain why.

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 Provide the Privacy Notice provided to the public by this system or any source systems. Include a copy of the notice in Appendix A of the PIA, the Federal Register citation, or Privacy Statement from collection of information such as forms or surveys.

A screen shot of the privacy notice from VA Form 10-2850D "Health Professions Trainee Data Collection Form" is included in Appendix A. SORN information can be found in 44 U.S.C. 3501, Department of Veterans Affairs, System of Records. The Notice of Privacy Practices (NOPP) can be found at the Department of Veterans Affairs, Veterans Health Administration, Notice of Privacy Practices.

6.1b If notice was not provided, explain why.

A screen shot of the privacy notice from VA Form 10-2850D "Health Professions Trainee Data Collection Form" is included in Appendix A. SORN information can be found in 44 U.S.C. 3501, Department of Veterans Affairs, System of Records.

6.1c Provide how the notice provided at the time of collection meets the purpose of use for this system.

Yes, in the 10-2850D, the applicant signs an authorization to release information and in the VA Handbook 1400.07 outlines submission requirements. Verbiage is included in appendix.

Additionally, the OAA-SC is covered under the following SORN:

Veterans Health Administration Human Capital Management-VA (161VA10A2) https://www.govinfo.gov/content/pkg/FR-2023-06-28/pdf/2023-13681.pdf. Disclosure may be made to individuals, organizations, private or public agencies, or other entities or individuals with whom VA has a contract or agreement to perform such services as VA may deem practicable for the purposes of laws administered by VA, in order for the contractor, subcontractor, public or private agency, or other entity or individual with whom VA has an agreement or contract to perform the services of the contract or agreement. This routine use includes disclosures by the individual or entity performing the service for VA to any secondary entity or individual to perform an activity that is necessary for individuals, organizations, private or public agencies, or other entities or individuals with whom VA has a contract or agreement to provide the service to VA.re to enter the description.

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.

Submission of documents is a requirement of employment. Certain information is required by VA HR when being hired. Information is VA employment and demographic data. The prospective employee has the right to work with their respective local VAMCHR office on what information they need to provide.

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.

Certain information is required by VA HR when being hired. Information is VA employment and demographic data. The prospective employee has the right to work with their respective local VAMC HR office on what information that need to provide.

6.4 <u>PRIVACY IMPACT ASSESSMENT: Notice</u>

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 Privacy Officer (PO) 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 Transparency:</u> This is referring to sufficient notice provided to the individual.

<u>Principle of Use Limitation:</u> The information used only for the purpose for which notice was provided either directly to the individual or through a public notice. The procedures in place must 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:

<u>Privacy Risk:</u> The risk for not providing notice would be a lack of transparency and the prospective applicant not being aware of VA's use of information.

<u>Mitigation:</u> Prospective applicants do not directly input or submit documents to the OAA-SC. Instead, they follow the local VAMC HR hiring procedures. VA HR employees and Education staff then submit those documents and information for OAA review.
Given this, mitigation is handled at both the local and nation level through the notices in the 10-2850D, VA Handbook 1400.07, and local HR procedures. Prospective applicants are made aware of how their personal information will be used in the hiring decision process.

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 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 VA Public Access Link-Home (efoia-host.com) to obtain information about FOIA points of contact and information about agency FOIA processes.***

Users have access to their own information in the OAA Support Center and for most of the system, no PII is used.

For the Advanced Fellowship Portal, users also have access to their account information and if something needs changed, they contact the OAA Advanced Fellowship team.

Advanced Fellows applicants who apply for a fellowship program submit their application and other required documentation to the local VAMC however, they do not have an account on the OAA Support Center, Advanced Fellowship sub-module.

The Needs and Excess Validation tool contains partial information from the PAID system which is viewable by the trainee.

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

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

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

OAA-SC 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.*

If a prospective applicant or a fellow who has been granted a fellowship with the VA finds that their information is inaccurate, they have several ways to update their information. They can notify their local HR department to correct the information or if they have been granted a fellowship, can update their information through systems used traditionally by VA employees. Once local HR staff are made aware of a needed correction, they can then update the individual's information in the OAA-SC.

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.

