The completion of Veterans Affairs Privacy Impact Assessments (PIAs) is mandated for any rulemaking, program, system, or practice that collects or uses PII under the authority of the E-government Act of 2002 (44 U.S.C. § 208(b)) and VA Directive 6508, Implementation of Privacy Threshold Analysis and Privacy Impact Assessment.

The PIA is designed to identify risk associated with the use of PII by a system, program, project or practice, and to ensure that vital data stewardship issues are addressed for all phases of the System Development Life Cycle (SDLC) of IT systems. It also ensures that privacy protections are built into an IT system during its development cycle. By regularly assessing privacy concerns during the development process, VA ensures that proponents of a program or technology have taken its potential privacy impact into account from the beginning. The PIA also serves to help identify what level of security risk is associated with a program or technology. In turn, this allows the Department to properly manage the security requirements under the Federal Information Security Management Act (FISMA).


Please note that the E-government Act of 2002 requires that a PIA be made available to the public. In order to comply with this requirement PIA will be published online for the general public to view. When completing this document please use simple, straight-forward language, avoid overly technical terminology, and write out acronyms the first time you use them to ensure that the document can be read and understood by the general public.
Privacy Impact Assessment for the VA IT System called:

<<VetPro Major Application>>
<<Office of Medical Staff Affairs >>

Date PIA submitted for review:

<< 7/28/2020 >>

System Contact

<table>
<thead>
<tr>
<th>Name</th>
<th>E-mail</th>
<th>Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Officer</td>
<td>Karen Strobel</td>
<td>518-275-6021</td>
</tr>
<tr>
<td>Information System Security Officer</td>
<td>Steve Cosby</td>
<td>919-474-3924</td>
</tr>
<tr>
<td>Information System Owner</td>
<td>Marianne Chick</td>
<td>919-474-3937</td>
</tr>
</tbody>
</table>
Abstract

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

VetPro is VHA’s credentialing internet-based software platform that is used for required credentialing of healthcare providers who require license, registration, or certification to qualify for their respective occupation. The system contains primary source verifications of the provider’s education, training, licensure, certification, work history, and clinical references. This electronic credentialing system facilitates uniform, accurate, and complete credentialing files to meet VHA’s and external accreditation body’s (e.g., The Joint Commission) requirements and standards.

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.
- The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.
- If your system is a regional GSS, VistA, or LAN, include a list of the hospitals/medical centers, or other regional offices that fall under your system. Additionally, what region is the system under?
- A general description of the information in the IT system.
- 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?
- Does the system use cloud technology? 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.
- Does a contract with Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII?
• 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 is the magnitude of harm if privacy related data is disclosed, intentionally or unintentionally? Would the reputation of the CSP or its customers (VA) be affected?

The VetPro Application is managed service major application used by all VHA Facilities for the credentialing of all VHA Licensed, and/or certified, registered health care providers this includes contractors and volunteers. The Veterans Health Administration (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 domiciliaries organized into 141 medical staffs.

Each VA 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.

Currently there over 50,000 individuals that have their information stored in VetPro. The information is shared between VA facilities internally and with the NPDB (National Practitioners Data Bank) and FSMB (Federation of State Medical Boards) 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

The VetPro Application shows that it is possible to create, validate and maintain an electronic credentials data file of verified data in a readily accessible and retrievable manner. VetPro legal Authority to operate is 77VA10E2E and Title 38 U.S.C. 501(a) and section 7304(a)(2)

Completion of the PIA will not result in business or technology changes or require the SORN to be amended.
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.

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:

- [x] Name
- [x] Social Security Number
- [x] Date of Birth
- [ ] Mother’s Maiden Name
- [x] Personal Mailing Address
- [x] Personal Phone Number(s)
- [x] Personal Fax Number
- [x] Personal Email Address
- [ ] Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- [ ] Financial Account Information
- [ ] Health Insurance Beneficiary Numbers Account numbers
- [x] 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
- [x] Other Unique Identifying Number (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.

