Privacy Impact Assessment for the VA IT System called:

Automated Standardized Performance Elements Nationwide (ASPEN)

Veterans Benefits Administration

Office of Field Operations Office of Field Operations

Date PIA submitted for review:

3/22/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Jean-Claude Wicks	Jean-Claude.Wicks@va.gov	202-502-0084
Information System Security Officer (ISSO)	Amy Gallagher	Amy.Gallagher@va.gov Amy.Gallagher@va.gov	727-319-5992
Information System Owner	Miosha Newbill	Miosha.Newbill@va.gov	512-326-6016

Abstract

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

Automated Standardized Performance Elements Nationwide (ASPEN) is an intranet web-based automated performance measurement system for the Department of Veterans Affairs, Veterans Benefit Administration, Office of Field Operations. ASPEN enables VBA to track employee, station, and nationwide performance. ASPEN centralizes performance data, facilitates performance management and quality review functionality, and provides web-based reports for workload management and quality, to determine trend analysis for Veteran Service Center (VSC) employees, including out-based/off-site employees. Employee metrics are tracked for productivity, quality, workload management, authorization timeliness, and customer service. Employee, station, and nationwide performance.

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.

Automated Standardized Performance Elements Nationwide (ASPEN) is owned by Product Line Management (Miosha Newbill)

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

ASPEN is an intranet web-based automated performance measurement system for the Department of Veterans Affairs, Veterans Benefit Administration, Office of Field Operations. ASPEN enables VBA to track employee, station, and nationwide performance. ASPEN centralizes performance data, facilitates performance management and quality review functionality, and provides web-based reports for workload management and quality, to determine trend analysis for Veteran Service Center (VSC) employees, including out-based/off-site employees. Employee metrics are tracked for productivity, quality, workload management, authorization timeliness, and customer service.

ASPEN is made up of 2 Virtual Production Servers and 1 Database SQL Server. ASPEN is using a Microsoft Windows Server 2012 Operating System with a SQL Server 2012 Database and Microsoft Web IIS.

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

VA Owned and VA Operated ISVA Owned and VA Operated IS

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.

15,000 users comprised of employees, supervisors, and quality reviewers in Veterans Service Centers at VBA VAROs.15,000 users comprised of employees, supervisors, and quality reviewers in Veterans Service Centers at VBA VAROs.

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

ASPEN tracks employee's metrics for productivity, quality, workload management, authorization timeliness, and customer service. Productivity is tracked by calculating weighted benefit actions input by the employee against the available time from the employee's work schedule (daily productivity equals actions divided by time multiplied times eight-hour baseline). Quality is tracked by supervisor/reviewers conducting quality reviews based on review questions by employee type to determine if the actions taken were appropriate and correct. Workload management, timeliness, and customer service are metrics tracked by exception. ASPEN contains PII, such as employee name, employee VA email, address, account name, and approximately 15 million unique VA claim numbers. ASPEN shares information with an internal VA System entitled VBA Data Management Warehouse.

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

ASPEN contains PII, such as employee name, employee VA email, address, account name, and approximately 15 million unique VA claim numbers. ASPEN shares information with an internal VA System entitled VBA Data Management Warehouse.

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.

ASPEN is located at a single site of the Philadelphia Information Technology Center (PITC). ASPEN is located at a single site of the Philadelphia Information Technology Center (PITC).

3. Legal Authority and SORN

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

SORN 58VA21/22/28 Compensation Pension Education and Vocational Rehabilitation and Employment Records. SORN 58VA21/22/28 Compensation Pension Education and Vocational Rehabilitation and Employment Records.

The Privacy Act of 1974, set forth at 5 U.S.C. 552a, states the legal authority to utilize this information. As per the SORN, The U.S. government is authorized to ask for this information under Executive Orders 9397, 10450, 10865, 12333, and 12356; sections 3301 and 9101 of title 5, U.S. Code; sections 2165 and 2201 of title 42, U.S. Code; sections 781 to 887 of title 50, U.S. Code; parts 5, 732, and 736 of title 5, Code of Federal Regulations; and Homeland Security Presidential Directive 12.

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

No further known SORN updates are known to be required at this time. ASPEN 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*

At this time, no changes are known to be required of the business processes as a result of this of this PIA.

