Privacy Impact Assessment for the VA IT System called:

Managed Service – VetPro Assessing

Veterans Health Administration (VHA)

VHA Credentialing and Privileging Office

Date PIA submitted for review:

8/16/2023

System Contacts

System Contacts:

	Name	E-mail	Phone Number
Privacy Officer	Ristene Mockel	Ristene.Mockel@va.gov	406-403-5298
Information System Security Officer (ISSO)	Steve Cosby	Steve.Cosby@va.gov	919-201-4837
Information System Owner	Marianne Chick	Marianne.Chick@va.gov	919-474-3937

Abstract

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

Managed Service – VetPro Assessing (VetPro) is a Veterans Affairs (VA) Government Off-The-Shelf credentialing software system used to credential healthcare providers. VetPro is an enterprise-level web-based application with a relational database and image processing components. VetPro includes a web-based front-end for basic input/output, with middle-tier modules and database procedures for image processing, and electronic data interchange with the National Practitioner Data Bank (NPDB) and the Federation of State Medical Boards (FSMB).

Overview

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

1 General Description

A. The IT system name and the name of the program office that owns the IT system.

Managed Service – VetPro Assessing (VetPro) is owned by VHA Credentialing and Privileging Office

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

The VetPro application is managed service major application used by all VHA facilities for the credentialing of all VHA licensed, certified, or registered health care providers, including contractors and volunteers.

VHA is the largest federal health care provider with more than 1,700 sites of care, including over 153 hospitals, over 800 community and facility-based clinics, over 133 nursing homes, and 48 domicilliaries organized into 141 medical staffs.

Each VHA facility enrolls providers requiring credentialing into the internet-based system https://fcp.vetpro.org. Providers then login and enter required information for their education, licenses, work history, peer references. This information is then primary source verified by credentialing coordinators at each facility.

Credentialing is one of the most critical activities performed in our healthcare facilities. It ensures that professionals who deliver health care have the qualifications and competence to provide that care. Deliverance of high-quality care and ensuring patient safety are firmly linked to your appropriate credentialing. Credentialing done appropriately reduces the risk to patients for adverse outcomes by completing a full assessment of the applicant prior to them being brought on duty.

The VetPro application creates a secure electronic database for credentialing of all VHA licensed, registered, or certified health care providers and enables sharing of verified credentials in support of regular and multiple appointments, rapid deployment, and telemedicine.

C. Indicate the ownership or control of the IT system or project.

VA Owned and VA Operated (hosted in the NIH CIT)

2. Information Collection and Sharing

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

Currently there over 600,000 individuals that have their information stored in VetPro. These individuals include VHA health care providers and credentialing coordinators.

E. A general description of the information in the IT system and the purpose for collecting this information.

VetPro contains the full name, social security number (SSN), and contact information (e.g., work email address) for all users, including health care providers and credentialing coordinators to assist with verifying the individual's identity. Additionally, VetPro contains credentialing information (e.g., state licensure, professional education, work history, etc.) and other information as needed to complete credentialing.

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

Credentialing information is shared between VHA facilities internally and with the NPDB and FSMB organizations.

The concept of shared credentials, specifically in an electronic format has far reaching implications and will assist in current efforts to:
1. Improve the quality and reliability of the credentialing process
2. Promote inter-facility sharing of health care resources and support national readiness
3. Facilitate the establishment of tele-medicine initiatives
4. Reduce initial and recredentialing costs

NPDB and FSMB are querying systems. Credentialing information is shared with NPDB and FSMB to obtain reports for the specific provider, such as whether the provider had an action taken against their professional licensure.

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

VetPro is a national system which includes all VHA facilities. Use of the systems, maintenance of PII, and controls are the same at all VHA facilities in VetPro.

3. Legal Authority and SORN

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

77VA10E2E/85 FR 7395 Health Care Provider Credentialing and Privileging Records-VA
Title 38 United States Code (U.S.C.) 501(a) and section 7304(a)(2)

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

SORN does not require amendment or revision.

VetPro does not use cloud technology.

D. System Changes

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

No.

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

No.

Section 1. Characterization of the Information

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

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

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

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

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

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

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

The VetPro application stores information necessary for credentialing of all VHA licensed, registered, or certified health care providers. This includes name, SSN, date of birth address, licenses, certification, registration with DEA (Drug Enforcement Agency), and other licensing organizations.

Financial Information only includes partial charge card information used to pay for NPDB queries.

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

PII Mapping of Components (Servers/Database)

Managed Service – VetPro Assessing consists of 18 key components (servers/databases) hosted by NIH CIT. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Managed Service – VetPro Assessing 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 the server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

Internal Database Connections

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
N/A	N/A	N/A	N/A	N/A	N/A

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

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

Credentialing information is entered into the system by individual providers and verification documents are scanned into the system by a coordinator or recorded through a Report of Contact. Additionally, VetPro has an interface with the NPDB and FSMB for purposes of ordering and receiving reports on the credentialed providers.