PII Mapping of Components

<VetPro> consists of 0 key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by <VetPro> and the reasons for the collection of the PII are in the table below.
PII Mapped to Components

<table>
<thead>
<tr>
<th>Components of the information system (servers) collecting/storing PII</th>
<th>Does this system collect PII? (Yes/No)</th>
<th>Does this system store PII? (Yes/No)</th>
<th>Type of PII (SSN, DOB, etc.)</th>
<th>Reason for Collection/Storage of PII</th>
<th>Safeguards</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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?

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.

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.

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 National Practitioner Data Bank and the Federation of State Medical Boards 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).
1.3 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.

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 National Practitioner Data Bank and the Federation of State Medical Boards for purposes of ordering and receiving reports on the credentialed providers.

1.4 What is the purpose of the information being collected, used, disseminated, created, or maintained?

Include a statement of why the particular SPI is collected, maintained, used, or disseminated in the system is necessary to the program's or agency's mission. Merely stating the general purpose of the system without explaining why this particular type of information should be collected and stored is not an adequate response to this question.

If the system collects, uses, disseminates, or maintains publicly available or commercial data, include a discussion of why commercial data is relevant and necessary to the system’s purpose.

This question is related to privacy control AP-2, Purpose Specification.

The information being collected, used, disseminated, created, or maintained by and through VetPro is used to complete the credentialing process appropriately. Provider enters this information into VetPro.

The use of the information being collected, used, disseminated, created or maintained is essential to patient safety and to the credentialing process. The information is being collected in order to enter providers in VetPro system and provide successful credentialing, thus identifying and verifying that the information entered by the provider is correct. The information is verified against educational institutions, licenses boards and past employment history. VetPro coordinators contact licensing board and education institutions outside of VetPro to verify this information. There is information that is send to National Practitioner Data Bank and the Federation of State Medical Boards to obtain additional Verification.
1.5 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.

There are various audits performed by the facility and Medical Staff Affairs to ensure the information is accurate. Information is checked against scan documents and outside sources like licensing boards to confirm the validity if entered data.

1.6 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).

1.7 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

Principle of Purpose Specification: 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 VHA Director, Medical Staff Affairs 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 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 VHA Director, Medical Staff Affairs for appropriate resolution or escalation.

**Section 2. Uses of the Information**

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

**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

This information is used to verify that the providers who are hired by the VA have the qualification they claim to have. The education institutions and past employment companies are contacted by mail or on the phone to verify this information

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

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.

2.3 PRIVACY IMPACT ASSESSMENT: Use of the information. 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. 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.

The information is covered through the Privacy Act of 1974, System of Records. Specifically, the “Health Care Provider Credentialing and Privileging Records – VA 77VA10E2E). 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; and, employee disciplinary or other adverse action, including discharge. The records and information may be used for statistical analysis, to produce various management reports, evaluate services, collection, distribution and utilization of resources, and provide clinical and administrative support to patient medical care. Only authorized users who completed VetPro security training can access VetPro and required manager approval. Providers are given access by coordinator to access their file to enter or update the information for a certain time period only after the HR confirms appointment.

The VHA Director, Medical Staff Affairs oversees the monitoring of user activities and access to the VetPro system through scheduled Security Assessment reports. Database Administrators assigned to VetPro (OI&T employees) monitor activities in the database. If there is unknown activity in the database servers such as unidentified modification in provider data, the Director, Medical Staff Affairs 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 ID 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 VHA Director, Medical Staff Affairs for immediate investigation and resolution. Credentialing Coordinators check the system for accuracy by verifying information entered by provider by directly contacting the organizations. They verify SSN number by checking the SSN
card. In addition, education, license, past employment history is verified by Primary Source Verifications to make sure names and dates matches.

**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

**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. 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. 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)? 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.