Appointed Fellows can update their information as any other VA employee can, through the HR Smart and PAID system. They would work with their HR office for procedures updating 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.

Appointed Fellows can update their information as any other VA employee can, through the HR Smart and PAID system. They would work with their HR office for procedures updating their information.

Prospective fellows can work with their local HR to work through changes and corrections in their information.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department's access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. ***For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals***

involved might change their behavior. *(Work with your Privacy Officer (PO) to complete all Privacy Risk questions in this section).*

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: The individual must be provided with the ability to find out whether a project maintains a record relating to them.

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

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

Follow the format below:

Privacy Risk: Since the information submitted is being used to make hiring decisions, there is a risk that a prospective fellow will not be hired based on incorrect data.

Mitigation: Appointed Fellows can update their information as any other VA employee can, through the HR Smart and PAID system. They would work with their HR office for procedures updating their information.

Prospective fellows can work with their local HR to work through changes and corrections in their information in accordance with local procedures.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures. (Work with your ISSO to complete this section).

8.1 The procedures in place to determine which users may access the system, must be 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?

The OAA-SC application and sub-modules are built using VA active directory authentication with custom roles tailored to each module. The OAA Helpdesk will process and assists users as needed.
The following flow chart defines how users request access to the OAA-SC information system.

User Request Flow:

1. The VAMC field user enters their VA information and requested access level into the New User Request form.
2. An email is sent to both OAA staff and the Designated Education Officer (DEO) of the facility where the user works.
3. The DEO checks the access request to ensure that the user should have access to the requested resources.
4. If the DEO grants the user access:
    a. An automated email is sent to the user as well as OAA staff.
    b. OAA staff reviews the request and DEO information to ensure accuracy.
    c. OAA staff as well as the OAA Data Management and Support Center (DMC) team activate the user's account.
5. If the DEO denies the user access,
    a. an automated email is sent to the user and OAA staff.
    b. OAA staff reviews the email and request.
    c. OAA staff and the OAA DMC team ensures that the account is deactivated and annotates the reason for denial.

Tools: All forms are internal to the VA Network.

1. OAA-SC Home Page
2. OAA-SC New Request Permission Form
3. OAA-SC Help Desk

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?

There are no users from other agencies who use OAA-SC.

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.

Field Staff User: This level allows for read/write actions to components based on approval from their VAMC Designated Education Officer. Each user at this level is individually approved access to authorized sub-components of OAA-SC.

VISN Staff User: Users at this level have access to systems and reports at the VISN level which contains information for all the VA Medical Centers.

VA Medical Center Designated Education Officer: This is a special user type approved by OAA staff that can approve individuals at their facility access to the various OAA sub-systems.

OAA Staff: This user type is reserved for individuals in OAA who oversee or assist in overseeing the various programs managed by OAA.

OAA Admin: This group of individuals is limited based on the sub-component business rules. OAA Data Management and Support Center personnel have Admin privileges over all systems however, in some sub-systems such as the Advanced Fellow Nomination Portal, OAA Staff assigned to the Advanced Fellowship Team have Admin privileges to assign and remove users as well as other functions to override/correct information entered by field users.

8.2. Contractor signed Non-Disclosure Agreement (NDA), Business Associate Agreement (BAA) etc. in place.

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.

8.2a Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

The OAA Data Management Team has signed a short-term contract to assist with the development and maintenance in OAA-SC components. Contracts are reviewed yearly by the OAA staff and the contracting officer. Background checks and clearance will be obtained prior to contractors beginning work. Additionally, NDA's will be signed by all contractors.

8.2a. Will VA contractors have access to the system and the PII?

Yes.

8.2b. What involvement will contractors have with the design and maintenance of the system?

Contractors provide application development support on most OAA-SC components to include feature enhancements, maintenance, and break-fix actions.

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.

Per VHA Handbook 1605.1, all users are required to complete the VHA Privacy and HIPPA Training course annually before being granted access to VHA systems. This training is managed at the local level and is required before having access to OAA-SC.