Application uses SSL (Secure Sockets Layer) to encrypt communications to require SSL 1.1 or above. In addition, the SOAP is used as a message protocol. Also, a unique username and password is provided when connecting to other systems.

Definitions:
SSL (Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and integral.
SOAP (Simple Object Access Protocol) is a messaging protocol that allows programs that run on disparate operating systems (such as Windows and Linux) to communicate using Hypertext Transfer Protocol (HTTP) and its Extensible Markup Language (XML).

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.

Credentialing policy requires that information submitted by the provider be verified with primary sources such as state licensing boards, educational institutions, etc., and this verification effort be documented within VetPro. Providers are also required to be queried against the NPDB and FSMB databases, as applicable.

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

Standardized ("canned") reports are available to VetPro users who have User Access roles which include access to the reports function. These reports do not create records and are used for internal control purposes. The data is not "newly derived" – it just pulls information from set fields for administrative monitoring of things such as processing times, expiring licensure, files in a certain processing status, etc.

1.3 How is the information collected?

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

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

Credentialing information is entered into the system by individual providers and verification documents are scanned into the system by a coordinator or recorded through a Report of Contact Additionally, VetPro has an interface with the NPDB and FSMB for purposes of ordering and receiving reports on the credentialed providers.

1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form's OMB control number and the agency form number.

The information is not collected on a form and is not subject to the Paperwork Reduction Act.

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

These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

There are various audits performed by the facility and VHA Credentialing and Privileging Office to ensure the information is accurate. Information is checked against scan documents and outside sources like licensing boards to confirm the validity of entered data.

1.4b If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

There are no contracts between VA and NPDB or VA and FSMB related to usage of querying services.

Reports in NPDB are records of actions taken by authorized organizations regarding health care practitioners, entities, providers, and suppliers who do not meet professional standards. Health care organizations (including VHA facilities) must register with NPDB and be authorized to report to the NPDB in accordance with federal regulations. Through VetPro, queries to NPDB are submitted to obtain NPDB reports on specific health care providers which include actions such as medical malpractice payments and adverse actions against the provider's clinical privileges. Reports are documented in the provider's VetPro file.

FSMB contains files/reports on physicians relating to any board or licensure actions against an individual physician. All information in FSMB is received and updated regularly from state medical boards. Through VetPro, queries to FSMB are submitted to obtain FSMB reports on specific physicians. Reports are documented in the physician's VetPro file.

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

Title 38 U.S.C. 501(a) and section 7304(a)(2):

(a)Unless specifically otherwise provided, the Under Secretary for Health shall prescribe all regulations necessary to the administration of the Veterans Health Administration, including regulations relating to—
(1)travel, transportation of household goods and effects, and deductions from pay for quarters and subsistence; and
(2)the custody, use, and preservation of the records, papers, and property of the Administration.
(b)Regulations prescribed by the Under Secretary for Health are subject to the approval of the Secretary.

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: The VetPro system requires a high level of protection due to the risk and magnitude of the loss or harm that could result from an inadvertent or deliberate disclosure, alteration, or destruction of the information.

Mitigation: The VA requires that a security incident reporting and response capability be established to ensure that computer security incidents are detected, reported, and corrected at the earliest possible time. The incident reporting and response process is designed to detect and respond to security incidents as they occur, assist in preventing future incidents from occurring through awareness, contain necessary response mechanisms to deal with incidents, and support security controls and procedures. This process is outlined in VetPro Policy 11, VetPro Incident Reporting.

The Director, VHA Credentialing and Privileging Office is responsible for administering the VetPro security and ensuring the implementation of the Incident Reporting System, including ensuring that:

- Security violations/incidents occurring associated with VetPro are reported to the appropriate facility ISO for appropriate documentation, resolution, or escalation
- All VetPro users on a regular basis understand they are responsible for reporting actual or suspected security incidents to their immediate supervisor or facility Information Security Officer (ISO), and the Director, Quality Standards.
- Supervisor (level 400) users are responsible for administering the VetPro security and ensuring the implementation of the Incident Reporting System within their own facilities, including ensuring:
- Security violations/incidents occurring associated with VetPro are reported to the appropriate facility ISO for appropriate resolution or escalation.
- All VetPro users on a regular basis understand they are responsible for reporting actual or suspected security incidents to their immediate supervisor or facility ISO, and the Director, VHA Credentialing and Privileging Office for appropriate resolution or escalation.