VetPro retention schedule is approved in accordance with RCS 10-1150.1 and RCS 10-1150.2 reference file #N1-15-10-007.

3.4 What are the procedures for the elimination of SPI?

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 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. 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. 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

VetPro only retains the information necessary for its purpose, 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 PRIVACY IMPACT ASSESSMENT: Retention of information
Discuss the risks associated with the length of time data is retained and what steps, if any, are
currently being taken to mitigate those identified risks.

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

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

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

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

Follow the format below:
Privacy Risk: 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. NOTE: Question 5 on Privacy Threshold Analysis should be used to answer this question.

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

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

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

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

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?

This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

<table>
<thead>
<tr>
<th>List the Program Office or IT System information is shared/received with</th>
<th>List the purpose of the information being shared/received with the specified program office or IT system</th>
<th>List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT system</th>
<th>Describe the method of transmittal</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.

This question is related to privacy control UL-1, Internal Use.
Follow the format below:

**Privacy Risk:** There is a risk that the data could be shared with an inappropriate VA organization or institution which would have a potentially catastrophic impact on privacy.

**Mitigation:** All VetPro users must complete annual Privacy Act training. Additionally, internal security monitoring is in place related to individuals who have access to the system and their current “need to know” and ensuring individuals do not have access to the system for longer than policy permits. All requests for access to information go thru the Privacy officer or the Program director. All users are required to complete annual security training to make sure the information in VetPro is used properly.

**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:** This question is #7 in the Privacy Threshold Analysis.

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.
<table>
<thead>
<tr>
<th>List External Program Office or IT System information is shared/received with</th>
<th>List the purpose of information being shared/received/transmitted with the specified program office or IT system</th>
<th>List the specific data element types such as PII/PHI that are shared/received with the Program or IT system</th>
<th>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</th>
<th>List the method of transmission and the measures in place to secure data</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>National Provider Date Base (NPDB)</strong></td>
<td>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.</td>
<td>SSN, Licensure, Certification, Registration, Education of Providers</td>
<td>Federal contracts are in place to share data 77VA10E2E (routine use numbers 4, 18, 21)</td>
<td>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).</td>
</tr>
<tr>
<td><strong>Federation of State Medical Boards (FSMB)</strong></td>
<td>To match up to providers for purposes of obtaining FSMB Reports to learn of adverse actions on licensures.</td>
<td>SSN, Licensure, Certification, Registration, Education of Providers</td>
<td>Federal Contract are in Place to share data 77VA10E2E routine use numbers 4, 18, 21)</td>
<td>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</td>
</tr>
</tbody>
</table>
If specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16, note them here.

N/A

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum Of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.

Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.

This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing.

Follow the format below:

<table>
<thead>
<tr>
<th>List External Program Office or IT System information is shared/received with</th>
<th>List the purpose of information being shared/received/transmitted with the specified program office or IT system</th>
<th>List the specific data element types such as PII/PHI that are shared/received with the Program or IT system</th>
<th>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</th>
<th>List the method of transmission and the measures in place to secure data</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>(such as Windows and Linux) to communicate using Hypertext Transfer Protocol (HTTP) and its Extensible Markup Language (XML).</td>
<td></td>
</tr>
</tbody>
</table>
**Privacy Risk:** Sharing of Information Outside of what is permitted by 77VA10A4. 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. SSL (Secure Sockets Layer) to encrypt communications between VetPro and NPDB and FSMB. 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).

**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.*

SORN for the system is 77VA10E2E.

[https://www.govinfo.gov/content/pkg/FR-2020-02-07/pdf/2020-02477.pdf](https://www.govinfo.gov/content/pkg/FR-2020-02-07/pdf/2020-02477.pdf)

A Privacy Statement displays upon log-in:

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. Additionally, providers must sign a Release of Information with the following wording in order to be credentialed as required for their VA position:

**Credentialed Release of Information Authorization**

In order for the ___________ to access and verify my educational background, professional qualifications and suitability for appointment, I hereby authorize the ___________ to make inquiries and consult with all persons, places of 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 and Signature required.