8.4 The Authorization and Accreditation (A&A) completed for the system.

8.4a If completed, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 11-Oct-2023
3. *The Authorization Status:* Authorized to Operate (ATO)
4. *The Authorization Date:* 04-Dec-2023
5. *The Authorization Termination Date:* 29-Nov-2025
6. *The Risk Review Completion Date:* 29-Nov-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 not completed 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. ***(Refer to question 1.8 of the PTA)***

N/A

9.2 Does the contract with the Hosting 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 3.3.1 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**
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.

NANCY KATZ-JOHNSON

Digitally signed by NANCY KATZ-JOHNSON
Date: 2025.01.03 16:43:44 -05'00'

Privacy Officer, Nancy Katz-Johnson

WESLEY BROWN

Digitally signed by WESLEY BROWN
Date: 2025.01.06 08:59:18 -06'00'

Information Systems Security Officer, Wesley Brown

JOHN PARISE

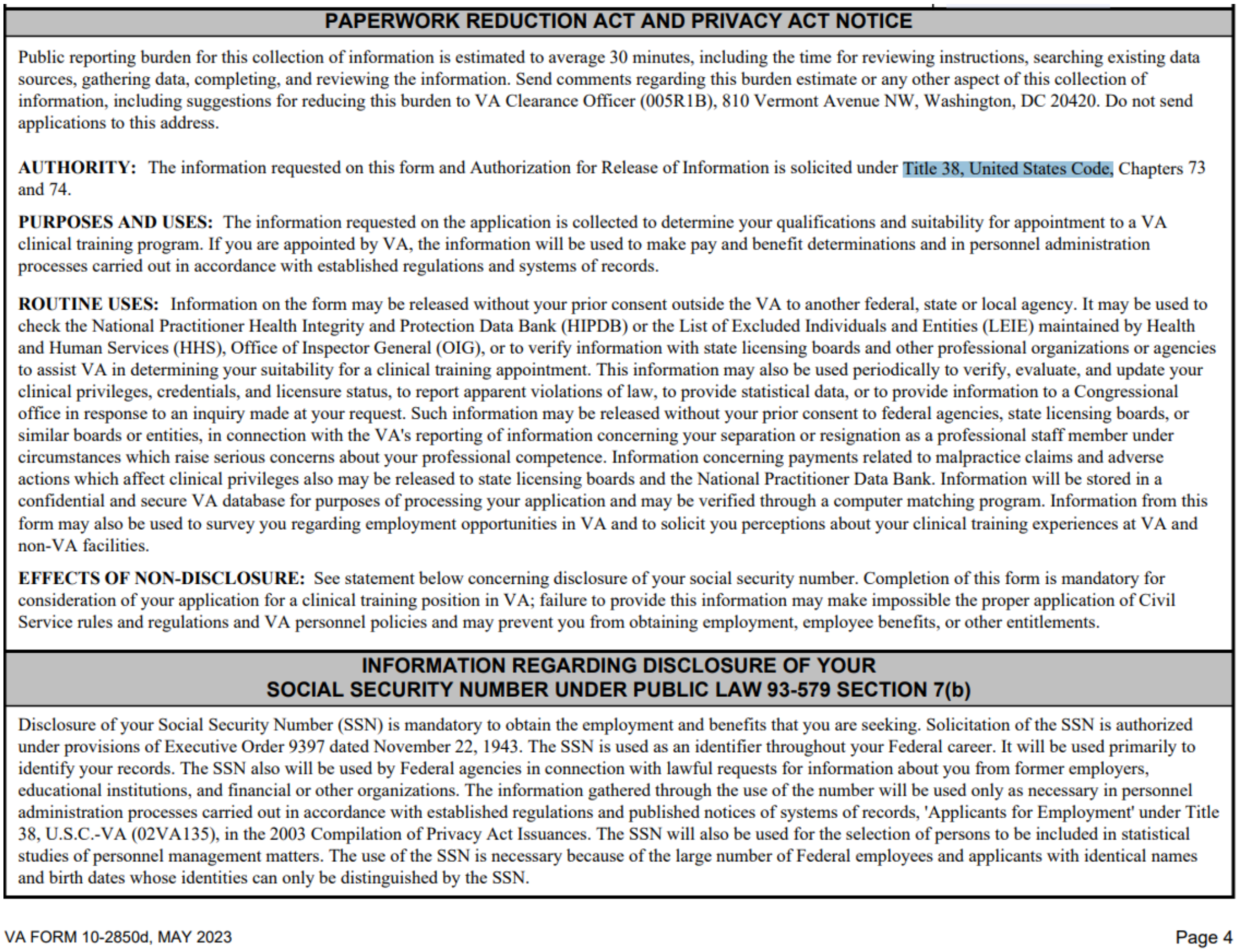
Digitally signed by JOHN PARISE
Date: 2025.01.06 10:43:17 -06'00'

Information Systems Owner, John Parise

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).