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 to Verify Identity
Social Security Number: Used to Verify Identity
Date of Birth: Used to Verify Identity
Mailing Address: Used to contact individual
Zip Code: Used to contact individual
Phone Number(s): Used to contact individual
Fax Number: Used to contact individual
Email Address: Used to contact individual
License/Certificate numbers: Used to verify the provider is qualified to work for hired occupation
Gender: Used to Verify Identity
Financial Information: Used to pay for NPDB query

Credentialing is foremost in-patient safety and ensuring only those with the highest qualifications provide care to the veterans. The information may be used for:

- Verifying the individual's credentials and qualifications for employment or utilization, appointment to the professional staff, and/or clinical privileges
- Advising prospective health care entity employers, health care professional licensing or monitoring bodies, the NPDB, or similar entities or activities of individuals covered by this system
- Accreditation of a facility by an entity such as the Joint Commission
- Audits, reviews and investigations conducted by staff of the health care facility, the Veterans Integrated Service Network (VISN) Directors and Division Offices, VA Central Office, VHA program offices, and the VA Office of Inspector General
- Law enforcement investigations; quality assurance audits, reviews and investigations
- Personnel management and evaluations
- Employee ratings and performance evaluations
- Employee disciplinary or other adverse action, including discharge
- Statistical analysis, to produce various management reports, evaluate services, collection, distribution and utilization of resources
- Providing clinical and administrative support to patient medical care.

2.2 What types of tools are used to analyze data and what type of data may be produced?
These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis.

Standardized ("canned") reports are available to VetPro users who have User Access roles which include access to the reports function. These reports do not create records and are used for internal control purposes. The data is not "newly derived" – it just pulls information from set fields for administrative monitoring of things such as processing times, expiring licensure, files in a certain processing status, etc.

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.

VetPro does not create or make available new or previously unutilized information about an individual,

2.3 How is the information in the system secured?

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

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

VetPro servers are provided by the NIH Center for Information Technology (NIH CIT). NIH protects the confidentiality and integrity of data in transit and at rest. Sensitive data at rest is encrypted to protect its confidentiality with encryption and secured protocol like HTTPS, SSL, TLS, FTPS to ensure integrity. NIH uses HTTPS using TLS 1.2 at the F5 gateway. NIH also uses tools such as Symantec DLP to monitor data exfiltration and Trustwave for content scanning.

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

The full SSN is not visible to most users on the frontend or in the database. For all users except for credentialing supervisor (400-level) and super user (500-level) users, SSNs are masked on the VetPro frontend, with only the first three digits of the SSN visible for identification purposes. SSNs are stored in the VetPro database with encryption.

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

Rules of behavior are required by individuals involved in the design, development, operation, and maintenance of records associated with VetPro information. All supporting personnel are required to complete annual PII/PHI training. Appropriate administrative, technical, and physical safeguards are implemented to insure the security and confidentiality of associated records and protection against threats or hazards to the security or integrity of VetPro PII/PHI information.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

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

2.4a How is access to the PII determined?

Users are granted the access role with the least access to PII which enables the user to complete their required functions in VetPro. If the user only needs access to a specific VHA facility or to a specific provider file in VetPro, then the user's access is restricted to only that VHA facility and/or specific provider file. Users are also only granted access for the period of time in which the user has a need-to-know for the data; and the user's access to the data is expired when access is no longer required.

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

Yes, they are documented in various Standard Operating Procedures (SOPs) published and maintained by the VHA Credentialing and Privileging Office. SOPs include:

- SOP-VMSA2 VetPro Personnel Security/Position Classification
- SOP-VMSA3 VetPro Security Awareness and Training
- SOP-VMSA7 Access Controls in VetPro
- SOP-VMSA8 Facility Level Access Control
- SOP-VMSA12 Sharing Files in VetPro

2.4c Does access require manager approval?

Whether access requires manager approval is dependent on the access role needed by the individual. See Section 8.1a for specific details.

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

The Director, VHA Credentialing and Privileging Office, oversees the monitoring of user activities and access to the VetPro system through scheduled Security Assessment reports. Database administrators assigned to VetPro (VA Office of Information Technology [OIT] employees) monitor activities in the database. If there is unknown activity in the database servers such as unidentified modification in provider data, the Director, VHA Credentialing and Privileging Office is notified, and software developers are requested to investigate the case with the database administrators. Confirmed suspicious activities would be reported to the VHA/ISO officer or facility ISO, as appropriate, for further investigation.

The database administrators use a variety of database tools to assist in this effort. Data tables which hold sensitive information have a corresponding history table recording any update operations performed to the corresponding data table. History tables contain information on date and time of a data change and the identity of the user making that change. Any discrepancies identified by any member of the VA VetPro support team, or issues brought to their attention by end users, would be promptly reported to the Director, VHA Credentialing and Privileging Office for immediately investigation and resolution.

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

All VetPro users and those with access to VetPro data (e.g., VetPro Helpdesk technicians, system administrators) are responsible for safeguarding PII.

Section 3. Retention of Information

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

3.1 What information is retained?

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

Name
Social Security Number
Date of Birth
Mailing Address
Zip Code
Phone Number(s)
Fax Number
Email Address
License/Certificate numbers
Gender
Financial Information

3.2 How long is information retained?

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

The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.