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. 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 have been 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 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks.

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

**Principle of Transparency:** Has sufficient notice been provided to the individual?

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

Follow the format below:

**Privacy Risk:** There is a risk that an individual may not receive notice that their information is being collected, maintained, processed, or disseminated by the Veterans’ Health Administration 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. SORN 77VA10E2E 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?

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.

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, Medical Staff Affairs. 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.

7.2 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 it is not timely, irrelevant, or inaccurate. To make a change to a record, the provider must make a written request to the Director, Medical Staff Affairs and indicate the specific information to be removed/corrected and why it meets the threshold of being not timely, irrelevant, or inaccurate. The Director, Medical Staff Affairs makes the determination of whether the permanent record should be modified, remain intact, or 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 Office of Medical Staff Affairs with questions and that the request must be submitted in writing by the provider to the Director of Medical Staff Affairs 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. 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 ensure data accuracy.

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.

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 Office of Medical Staff Affairs with questions and that the request must be submitted in writing by the provider to the Director of Medical Staff Affairs 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?

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.

ROLES AND RESPONSIBILITIES:
a. The VHA Director is responsible for determining the access to VetPro of individuals who have a need to enter the system in accordance with statute, regulation, and VA policy and procedures, including but, not limited to the Privacy Act System of Records Notice 77VA10A, and information security. The Director develops protocol to authorize user accounts for lead Credentialers at each facility. The Director ensures completion of a review of all user level access above the level of individual provider is completed by each facility at least once a quarter, or more frequently when indicated.

b. Facility level lead Credentialers at each facility are responsible for determining the access to VetPro of individuals who have a need to enter the system in accordance with statute, regulation, and VA policy and procedures, including, but not limited to the Privacy Act System of Records Notice 77VA10A, and information security. Facility level lead Credentialers are also responsible for reviewing all user level access above the level of individual provider at least once a quarter, or more frequently when indicated by the OQSV (Office of Quality, Safety and Value) staff.

c. VetPro users are responsible for assuring reasonable measures are taken to safeguard personal authenticators for the VetPro system, including, but not limited to maintaining possession of personal individual log-on and password information. VetPro users are responsible for not loaning or sharing personal authenticators with others and immediately reporting lost or compromised authenticators to the Director, Credentialing and Privileging. VetPro users are also responsible for reading and attesting to compliancy of the VetPro Rules of Behavior.

Length of Access: Access will be granted to VetPro users for the length of time necessary to accomplish required tasks. In those instances where access needs to be renewed or extended, such action will be taken by a user with a higher level of access who confirms the individual’s need to access VetPro as well as the individual’s identity in accordance with the VetPro Policy – 9, Responding To Requests For Access and Password Assistance. General guidelines for access are:

1. Provider access is automatically set by VetPro to 45 days upon enrollment or action that reopens a file for update, credentialing, or reclassification. If access needs to be extended, it will be extended by a coordinator or higher level for the length of time necessary to complete the electronic submission process but should not exceed 90-days or the expiration of the provider’s current appointment, whichever is shorter.

2. Guest users should be given access only for the length of time necessary to complete the necessary actions for which access is given, but should not exceed 12 months. If access needs to be extended, it will be extended by a coordinator or higher level for the length of time necessary to complete the necessary actions but should not exceed 12 months.

3. Service Chief/Liaison should be given access for the period the individual holds the position and requires access to the credentialing files but should not exceed 24 months. If access needs to be extended, it will be extended by a coordinator or higher level for the length of time necessary but should not exceed 24 months.

4. Share Coordinator users should be given access for a period not to exceed 24 months. If the share coordinator holds their position for less than 24 months or for requires less than 24 months to complete required actions and the length of shared appointments the required period of access should be reflected accordingly. In those instances where the shared access is to facilitate the transfer of a provider, the access at the primary facility will terminate upon transfer to the receiving facility. If access needs to be extended, it will be extended by a coordinator or higher
level for the length of time necessary but should not exceed 24 months. Access at this level must be restricted.