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

no changes are known to be required of ASPEN no changes are known to be required of ASPEN

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)

- Other: Active Directory Account ID, Claim number, Account ID Name, Work Email Address, Active Directory (AD) account name

PII Mapping of Components (Servers/Database)

ASPEN consists of 1 key component database (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by ASPEN 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
ASPEN	Yes	Yes	Employee Name, Claim number	PII is collected to track employee performance and quality on a per claim basis	VA Network Only which requires two factor authentication access is controlled by Role Based Access (RBAC)

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?

ASPEN receives information directly from the user interface. Employee users enter their weighted production actions which include VA claim numbers which could be SSNs. No employee SSNs are used. Weighted production actions are benefit actions taken by the employee which have a descriptive type and assigned weight by the Veterans Benefits Administration (VBA). Total weight is used in calculating productivity. (Example Claim Establishment – CEST, weight 0.1)

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.

ASPEN does not collect information from sources other than individuals.

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

ASPEN produces productivity and quality reports by aggregating the data collected within from the employees.

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?

ASPEN collects information solely through the user interface. ASPEN collects information solely through the user interface.

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.

N/A

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.

As information is input by the employees related to production actions and exclude time, ASPEN is has built in functionality so supervisors and reviewers are required to validate exclude time and production actions accordingly. Records are marked as validated or quality review completed or not valid in ASPEN accordingly. ASPEN data is manually validated by the supervisors and reviewers by manual comparison against leave records and case files accordingly. Data is validated at least monthly and for every quality review established. rated or quality review completed or not valid in ASPEN accordingly.

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.

As information is input by the employees related to production actions and exclude time, ASPEN is designed so supervisors and reviewers are required to validate exclude time and production actions accordingly. Records are marked as validated or quality review completed or not valid in ASPEN accordingly. ASPEN data is manually validated by the supervisors and reviewers by manual comparison against leave records and case files accordingly. Data is validated at least monthly and for every quality review established. ASPEN does not use a commercial aggregator. ASPEN does not use a commercial aggregator.

1.5 What specific legal authorities, arrangements, and agreements defined the collection of information?

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders. This question is related to privacy control AP-1, Authority to Collect

The full legal authority to operate ASPEN is established in SORN 58VA21/22/28 Compensation Pension Education and Vocational Rehabilitation and Employment Records

The Privacy Act of 1974, set forth at 5 U.S.C. 552a, states the legal authority to utilize this information. As per the SORN, The U.S. government is authorized to ask for this information under Executive Orders 9397, 10450, 10865, 12333, and 12356; sections 3301 and 9101 of title 5, U.S. Code; sections 2165 and 2201 of title 42, U.S. Code; sections 781 to 887 of title 50, U.S. Code; parts 5, 732, and 736 of title 5, Code of Federal Regulations; and Homeland Security Presidential Directive 12.

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

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks. (*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: ASPEN collects PII in the forms of employee name and email, as well VA claim numbers (SSNs) on a per production action basis. If employee performance or quality information were compromised, then bad actors would potentially know what employees were meeting or not meeting production and quality standards set by VA. Bad actors would also have access to large amounts of claim numbers, but no other PII is stored in the weighted production action records to make any association with the raw claim number.

Mitigation: Because of the nature of ASPEN, only employees and supervisors with a need to know have access to employee productivity and quality data. ASPEN follows best practices in controls dictated in NIST 800-53 and VA Directive and handbook 6500 for securing the information system and data. ASPEN requires two factor authentications, and employs: Role Based Access Controls (RBAC), Secure Socket Layer (SSL), encryption at rest, tested Open Web Application Security Project (OWASP) best practices, audit logging, and system timeouts.

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.

ASPEN collects information for the purpose to track and report on employee production and quality performance used directly by VA to conduct employee performance measurement and review. Employee's Name: Used to track productivity and quality to the employee Employee's email: Used to track productivity and quality to the employee Claim Number (SSN): Used to track and validate productivity and quality to the claim-based action performed by the employee. Account ID: Used to track individuals that utilize this system.

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.

ASPEN calculates information related to employee production performance and quality. This information is used by supervisors to complete employee performance summary and final ratings. The calculation is provided upon request of report, but no new record is created. Matching and confirmation is done by supervisors and reviews on a per record basis for quality reviews and monthly for performance metrics is created.

2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

The employee production performance and quality reports generated are used to inform supervisors and employees of employee performance against their standards. Supervisors discuss employee performance as part of the Performance is employed to ensure only the employee's supervisor has access to their respective employees' data. management processes.
RBAC is employed to ensure only the employee's supervisor has access to their respective employees' data.

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?

