Privacy Impact Assessment for the VA IT System called:

Office of Academic Affiliations Support Center (OAA-SC)

Office of Academic Affiliations, Veterans Health Administration

Date PIA submitted for review:

10/26/2021

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Peggy Pugh	Margaret.Pugh@va.gov	202-731-6843
Information System Security Officer (ISSO)	Richard Alomar-Loubriel	Richard.Alomar-Loubriel@va.gov	787-696-4091
Information System Owner	John Parise	John.Parise@va.gov	314-250-7618

Abstract

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

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 onesub-component called the Advanced Fellowship Nomination Portal.

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.

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:

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *Indicate the ownership or control of the IT system or project.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *A general description of the information in the IT system and the purpose for collecting this information.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.*
- *A citation of the legal authority to operate the IT system.*

- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*
- *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?*

The Office of Academic Affiliations Support Center is developed and maintained by the Office of Academic Affiliations, Veterans Health Administration. 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. Mostof the system does not contain PII except for one website of (OAA-SC) called the Advanced Fellowship Nomination Application.

There are approximately 500 current and 4,000 previously appointed Advanced Fellows in the system. Information collected and stored by the OAA-SC include the Curriculum Vitae submitted by the Fellow, as well as HR Smart Information (Occupation and Job Code) and starting pay if the Fellow is accepted into a program. The database system stores the name, personal email address, and veteran status of the fellow.

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.

- 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.

- Educational Activity Record (EAR) Calculator: The purpose of the EAR calculator is to assist with calculations in which the trainee has used multiple types of leave exceptions. Field Users enter a month or block, trainee type, days worked, and can then select up to 17 different conditions to be calculated.

- Nurse Practitioner Residency Evaluation Portal: The NPR evaluation portal is multifunctional in nature: (1) allows monitoring individual program compliance with evaluation requirements, (2) serves as a national multi-site evaluation data collection system, (3) enables sharing facility-level evaluation findings and reports with relevant stakeholders, and (4) provides a number of practical evaluation tools and resources to VA medical centers in order to help sites to effectively conduct site-specific, local program evaluation. The portal has two distinctly built interfaces: one that serves the needs of field-based program directors (PD) and faculty/preceptors, and another one that fulfills evaluation requirements of VA OAA nursing trainees. Prior to each academic year (AY), the VA OAA conducts web-based training sessions with the relevant stakeholders to orientusers on proper utilization of the OAA Nursing Education Evaluation Portal instruments and resources. In addition, to ensure timely communication of findings to stakeholders, the VA OAAdeveloped a variety of portal-based, fully automated evaluation data reports pertaining to the individual VA, site-specific evaluation data.

- Post-Baccalaureate Nurse Residency Evaluation Portal: The PB-RNR evaluation portal is multifunctional in nature: (1) allows monitoring individual program compliance with evaluation requirements, (2) serves as a national multi-site evaluation data collection system, (3) enables sharing facility-level evaluation findings and reports with relevant stakeholders, and (4) provides a number of practical evaluation tools and resources to VA medical centers in order to help sites to effectively conduct site-specific, local program evaluation. The portal has two distinctly built interfaces: one that serves the needs of field-based program directors (PD) and faculty/preceptors, and another one that fulfills evaluation requirements of VA OAA nursing trainees. Prior to each academic year (AY), the VA OAA conducts web-based training sessions with the relevant stakeholders to orient users on proper utilization of the OAA Nursing Education Evaluation Portal instruments and resources. In addition, to ensure timely communication of findings to stakeholders, the VA OAA developed a variety of portal-based, fully automated evaluation data reports pertaining to the individual VA, site-specific evaluation data.

- 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.

The application and all sub-components are hosted out of one location located at Jefferson Barracks, MO. Currently, the application has been granted an ATO which is valid through January 22, 2022. As of this writing, an application package is in the process of being completed to extend the ATO end date. Additionally, there will not be any technology changes once the PIA is completed.

Section 1. Characterization of the Information

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

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

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

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

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

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

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

- Employment History
- Education History

PII Mapping of Components

OAA-SC consists of one key components (databases). 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.