Retention is in accordance with Paper records RCS 10-1 1150.1 and RCS 10-1150.2 reference file #N1-15-10-007 that have been scanned and verified for accuracy are destroyed by in accordance with RCS 10-1 1150.1 and RCS 10-1150.2 reference file #N1-15-10-007.
https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

Electronic files are deleted 30 years after the last episode of employment, appointment, contract, etc. from VA. In the case of applicants not selected for VA employment, appointment, contract, etc., electronic files are deleted 2 years after non-selection or when no longer needed for reference, whichever is sooner.

Paper records are retired to the VA Records Center and Vault (VA RC&V) 3 years after the individual separates from VA employment or when no longer utilized by VA (in some cases, records may be maintained at the facility for a longer period of time) and are destroyed 30 years after separation. Paper records for applicants who are not selected for VA employment or appointment are destroyed 2 years after non-selection or when no longer needed for reference, whichever is sooner.

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

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

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

Yes.

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

VetPro retention schedule is approved in accordance with RCS 10-1 1150.1 and RCS 10-1150.2 reference file #N1-15-10-007. https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

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 files are deleted by the VetPro administrator 30 years after the last episode of employment, appointment, contract, etc. from VA. In the case of applicants not selected for VA employment, appointment, contract, etc., electronic files are deleted 2 years after non-selection or when no longer needed for reference, whichever is sooner.

Paper records are retired to the VA RC&V 3 years after the individual separates from VA employment or when no longer utilized by VA (in some cases, records may be maintained at the facility for a longer period of time) and are destroyed 30 years after separation. Paper records for applicants who are not selected for VA employment or appointment are destroyed 2 years after non-selection or when no longer needed for reference, whichever is sooner. All elimination procedures are approved by NARA.

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.

VetPro only retains the information necessary for its purpose and PII retained only for as long as necessary and relevant to fulfill the specified purposes. Everyone is trained on policies and procedures for how PII is to be used and protected. PII is used to train new coordinators and testing new code for the system enhancements, as needed. PII is not used for research. There are controls are in place to minimize the use of PII. For training and testing, the test facility is created that does not use real PII, in addition the PII used is limited to only first 3 digits or letters.

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

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that the information maintained by VetPro will be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached.

Mitigation: Retention is in accordance with RCS 10-1 1150.1 and RCS 10-1150.2 reference file #N1-15-10-007.Paper records that have been scanned and verified for accuracy are destroyed by in accordance with RCS 10-1 1150.1 and RCS 10-1150.2 reference file #N1-15-10-007.1. Electronic files are deleted 30 years after the last episode of employment, appointment, contract, etc. from VA. In the case of applicants not selected for VA employment, appointment, contract, etc., electronic files are deleted 2 years after non-selection or when no longer needed for reference, whichever is sooner.

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 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: No risk identified. VetPro has no internal sharing and therefore no risk associated with internal sharing and disclosure.

Mitigation: No mitigation identified. VetPro has no internal sharing and therefore no risk associated with internal sharing and disclosure.

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***
National Provider Date Base (NPDB)	To match up to providers for purposes of obtaining NPDB Queries on these providers to learn of any adverse actions, malpractice/tort claims/payments, etc.	SSN, Licensure, Certification, Registration, Education of Providers	Federal contracts are in place to share data 77VA10E2E/ 85 FR 7395 (routine use numbers 4, 18, 21)	SSL (Secure Sockets Layer) to encrypt communications between VetPro and NPDB Uses SOAP (Simple Object Access Protocol) as a messaging protocol that allows programs that run on disparate operating systems (such as Windows and Linux) to communicate using Hypertext Transfer Protocol (HTTP) and its Extensible Markup Language (XML).

Federation of State Medical Boards (FSMB)	To match up to providers for purposes of obtaining FSMB Reports to learn of adverse actions on licensures.	SSN, Licensure, Certification, Registration, Education of Providers	Federal contracts are in place to share data 77VA10E2E/ 85 FR 7395 (routine use numbers 4, 18, 21)	SSL (Secure Sockets Layer) to encrypt communicatio ns between VetPro and NPDB Uses SOAP (Simple Object Access Protocol) as a messaging protocol that allows programs that run on disparate operating systems (such as Windows and Linux) to communicate using Hypertext Transfer Protocol (HTTP) and its Extensible Markup Language (XML).

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

Follow the format below:

Privacy Risk: Sharing of Information Outside of what is permitted by 77VA10E2E/85 FR 7395. The risk that the data could be shared with an inappropriate and/or unauthorized external organization or institution.

Mitigation: Privacy Training is provided to VetPro users on an annual basis which includes coverage of the 24 routine uses. Consultation with the facility level Privacy Officer is recommended prior to release of any information. VetPro uses SSL to encrypt communications between VetPro and NPDB and FSMB. VetPro uses SOAP as a messaging protocol that allows programs that run on disparate operating systems (such as Windows and Linux) to communicate using HTTP and its XML.