The Data is kept internal to the VA ASPEN implements cryptographic mechanisms to protect data in transit and at rest. ASPEN utilized FIPS 140-2 HTTPS certificate-based encryption to protect data in transit, and also implements encryption at rest of the entire database. ASPEN implements cryptographic mechanisms to protect data in transit and at rest. ASPEN utilized FIPS 140-2 HTTPS certificate-based encryption to protect data in transit, and also implements encryption at rest of the entire database.

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

Yes, SSNs collecting in regard to veterans claims numbers on production actions are further protected from disclosure by employing RBAC which only allows the employee who entered the production action and his/her immediate supervisor access to view the aim numbers. Data is protected at rest and in transit by FIPS 140-2 HTTPS certificate-based and full database encryption. ASPEN employs multifactor authentication using SSOi PIV authentication where re-authentication occurs at regular intervals between the application layer and SSOi IAM. claim numbers.

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

This question is related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest PII is protected in accordance with OMB M-06-15. All employees in VA must complete annual Cyber Security Awareness an AC which only allows the employee who entered the production action and his/her immediate supervisor access to view the claim numbers. Data is protected at rest and in transit by FIPS 140-2 HTTPS certificate-based and full database encryption. ASPEN employs multifactor authentication using SSOi PIV authentication where re-authentication occurs at regular intervals between the application layer and SSOi IAMd Rules of Behavior training so their role in protecting PII is well understood. PII is further protected from disclosure by employing RBAC.

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?

The minimum-security requirements for ASPEN's moderate impact system cover 17 security-related areas regarding protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas include: access control; awareness and training; audit and accountability; assessment, authorization, and security assessments; configuration management; contingency planning; identification and authentication. incident response; maintenance; media protection; physical and environmental protection; planning. personnel security; risk assessment; systems and services acquisition; system communications protection; system and information integrity. ASPEN employs all security controls in the respective moderate impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 and specific VA directives like the following, 6510 Identity and Access Management, 6508 Implementation of Privacy Threshold Analysis and Privacy Impact Assessment, 6403 Software Asset Management, 6309 Collections of Information, 6300 Records and Information Management, 0710 Personnel Security and Suitability Program. All personnel (employees and contractors) that work on the system complete and sign the VA Rules of Behavior. Access to ASPEN requires supervisor approval and supervisor/review access is assigned by the Regional Office and further reduced by the work team. Access to data in ASPEN is based on built in functionality of Role Based Access Controls (RBAC) where users and supervisor can only see data assigned to them. Procedures and responsibilities for access are documented in the ASPEN users guide. Access controls, monitoring, and safeguard of PII are documented in the appropriate Access Control (AC) family in the ASPEN System Security Plan (SSP).

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

Yes, criteria, procedures, controls, and responsibilities regarding access are documented in the ASPEN users guide.

2.4c Does access require manager approval?

Yes Access to ASPEN requires Manager approval.

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

yes SSOi and ASPEN employ logging capabilities to track access to the information system.

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

ISOS Safeguarding PII is the responsibility of the information system owner, information system security officer, and privacy officer. All users of ASPEN are required by the VA Rules of Behavior to protect PII data from disclosure.

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*

The following information is retained by ASPEN: Name, Social Security Number, Email and Account ID.

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.*

As performance records are necessary as part of the supervisor's personnel files to document employee's annual performance reviews, all ASPEN data is retained at this time. Occasional archive of prior years is conducted based on database growth and performance requirements, in those cases summary archived reports are made available at the supervisor/reviewer level. Currently, FY2006-FY2015 are archived and retained on-line for access requirements, in those cases summary archived reports are made available at the supervisor/reviewer level.

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

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

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

Yes

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

These records are retained and disposed of in accordance with the General Records Schedule 2.2 (080) approved by National Archives and Records Administration (NARA) https://www.archives.gov/records-mgmt/grs.html

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.

Records/digital information will be eliminated following the sanitization procedures in VA Handbook 6300.1 Records Management Procedures and VA Handbook 6500.1 Electronic Media Sanitization. Records will not be eliminated until decommissioning at which time it will follow the process outlined in 6500.1.me it will follow the process outlined in 6500.1.

3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

ASPEN does not use PII in its research, testing or pre-production environments, nor is it used for training or research.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

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

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

Follow the format below:

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

Mitigation: To mitigate the risks of information retention, ASPEN adheres to NARA Records Control Schedule. When a records retention date is reached, the individuals' information is disposed of.