PII Mapped to Components

Note: Due to the PIA being a public facing document, please do not include the server names in the table. The first table of 3.10 in the PTA should be used to answer this question.

PII Mapped to Components

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
OITESTL100	YES	YES	Name, Personal Email, Veteran Status, Home Address, Education History, Employment History	To verify and nominated Advanced Fellows.	* Database traffic is encrypted. * Web portal uses SSL. * Users must register and are vetted by OAA staff. * Data is encrypted at rest in the database. * Users are authenticated using VA active directory as opposed to passwords. * The system can only be accessed within the VA firewall.

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

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 then uploaded to the system.

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 1.3 indicate why the system is using this source of data.

- *N/A*

If the system creates information (for example, a score, analysis, or report), list the system as a source of information.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

- *N/A*

1.3 How is the information collected?

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 technology used in the storage or transmission of information in identifiable form?

If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form's OMB control number and the agency form number.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

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

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.

If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.
This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

- 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 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

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

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks.

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

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

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

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

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

Follow the format below when entering your risk assessment:
<u>Privacy Risk:</u>
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.

<u>Mitigation:</u>

OAA-SC uses a number of 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 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.

Name: Used for verification in employment.

Personal Mailing Address: Used in verification as well as to receive employment information from the VA.

Personal Email: Used to contact the individual during the employment process.

Personal Phone: Used to contact the individual during the employment process as well as after the fellow is employed.

Military Service: Used to establish veterans' preference as well as reporting on number of veterans hired.

Employment History: This is used to verify that the applicant has the necessary experience for the fellowship as well as reference checks.

Education History: Used to ensure that the applicant has the necessary education requirements a fellowship in the VA.

2.2 What types of tools are used to analyze data and what type of data may be produced?

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.

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.
This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

- Not applicable in this system.

2.3 How is the information in the system secured?

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?

- *Not applicable*

2.3 c 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)*

This question is related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest

2.4 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u> How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. <u>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.</u>

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

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

<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.

The PIA and SORN are clear about the uses of the stored information. All information is relevant and are used in hiring decisions, onboarding, and employment of the fellow.

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,

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

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?

The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.
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 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so please indicate the name of the records retention schedule.

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.
This question is related to privacy control DM-2, Data Retention and Disposal.

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.

3.4 What are the procedures for the elimination of SPI?

Explain how records are destroyed or eliminated at the end of the 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

Applicable federal regulatory requirements Records Control Schedule 10-1 will be followed for eliminating and disposing data. We electronically receive our data from local VAMCs. All records are received within stored in electronic format and removed from the database as required by retention policy.

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. Have policies and procedures been developed to minimize the use of PII 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 <u>PRIVACY IMPACT ASSESSMENT: Retention of information</u>

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks.

While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

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

<u>Principle of Minimization:</u> Does the project retain only the information necessary for its purpose? Is the PII retained only for as long as necessary and relevant to fulfill the specified purposes?

<u>Principle of Data Quality and Integrity:</u> Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?
This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:
<u>Privacy Risk:</u>

Due to the sensitive nature of this data, there is a risk that if data were accessed or received by unauthorized parties, personal or professional harm may result for the affected individual.

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.

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
N/A	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 Department and what steps, if any, are currently being taken to mitigate those identified risks.
This question is related to privacy control UL-1, Internal Use.

Follow the format below:
<u>Privacy Risk:</u> N/A

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

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

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

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

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

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

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

Data Shared with External Organizations

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

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: N/A

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 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?

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. If notice was provided in the Federal Register, provide the citation.

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

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. This question is 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.

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-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.

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 VAMC HR office on what information that 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.

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

<u>Principle of Transparency:</u> Has sufficient notice been provided to the individual?

<u>Principle of Use Limitation:</u> 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:
<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 What are the procedures that allow individuals to gain access to their information?

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.

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).

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.

This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

- 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.

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 HRSmart 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.

7.4 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.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.

Appointed Fellows can update their information as any other VA employee can, through the HRSmart 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.