Section 6. Notice

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

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

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

6.1a This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

Notice is provided. A Privacy Statement, including reference to the Privacy Act, Title 38 U.S.C., and how the information will be used, is received upon log-in and health care providers sign a Credentialing Release of Information. See attachments in Appendix A 6.1.

77VA10E2E/85 FR 7395
https://www.oprm.va.gov/docs/SORN/Current_SORN_List_05_30_2023.pdf

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

Notice was provided. See attachments in Appendix A 6.1.

6.1c Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

All VetPro users receive the Privacy Statement each time the user logs into VetPro. The Privacy Statement includes how and why the user's data will be used and under which authority.

Additionally, provider users receive and are required to sign the Release of Information in order to begin the credentialing process. The Release of Information includes how and why the provider's data will be used.

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.

No, not if information is provided in accordance with 77VA10E2E/85 FR 7395. Information collected is required in order to obtain or maintain VA employment. If provider chooses not to enter required information this may delay their employment with the VHA.

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.

When individuals submit their information, they are afforded the opportunity to review the Privacy Statement and could choose not to submit the information accordingly. The information provided by them is solely used to verify their credentials and is used to make decision regarding the employment with VA. Providers sign release of information form to consent on how the information is being used.

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 System ISSO to complete all Privacy Risk questions inside the document this section).

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

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

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

Privacy Risk: There is a risk that an individual may not receive notice that their information is being collected, maintained, processed, or disseminated by the VHA prior to providing the information to the VHA.

Mitigation: A Privacy Statement is displayed to every user when they log in to VetPro. Providers also must submit a signed Release of Information Authorization. An initial credentialing letter is sent to providers prior to VetPro access with the details on what information is required and is collected by the VA. 77VA10E2E/85 FR 7395 is also a form of notice, as well as this PIA.

Section 7. Access, Redress, and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

7.1 What are the procedures that allow individuals to gain access to their information?

These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. ***For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.***

A Provider, when requesting access to their record, need to make a request in writing through the Privacy Officer. Also, request can be made to the Director, VHA Credentialing and Privileging Office.

Credentialers are required to maintain a record of any information released from a provider's credentialing records under the authority of the Privacy Act. At minimum, the information to be recorded would include the name of the practitioner whose record is being released, date of the request, description and purpose of the request, name and address of the requestor, and date of response. Common releases that would be recorded would include requests from individuals to see their own credentials files, requests from other medical facilities requesting confirmation of a provider's status at your facility, etc.

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).

VetPro 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.

VetPro 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.

Records are only corrected if there is evidence that the current information in the record is not timely, is irrelevant, and/or inaccurate. To make a change to a record, the provider must make a written request to the Director, VHA Credentialing and Privileging Office, and indicate the specific information to be removed/corrected and why it meets the threshold of not being timely, relevant, and/or accurate. The Director, VHA Credentialing and Privileging Office, makes the determination of whether the permanent record should be modified, remain intact, or be amended.

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.

Individuals requesting correction of their information within VetPro notify the credentialing staff at their facility. The credentialing staff have been trained that they are to contact the VHA Credentialing and Privileging Office with questions and that the request must be submitted in writing by the provider to the Director, VHA Credentialing and Privileging Office explaining what in the file is inaccurate, irrelevant, or not timely, as well as how the information was entered into the file.

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.

The records are reviewed to ensure the information can indeed be removed in accordance with the request from the provider explaining what amendment needs to be made in the file. The provider is provided written notification of the decision to remove/ modify their credentialing record. If the amendment is approved, the VetPro database administrators are provided the information to make the file modification.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

Privacy Risk: Inaccurate, untimely, or irrelevant information contained in a provider's credentialing file. There is a risk that a provider or a volunteer does not know how to obtain access to their records or how to request corrections to their records and that the record could contain inaccurate information and subsequently effect the care the Veteran receives.

Mitigation: Individuals requesting correction of their information within VetPro notify the credentialing staff at their facility. The credentialing staff have been trained that they are to contact the VHA Credentialing and Privileging Office with questions and that the request must be submitted in writing by the provider to the Director, VHA Credentialing and Privileging Office explaining what in the file is inaccurate, irrelevant, or not timely, as well as how the information was entered into the file. The records are reviewed to ensure the information can indeed be removed in accordance with the request from the provider explaining what amendment needs to be made in the file. The provider is provided written notification of the decision to remove/ modify their credentialing record. If the amendment is approved, the VetPro database administrators are provided the information to make the file modification.

Section 8. Technical Access and Security

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

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

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

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

All VetPro users will meet VA computer access requirements and are generally defined as follows:

- Providers (level 50) may or may not be employees, but only have access to information that they are entering in the system, which is in compliance with the Privacy Act.
- Summary Printers (level 75) must have a need to know and will be given access by the Credentialing and Privileging Manager in accordance with the Privacy Act System of Records Notice 77VA10E2E and VA Information Security policy and procedures. These regulations, policies, and procedures may allow access to information, but not access to VA computer systems, in which case a VetPro user with appropriate computer access will retrieve the information.
- Guest users (level 100) must have a need to know and will be given access by facility coordinators in accordance with the Privacy Act System of Records Notice 77VA10E2E and VA Information Security policy and procedures. These regulations, policies, and procedures may allow access to information, but not access to VA computer systems, in which case a VetPro user with the appropriate computer access will retrieve the information.