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***
Veterans Benefits Administration	The VBA Office of PA&I uses the information to aggregate performance across employee type (VSR, RVSR, etc) and Stations for forecasting purposes.	Claim number. Production count, weight, employee name, employee total hours	SQL ODBC connection

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: Maintaining PII poses the risk that data could be shared in the VA and the data may be disclosed to individuals not requiring access, increasing the risk of misused information.

Mitigation: The potential harm is mitigated by access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information integrity, security assessment and authorization, incident response, risk assessment, planning and maintenance, accountability, audit and risk management, data quality and integrity, data minimization and retention, individual participation and redress, need-to-know, transparency and use limitation.

For elevated privileges, Electronic Permission Access System (ePAS) mitigates the risk of inadvertently sharing or disclosing information by assigning access permissions based on need to know. Only personnel with a clear business purpose for accessing the information are allowed to access ASPEN and the information contained within.

The use of a Personal Identity Verification (PIV) card is implemented. This ensures the identity of the user by requiring two-factor authentication. All user level employee's must be approved by their supervisor and are assigned to a specific Regional Office and team to ensure least privilege.

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.

ASPEN does not share information with any external organization.

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

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

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

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

Data Shared with External Organizations

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

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: ASPEN does not share data with external entities to VA.

Mitigation: N/A

Section 6. Notice

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

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

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

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

Information related to employment such as performance metrics may be collected, and employees are notified via their performance standards. Employees are notified of their performance standards via VA Form 0750- Performance Appraisal.

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

Please provide response here a) VA Agency has a privacy policy located at to generically provide privacy notice to all individuals who may interact with VA on the VA.GOV website. In addition, VBA provide additional notice via the SORN and PIA postings. b) within all System of Records Notices published. c) VBA routinely updates SORNs for altered system of record that include major changes or changes in the routine use. See the enclosed evidence screen shots of OPRM review web pages and current list of SORNs updated 11/23/2021. VA web sites: OPRM Intranet
https://vaww.oprm.va.gov/privacy/systems_of_records.aspxhttps://vaww.oprm.va.gov/docs/Current_SORN_List_11_23_2021.pdf

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.

Please provide response here See 6.1b.See 6.1b.

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.

While employees may decline to provide information, tracking performance may be hindered as employee's are compelled to report work products completed to their supervisors as a condition of employee performance standards. There is no penalty or denial of service attached service attached While employees may decline to provide information, tracking performance may be hindered as employee's are compelled to report work products completed to their supervisors as a condition of employee performance standards. There is no penalty or denial of service.

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.

While employees may have a right to consent, ASPEN data is only used for performance metrics agreed upon in the employee performance standards reviewed and acknowledged by the employee annually. While employees may have a right to consent,

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?

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

Follow the format below:

Privacy Risk: VA mitigates the risk by documenting expectations of performance in signed acknowledged performance standards. Employee performance is tracked by supervisors and may be reported manually until access is provided for employees. Supervisors may always fall back to manually collected data in supervisor personnel folders to track performance.

Mitigation: VA mitigates the risk by documenting expectations of performance in signed acknowledged performance standards. Employee performance is tracked by supervisors and may be reported manually until access is provided for employees. Supervisors may always fall back to manually collected data in supervisor personnel folders to track performance.

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.***

Members of the public have no need to know or access to ASPEN. Any member of the public wishing for copies of production records should contact their local Privacy/FOIA office where their records are located: https://www.benefits.va.gov/benefits/offices.asp. Procedures for employee's establishing a profile in ASPEN to enter their production records is available in the ASPEN user's guide. Employees must be approved by their local supervisor for access to ASPEN. All quality reviews and performance totals established on employee records are available for employees to review online at any time within ASPEN. Production record refer to the productivity weighted action records stored in ASPEN.asp.

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).

Members of the public have no need to know or access to ASPEN.ASPEN is not exempt from the Privacy Act. ASPEN is not exempt from 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.

Any member of the public wishing for copies of production records should contact their local Privacy/FOIA office where their records are located: https://www.benefits.va.gov/benefits/offices.asp.

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.

The employee's supervisor is always the first contact for correcting inaccurate or erroneous information. The supervisor has the ability to return work products, mark valid or invalidate production level or exclude time records. Additionally, ServiceNow via YourIT has the assignment group "PHI SME ASPEN" for any IT or system related tickets. These tickets are for system outages, defects, or issues related to the system's operation. Questions about individual quality reviews or validating work products are handled by the local supervisors as a function in ASPEN. The employee would contact their supervisor if inaccurate or erroneous information is found in ASPEN. The supervisor can then perform certain tasks within ASPEN that may correct the issue; like, return work products, mark valid or invalidate production level or exclude time records. If the issue cannot be corrected that way, the supervisor can submit a ServiceNow request to the ASPEN System Administrators by using the assignment group "PHI SME ASPEN" (which stands for Philadelphia Subject Matter Expert group for ASPEN)via information.