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

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

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

Follow the format below:

Privacy Risk: 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 HRSmart 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.

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

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

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?

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.

This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.

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.

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.

Yes, 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.

8.3 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.

Yearly training is required for all users including additional training for managing PII and HIPPA included in the VA Privacy and Information Security Awareness and Rules of Behavior (WBT) as well as annual Government Ethics courses. Additional training is managed at the sub-component level in the OAA-SC if special training is necessary.

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

If Yes, provide:

1. *The Security Plan Status,*
2. *The Security Plan Status Date,*
3. *The Authorization Status,*
4. *The Authorization Date,*
5. *The Authorization Termination Date,*
6. *The Risk Review Completion Date,*
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH).*

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

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

Yes, the ATO was certified on 09/30/2021 and expires on 01/28/2022.

Security Plan Status: Approved
Security Plan Status Date: 11/17/2021
Authorization Status: Approved
Authorization Date: 09/30/2021
Authorization Termination Date: 01/28/2022
Risk Review Date: 09/27/2021
FIPS 199 Classification: Moderate

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).

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.

N/A

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract)

This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

N/A

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

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

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

N/A

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

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met?

This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

N/A

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

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

N/A

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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

Signature of Responsible Officials

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

Margaret L. Pugh 104985

Digitally signed by Margaret L. Pugh 104985
Date: 2021.12.08 15:21:24 -05'00'

Privacy Officer, Peggy Pugh

RICHARD ALOMAR-LOUBRIEL 139039

Digitally signed by RICHARD ALOMAR-LOUBRIEL 139039
Date: 2021.12.08 15:59:29 -05'00'

Information Systems Security Officer, Richard Alomar-Loubriel

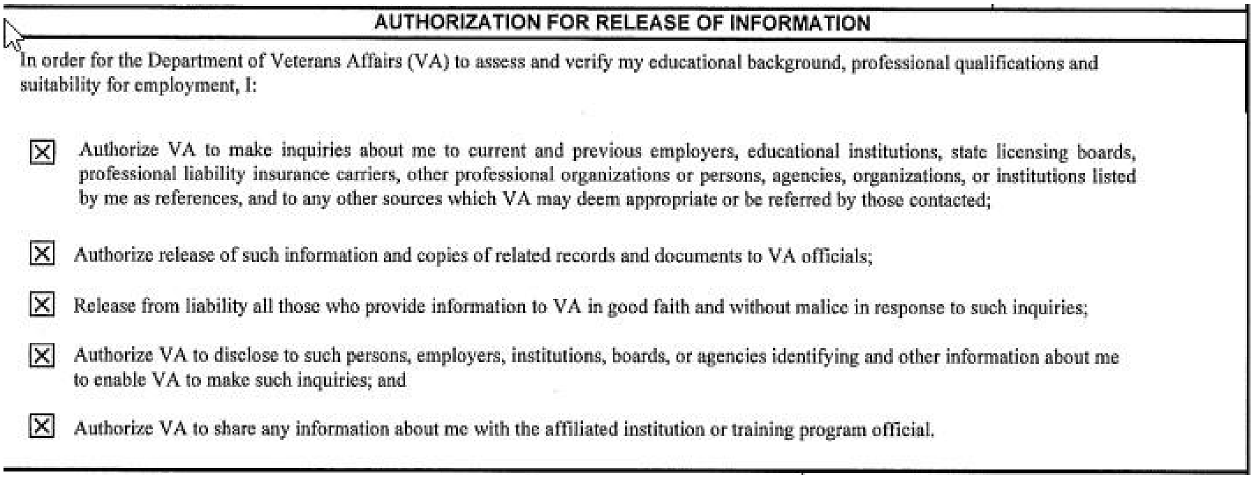
John D. Parise 643052

Digitally signed by John D. Parise 643052
Date: 2021.12.02 15:52:07 -06'00'

System Owner, John Parise

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).