VA Form 10-2850D.



PAPERWORK REDUCTION ACT AND PRIVACY ACT NOTICE

Public reporting burden for this collection of information is estimated to average 30 minutes, including the time for reviewing instructions, searching existing data sources, gathering data, completing, and reviewing the information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to VA Clearance Officer (005R1B), 810 Vermont Avenue NW, Washington, DC 20420. Do not send applications to this address.

AUTHORITY: The information requested on this form and Authorization for Release of Information is solicited under Title 38, United States Code, Chapters 73 and 74.

PURPOSES AND USES: The information requested on the application is collected to determine your qualifications and suitability for appointment to a VA clinical training program. If you are appointed by VA, the information will be used to make pay and benefit determinations and in personnel administration processes carried out in accordance with established regulations and systems of records.

ROUTINE USES: Information on the form may be released without your prior consent outside the VA to another federal, state or local agency. It may be used to check the National Practitioner Health Integrity and Protection Data Bank (HIPDB) or the List of Excluded Individuals and Entities (LEIE) maintained by Health and Human Services (HHS), Office of Inspector General (OIG), or to verify information with state licensing boards and other professional organizations or agencies to assist VA in determining your suitability for a clinical training appointment. This information may also be used periodically to verify, evaluate, and update your clinical privileges, credentials, and licensure status, to report apparent violations of law, to provide statistical data, or to provide information to a Congressional office in response to an inquiry made at your request. Such information may be released without your prior consent to federal agencies, state licensing boards, or similar boards or entities, in connection with the VA's reporting of information concerning your separation or resignation as a professional staff member under circumstances which raise serious concerns about your professional competence. Information concerning payments related to malpractice claims and adverse actions which affect clinical privileges also may be released to state licensing boards and the National Practitioner Data Bank. Information will be stored in a confidential and secure VA database for purposes of processing your application and may be verified through a computer matching program. Information from this form may also be used to survey you regarding employment opportunities in VA and to solicit you perceptions about your clinical training experiences at VA and non-VA facilities.

EFFECTS OF NON-DISCLOSURE: See statement below concerning disclosure of your social security number. Completion of this form is mandatory for consideration of your application for a clinical training position in VA; failure to provide this information may make impossible the proper application of Civil Service rules and regulations and VA personnel policies and may prevent you from obtaining employment, employee benefits, or other entitlements.

INFORMATION REGARDING DISCLOSURE OF YOUR SOCIAL SECURITY NUMBER UNDER PUBLIC LAW 93-579 SECTION 7(b)

Disclosure of your Social Security Number (SSN) is mandatory to obtain the employment and benefits that you are seeking. Solicitation of the SSN is authorized under provisions of Executive Order 9397 dated November 22, 1943. The SSN is used as an identifier throughout your Federal career. It will be used primarily to identify your records. The SSN also will be used by Federal agencies in connection with lawful requests for information about you from former employers, educational institutions, and financial or other organizations. The information gathered through the use of the number will be used only as necessary in personnel administration processes carried out in accordance with established regulations and published notices of systems of records, 'Applicants for Employment' under Title 38, U.S.C.-VA (02VA135), in the 2003 Compilation of Privacy Act Issuances. The SSN will also be used for the selection of persons to be included in statistical studies of personnel management matters. The use of the SSN is necessary because of the large number of Federal employees and applicants with identical names and birth dates whose identities can only be distinguished by the SSN.

VA FORM 10-2850d, MAY 2023 Page 4

HELPFUL LINKS:

Records Control Schedule 10-1 (va.gov)

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 Directive 1605.04
IB 10-163p (va.gov)