- Service Chief/Liaison users (level 200) are assigned access by facility coordinators responsible for managing VetPro access to VetPro files. These individuals are Federal employees and have already met Federal requirements of a National Agency Check with written inquiries and all Federal information systems access personnel security requirements with a demonstrated need to know. This level of user is an individual with already established access to VA computer systems. The demonstrated need to know complies with the Privacy Act System of Records Notice 77VA10E2E. Access is usually restricted to the specific file(s) to which the user has demonstrated a need to know. This is a level at which facility review occurs and recommendation for appointment is documented.
- Share Coordinator users (level 250) are assigned access by facility coordinators responsible for managing VetPro access to VetPro files. These individuals are Federal employees and have already met Federal requirements of a National Agency Check with written inquiries and all Federal information systems access personnel security requirements with a demonstrated need to know. This level of user is an individual with already established access to VA computer systems. The demonstrated need to know complies with the Privacy Act System of Records Notice 77VA10E2E. Access is always restricted to the specific file(s) to which the user has demonstrated a need to know. This is a level at which the credentialing work is accomplished.
- Credentialing Specialist (level 300) and Credentialing and Privileging Specialist (level 350) users are assigned access by another facility Specialist or the Credentialing and Privileging Manager responsible for managing VetPro access to VetPro files. These individuals are Federal employees and have already met Federal requirements of a National Agency Check with written inquiries and all Federal information systems access personnel security requirements with a demonstrated need to know. This level of user is an individual with already established access to VA computer systems. The demonstrated need to know complies with the Privacy Act System of Records Notice 77VA10E2E. This is a level at which the credentialing work is accomplished.
- Credentialing and Privileging Manager users (level 400) are assigned by the Director, VHA Credentialing and Privileging Office (or designee) following nomination by appropriate VA facility leadership as the lead representatives for the facility to the VHA Credentialing and Privileging Office. These individuals are Federal employees and have already met Federal requirements of a National Agency Check with written inquiries and all Federal information systems access personnel security requirements with a demonstrated need to know. This level of user is an individual with already established access to VA computer systems. The demonstrated need to know complies with the Privacy Act System of Records Notice 77VA10E2E. This is a level at which the credentialing work is accomplished.
- Super User (level 500) is restricted to staff in the VHA Credentialing and Privileging Office. This level of user is an individual with already established access to VA computer systems and the additional personnel security requirements define in SOP-VMSA2 Personnel Security/Position Classification Policy, including, but not limited to, the submission and favorable adjudication of a full background investigation.

- Maintenance access (level 500) is restricted to staff in the VHA Credentialing and Privileging Office and individuals on contract with the VHA Credentialing and Privileging Office and the appropriate levels of background investigation as defined in the SOP-VMSA6 Acquisition Policy including, but not limited to, the submission and favorable adjudication of a full background investigation.

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?

Auditors from VA Office of Inspector General (VA OIG), Government Accountability Office (GAO), and Joint Commission may be granted Guest (100-level) access to the VHA facilities which are being audited. Auditors are granted restricted access to only those provider files included in the audit.

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.

Role (User level)	**Access to Licensed Independent Practitioner (LIP) Files**	**Access to Non LIP Files**	**Functionality**
Provider (050)	No	No	Access only to their own records
Summary Printer (75)	Restricted	Restricted	Read and print access only for practitioners that have a current appointment at the facility and only to be provided to the Veteran at their request (i.e., surgery patients)
Guest (100)	Restricted	Restricted	Read only access to one or more practitioner files within their account based on a need-to-know.
Service Chief/Director (200)	Restricted	Restricted	▪ Read only access to one or more practitioner files within their account based on a need-to-know. ▪ Write access to the Service Chief Approval screen.
Share Coordinator (250)	Yes Restricted	Yes Restricted	▪ Secondary specialist to access a practitioner's file within the system based on a need-to-know. ▪ Write access to the following: o Verifying credentials in the practitioner's file, o Running reports,

			○ Performing NPDB Continuous Query (CQ) registrations or single queries ○ Performing FSMB queries, ○ Assigning Service Chief approval request, and ○ Entering appointment committee minutes and appointments.
Credentialing Specialist (300)	View only access	Yes	▪ Full read, write, and reports access (described above) to non-LIP practitioner files ▪ View access similar to Guest access (100) to the LIP files ▪ Can enroll new practitioners ▪ Can enroll new user accounts at same or lower access
Credentialing and Privileging Specialist (350)	Yes	Yes	▪ Full read, write, and reports access (described above) to both LIP and non-LIP practitioner files ▪ Can enroll new practitioners ▪ Can enroll new user accounts at same or lower access
Credentialing and Privileging Manager (400)	Yes	Yes	▪ Limited to one (1) per facility ▪ All read, write, and report access (described above) to all practitioner files in the facility ▪ Responsible for maintaining all specialist accounts
Super User (500)	Yes	Yes	▪ Restricted to VetPro Program Staff, VHA Credentialing and Privileging Office and Office of Information and Technology ▪ Same privileges as the Credentialing and Privileging Manager with extended capability to manage account
Maintenance Access (500)	Yes	Yes	▪ Restricted to VetPro Program Staff, VHA Credentialing and Privileging Office, Office of Information and Technology, and contract staff

			▪ Access is through a static IP address registered with external server provider for software and data base management

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.