https://www.va.gov/vaforms/medical/pdf/vha-10-2850d-fill.pdf



AUTHORIZATION FOR RELEASE OF INFORMATION

In order for the Department of Veterans Affairs (VA) to assess and verify my educational background, professional qualifications and suitability for employment, I:

☒ Authorize VA to make inquiries about me to current and previous employers, educational institutions, state licensing boards, professional liability insurance carriers, other professional organizations or persons, agencies, organizations, or institutions listed by me as references, and to any other sources which VA may deem appropriate or be referred by those contacted;

☒ Authorize release of such information and copies of related records and documents to VA officials;

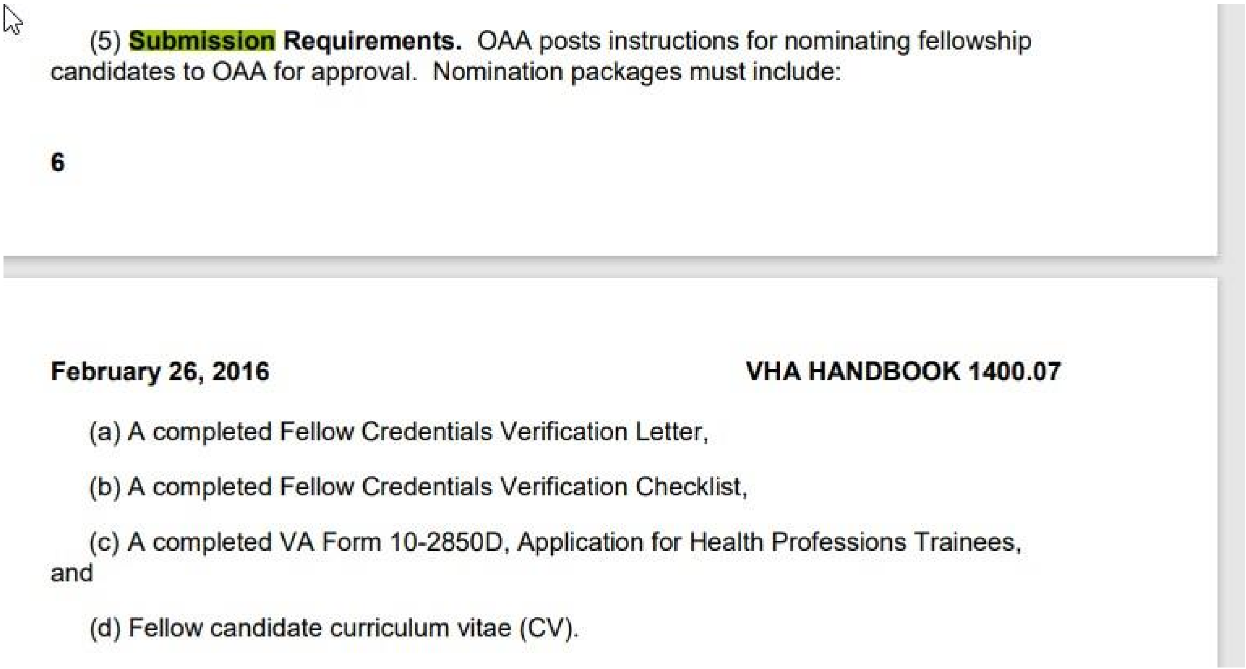
☒ Release from liability all those who provide information to VA in good faith and without malice in response to such inquiries;

☒ Authorize VA to disclose to such persons, employers, institutions, boards, or agencies identifying and other information about me to enable VA to make such inquiries; and

☒ Authorize VA to share any information about me with the affiliated institution or training program official.

https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=3179

VA Handbook 1400.07



(5) **Submission Requirements.** OAA posts instructions for nominating fellowship candidates to OAA for approval. Nomination packages must include:

6

February 26, 2016 **VHA HANDBOOK 1400.07**

(a) A completed Fellow Credentials Verification Letter,

(b) A completed Fellow Credentials Verification Checklist,

(c) A completed VA Form 10-2850D, Application for Health Professions Trainees, and

(d) Fellow candidate curriculum vitae (CV).