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.

Employees are directed via the ASPEN users guide and ServiceNow YourIT knowledge-based articles to contact their supervisors first to correct information in ASPEN, additional Knowledge Articles on ServiceNow provide additional steps to be taken to route issues to local supervisors or create an IT incident ticket. uses to local supervisors or create an IT incident ticket.

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.

Since ASPEN is a performance tracking system, it is driven by employees entering production actions and exclude time as well as supervisor/reviewers adding quality review records. Employees may change/correct production records for up to 7 days and exclude time up to 15 days. Beyond those timeframes, supervisors can correct information for the employee. time up to 15 days. Beyond those timeframes, supervisors can correct information for the employee.

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: Employee can access and correct their information in ASPEN for up to 14 calendar days. The risk of employees not being able to update information past 14 days is mitigated by the procedures documented in the ASPEN user's guide where the employee contacts their supervisor to correct records over 14 days old.

Mitigation: ASPEN deploys least privilege to the Regional Office and team level. Access is controlled by teams and employees cannot access each other records. Aside from the owning employee, only supervisors can access employee records and their access to individual teams must be approved by their supervisor usually the Assistance Veteran Service Center Manager (AVSCM) or Veteran Service Center Manager (VSCM) in the Veterans Service Center.

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.

ASPEN end users requests must first be approved by their supervisor and profiles are established by supervisors who have local Regional Office Program Administration (RO PA). The three main roles in ASPEN are employees, supervisors/reviewers, and local ROPAs. Employees may input their production actions and exclude time. Supervisor/reviewers may view employee records by assigned teams, establish quality review records, validate production actions, validate exclude time (supervisors only), and run performance reports. Local RO PAs may establish and update employee profiles.

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?

Please provide response here ASPEN does not have users from other Agencies. ASPEN does not have users from other Agencies.

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.

ASPEN employs Role Based Access Controls (RBAC). The main roles for a typical user are: employee, reviewer, and supervisor. Employees enter their production data as well as any exclude time from their scheduled work hours. Reviewers and Supervisors validate production items entered and conduct quality reviews on select claim activities. Additional, Supervisors validate employee exclude time inputs. Finally the Regional Office Program Administrators manage the employee profile records in the system (see the below chart).

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

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access

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

Contractors do not have access to ASPEN through the User Interface (UI); however, they may be hired to work on the system to provide support to the administration of the application, database, or infrastructure. Those contractors are required to follow the EPAS process as well as minimum requirements outlined by the VA Rules of Behavior. Access is verified through VA personnel before access is granted to contractors. Contracts are reviewed annually at a minimum by a contracting official representative (COR) or project manager (PM). Contractors providing support to ASPEN must complete annual VA Privacy and Information Security Awareness and Rules of Behavior training in Toma Management System (TMS). All contractors are cleared using the VA background investigation process. EPAS process as well as minimum requirements outlined by the VA Rules of Behavior.

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.

Personnel accessing information systems must read and acknowledge the VA Rules of Behavior (ROB) prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training which all personnel must complete via the VA's Talent Management System (TMS). After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Complete
2. *The System Security Plan Status Date:* 3/10/2023
3. *The Authorization Status:* 1 year
4. *The Authorization Date:* May 21, 2022
5. *The Authorization Termination Date:* Please provide response here May 20, 2023
6. *The Risk Review Completion Date:* 3/10/2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* moderate

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

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

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)*

No, ASPEN does not use cloud technology.

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

ID	Privacy Controls
IP	**Individual Participation and Redress**
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
SE	**Security**
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR	**Transparency**
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

JEAN-CLAUDE WICKS

Digitally signed by JEAN-CLAUDE WICKS
Date: 2023.03.27 05:41:12 -06'00'

Privacy Officer, Jean-Claude Wicks

AMY GALLAGHER

Digitally signed by AMY GALLAGHER
Date: 2023.03.29 14:57:33 -04'00'

Information System Security Officer, Amy Gallagher

Miosha L. Newbill 260638

Digitally signed by Miosha L. Newbill 260638
Date: 2023.03.29 16:50:14 -05'00'

Information System Owner, Miosha Newbill

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).

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