If they have a "need to know". Contractors are covered by contractual agreements. VetPro is maintained by contract developers who must undergo extensive background checks and complete annual privacy and information security training. Contractors do not make any decisions on design or maintenance, without direct oversight from Program Manager. Contracts are reviewed on the annual basis by the Program Manager and Director of the Program.

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

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

All VA employees and contractors must take the VA Privacy and Information Security Awareness and Rules of Behavior training on an annual basis. All VetPro Security & Confidentiality Training specific to VetPro is provided on an annual basis to all users with 250-level and above access. Privacy Act Training is also provided annually to all users with 250-level access and above in VetPro. Rules of Behavior are electronically signed initially when VetPro access is provided and annually thereafter. Completed templates are sent to all Veterans Integrated Service Network (VISN) Credentialing and Privileging Officers and VISN Support staff in the VHA Credentialing and Privileging Office prior to all credentialers being granted access to VetPro to obtain the completion dates for the annual and initial trainings.

There is also a User Manual for all users provided through the VHA Credentialing and Privileging Office intranet site.

There are Standard Operating Procedures included on the Website as well explaining access, etc.

VA Health Insurance Portability and Accountability Act (HIPAA), Privacy, or Security Awareness training required as well for all VA employees, volunteers, and contractors who use VetPro, in addition to above.

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

Yes.

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 12-Apr-2023
3. *The Authorization Status:* Authorization to Operate (ATO)
4. *The Authorization Date:* 20-May-2023
5. *The Authorization Termination Date:* 16-Nov-2023
6. *The Risk Review Completion Date:* 09-May-2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* High

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

8.4b If No or In Process, provide your ***Initial Operating Capability (IOC) date.***

N/A

Section 9 – Technology Usage

The following questions are used to identify the technologies being used by the IT system or project.

9.1 Does the system use cloud technology? If so, what cloud model is being utilized?

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1*. (Refer to question 3.3.1 of the PTA)*

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). (*Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.*

N/A

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

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

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

N/A

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

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

N/A

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

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

N/A

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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

Signature of Responsible Officials

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

RISTENE MOCKEL

Digitally signed by RISTENE MOCKEL
Date: 2023.08.24 13:48:29 -06'00'

Privacy Officer, Ristene Mockel

Steve M. Cosby 223809

Digitally signed by Steve M. Cosby 223809
Date: 2023.08.24 09:23:42 -04'00'

Information Systems Security Officer, Steve Cosby

Marianne Chick 200135

Digitally signed by Marianne Chick 200135
Date: 2023.08.30 17:48:45 -04'00'