(5) Coordinator users should be given access for the period of time the individual holds the position and requires access to the credentialing files but should not exceed 24 months. If access needs to be extended, it will be extended by another Coordinator or a Supervisor for the length of time necessary but not to exceed 24 months.

(6) Supervisor users should be given access for the period of time the individual holds the position and requires access to the credentialing files but should not exceed 24 months. If access needs to be extended, it will be extended by another Supervisor or member of the VetPro Help Desk team for the length of time necessary but not to exceed 24 months.

d. Termination of access:

(1) For all Providers, access expires in 45 days from the time of enrollment or password change/expiration.

(2) Facility level user access will be terminated by the Supervisor at the facility upon departure of the user from a position with need to know requirements. This will be accomplished by expiring the account on the User/Staff Maintenance Screen, under Staff Tab. If the user had restricted access, access to individual provider files must also be expired on the User/Staff Maintenance Screen, Staff Tab by clicking the “Click here to enter/update Access Restrictions” link. To expire access to a specific file, click the box by the provider’s name and the screen opens displaying an “Expiration Date” field that can be modified. Enter a date of today or earlier and click the “Update” button in accordance with VetPro Policy 7, Access to VetPro.

e. Access monitoring – Facility level access will be monitored by the Supervisor at the facility for the appropriateness of user accounts and continuation of access.

f. Personnel security requirements for access – All VetPro Users will meet VA computer access requirements and are generally defined as follows.

(1) 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.

(2) 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 77VA10Q 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.

(3) 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 77VA10Q. 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.

(4) Share Coordinator users (level 250) are assigned access by the facility coordinators responsible for managing VetPro access to VetPro provider 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 77VA10Q. 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.

(5) Coordinator users (level 300) are assigned access by another facility coordinator or the Supervisor responsible for managing VetPro access to VetPro provider 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 77VA10Q. This is a level at which the credentialing work is accomplished.

(6) Supervisor users (level 400) are assigned by the Director, Credentialing and Privileging (or designee), following nomination by the appropriate VA facility leadership as the lead representatives for the facility to the Office of Safety and Risk Awareness, Veterans Health Administration. 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 77VA10Q. This is a level at which the credentialing work is accomplished.

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 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 the BAA 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.*

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.

VetPro Security & Confidentiality Training is specific to VetPro training is provided on an annual basis to all users with 250 and above access. Privacy Act Training is also provided annually to all users with 250 access and above in VetPro. Rules of Behavior are electronically signed initially when access is provided. Templates are sent to all VISN Liaisons 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 provided through the Medical Staff Affair Website for all users. There are Standard Operating Procedures included on the Website as well explaining access, etc. VA HIPAA, Privacy, or Security Awareness training required as well for all VA employees, volunteers and contractors in addition to above.

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

*If Yes, provide:*

1. The date the Authority to Operate (ATO) was granted,
2. Whether it was a full ATO or ATO with Conditions,
3. The amount of time the ATO was granted for, and
4. 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.*

ATO with conditions was granted. Authorization Termination Date: 19-Mar-2021, granted 20-MAR-2020. IPS 199 classification is HIGH
## Section 9. References

### Summary of Privacy Controls by Family

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

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

Karen A Strobel
164963
Digitally signed by Karen A Strobel 164963
Date: 2020.09.16 11:54:00 -04'00'
Privacy Officer, Karen Strobel

Steve M. Cosby
223809
Digitally signed by Steve M. Cosby 223809
Date: 2020.09.17 08:41:32 -04'00'
Information Security Systems Officer, Steve Cosby

Marianne Chick
200135
Digitally signed by Marianne Chick 200135
Date: 2020.09.16 15:18:44 -04'00'
Information System 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).