Information Systems Owner, Marianne Chick

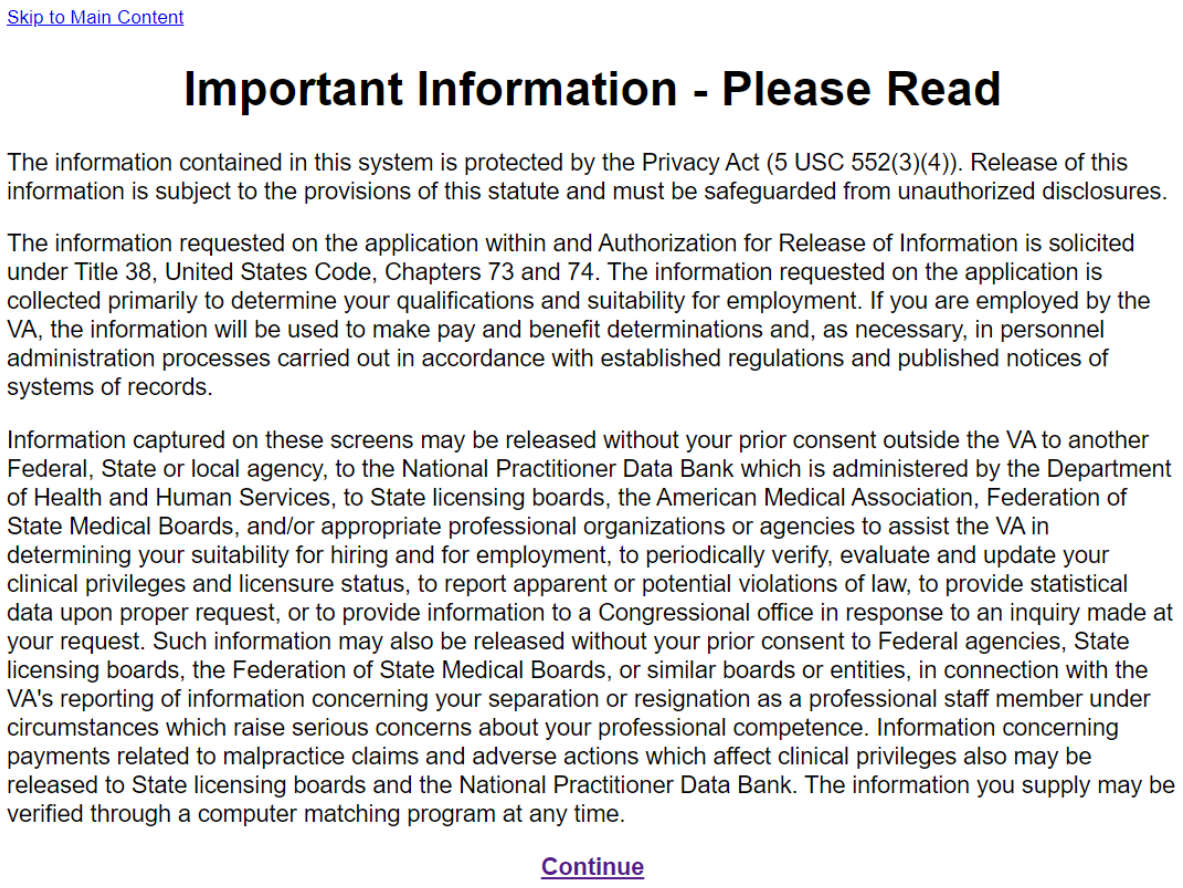
APPENDIX A-6.1

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).

77VA10E2E/85 FR 7395 Health Care Provider Credentialing and Privileging Records-VA:

https://www.federalregister.gov/documents/2020/02/07/2020-02477/privacy-act-of-1974-system-of-records

Privacy Statement is received upon log-in:



Skip to Main Content

Important Information - Please Read

The information contained in this system is protected by the Privacy Act (5 USC 552(3)(4)). Release of this information is subject to the provisions of this statute and must be safeguarded from unauthorized disclosures.

The information requested on the application within and Authorization for Release of Information is solicited under Title 38, United States Code, Chapters 73 and 74. The information requested on the application is collected primarily to determine your qualifications and suitability for employment. If you are employed by the VA, the information will be used to make pay and benefit determinations and, as necessary, in personnel administration processes carried out in accordance with established regulations and published notices of systems of records.

Information captured on these screens may be released without your prior consent outside the VA to another Federal, State or local agency, to the National Practitioner Data Bank which is administered by the Department of Health and Human Services, to State licensing boards, the American Medical Association, Federation of State Medical Boards, and/or appropriate professional organizations or agencies to assist the VA in determining your suitability for hiring and for employment, to periodically verify, evaluate and update your clinical privileges and licensure status, to report apparent or potential violations of law, to provide statistical data upon proper request, or to provide information to a Congressional office in response to an inquiry made at your request. Such information may also be released without your prior consent to Federal agencies, State licensing boards, the Federation of State Medical 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. The information you supply may be verified through a computer matching program at any time.

Continue

Credentialing Release of Information:

Department of Veterans Affairs

Credentialing Release of Information Authorization

In order for the _____ to access and verify my educational
Insert Facility Name

background, professional qualifications and suitability for appointment, I hereby authorize the

_____ to make inquiries and consult with all persons, places of
Insert Facility Name

employment, education, malpractice carriers, State licensing boards, or other similar government and non-governmental entities who have or may have information bearing on my moral, ethical and professional qualifications and competence to carry out the privileges I have requested.

I consent to the release of information about my ability and fitness for Federal appointment and I authorize release of such information and copies of related records and/or documents to VA officials to include not only the requested information for verification but information concerning each lawsuit, civil action, or other claim brought against me for malpractice or negligence; each disciplinary action under consideration or taken; any open or previously concluded investigations; and any changes in the status of a credential and all supporting documentation related to the information provided.

I authorize the VA to disclose to such persons, employers, institutions, boards or agencies identifying and other information about me sufficient to enable the VA to make such inquiries.

I release from liability all those who provide information to the Department of Veterans Affairs in good faith and without malice in response to such inquiries.

Full Name	Date

Signature

VA FORM JAN 2008 **10-0459**

HELPFUL LINKS:

Record Control Schedules:

https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

General Records Schedule 1.1: Financial Management and Reporting Records (FSC):

https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

National Archives (Federal Records Management):

https://www.archives.gov/records-mgmt/grs

VHA Publications:

https://www.va.gov/vhapublications/publications.cfm?Pub=2

VA Privacy Service Privacy Hub:

https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices