Privacy Impact Assessment for the VA IT System called:

# Health Data and Analytics Platform (HDAP) Data and Analytics

# Veterans Affairs Central Office

Date PIA submitted for review:

September 6, 2022

System Contacts:

*System Contacts*

| | Name | E-mail | Phone Number |
|---|---|---|---|
| Privacy Officer | Phillip Cauthers | Phillip.cauthers@va.gov | 503-721-1037 |
| Information System Security Officer (ISSO) | Albert Estacio | Albert.Estacio@va.gov | 909-583-6309 |
| Information System Owner | Michelle Clark | Michelle.Clark3@va.gov | 512-981-4929 |

## Abstract

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

The Health Data and Analytics Platform (HDAP) is an open-architected, cloud-based data analytics platform for consolidating, curating, and analyzing data across the VA. The platform enables evidence-based decision making to improve outcomes for Veterans and their families through the delivery of data insights, to include those to be derived from predictive analytics to VA employees across Administrations. VA project teams can leverage raw data, data products, and models already curated by the HDAP team and other users, ingest additional data, or build and publish their own data assets. As a component of the Data and Analytics Product Line, HDAP will enable the combination of health record data with other data under VA management that may help VHA identify Veterans at risk of negative health outcomes. Such data can be called "social determinants of health" and may include benefits information or Veteran self-reported data through VA sponsored social media. Through the application of role and attribute-based access control, HDAP will enable such data combinations while still protecting the privacy of Veteran data and complying with VA privacy and security policies.

## Overview

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

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

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

The Health Data and Analytics Platform (HDAP) is the VA's quintessential source for all Veteran experience and health data. HDAP is a core component of business intelligence that provides historical, real-time, and predictive views of enterprise operations enabling evidence-based decision making to improve outcomes for Veterans and their families through the delivery of data insights to VA employees across Administrations.
HDAP provides an opportunity to:
•Integrate Veteran data from multiple sources into a single database and data model
•Maintain Veteran experience history and health data
•Integrate data from multiple source systems, enabling a central view across the enterprise
•Improve data quality and present the organization's information consistently
•Provide a single common data model for all data of interest regardless of the data's source
•Restructure the data to make better decisions
•Deliver enhanced business intelligence
•Perform predictive analysis for medical trends across clinics, patients, or contact center information
•Proactive reach out to Veterans based on predictive patterns
•Develop predictive Key Performance Indicator (KPI) reporting for better performance and outcome
•Improve workforce management recommendations based on medical trends across clinics, patients, or contact center information.

HDAP aggregates Veteran data obtained from various disparate data sources across VA.

The current System of Records Notice (SORN) are applicable, but some will need to be updated or modified for this system or collection. The applicable legal authority falls under SORN: Title 5 U.S.C 301, Title 26 U.S.C 61. Title 38, U.S.C. sections 31, 109, 111,501, 1151 1703, 1705, 1710, 1712, 1717,1720, 1721, 1724, 1725, 1727, 1728,1741 – 1743, 1781, 1786, 1787, 3102,5701 (b) (6) (g) (2) (g) (4) (c) (1), 5724, 7105,7332, and 8131–8137. 38 Code of Federal Regulations 2.6 and 45 CFR part 160 and 164. Title 44 U.S.C and Title 45 U.S.C. Veterans Access, Choice, and Accountability Act of 2014 and SORN 54VA10NB3: Title 38, United States Code, sections 501(a), 501(b), 1703, 1720G, 1724, 1725, 1728, 1781, 1787, 1802, 1803, 1812, 1813, 1821, Public Law 103–446 section 107 and Public Law 111–163 section 101. Additional SORNs are 158VA10NC5, 172VA10/ 86 FR 72688, 24VA10A7, 173VA005OP2, 58VA21/22/28/86 and 197VA10.

HDAP is hosted in the FedRAMP MODERATE Microsoft Azure GovCloud (MAG). All virtual machines, operating systems, and applications are secured and validated by the VAEC cloud team as well as VA software assurance organization and tracked within the program ATO. Completion of this PIA would not affect any technology or business process changes.
Ownership data rights stay within the VA.

HDAP audience is currently estimated at 150 users.

## Section 1. Characterization of the Information

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

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

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

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

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

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

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

Biometrics, PHI

**PII Mapping of Components**

**Health Data and Analytics Platform** consists of **five** key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **Health Data and Analytics Platform** and the reasons for the collection of the PII are in the table below.

**PII Mapped to Components**

**Note**: Due to the PIA being a public facing document, please do not include the server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

*PII Mapped to Components*

| Database Name of the information system collecting/storing PII | Does this system collect PII? (Yes/No) | Does this system store PII? (Yes/No) | Type of PII (SSN, DOB, etc.) | Reason for Collection/ Storage of PII | Safeguards |
|---|---|---|---|---|---|
| CDW | Yes | Yes | Name, Social Security Number, Email, Health Information Benefits Information, Claims Decision DD-214, Mailing Address, Phone Number, Date of Birth | To ingest Veteran data into the SDP environment for data reporting and analytics purposes, and clinical care decision making | Role-based access granted through the Elevated Privileges Access System (EPAS)<br><br>•Data is encrypted at rest and in transit |
| CDWWork | Yes | Yes | Name, Social Security Number, Email, Biometrics, Financial Information, Health Information, Benefits Information, Claims Decision, DD-214, Mailing Address, Phone Number, Date of Birth | To ingest Veteran data into the SDP environment for data reporting and analytics purposes, and clinical care decision making. | Role-based access granted through the Elevated Privileges Access System (EPAS)<br>•Data is encrypted at rest and in transit |
| CDW | Yes | Yes | Name, Social Security Number, Email, | To ingest veteran data | Role-based access |

| | | | | | |
|---|---|---|---|---|---|
| | | | Health Information, Benefits Information, Claims Decision, DD-214, Mailing Address, Phone Number, Date of Birth | into the SDP environment for data reporting and analytics purposes, and clinical care decision making. | granted through the Elevated Privileges Access System (EPAS)<br>• Data is encrypted at rest and in transit |
| CDWWork2 (Millennium Cerner Data) | Yes | Yes | Name, SSN, Date of birth, Race /ethnicity, Vital Status, Gender, City of residence, County of residence, Zip code, Hospitalization dates, Date of diagnosis, Date of death, Private insurance status, Laboratory results, Medications and therapies, Outpatient/inpatient clinic visits | To ingest veteran data into the SDP environment for data reporting and analytics purposes, and clinical care decision making. | Role-based access granted through the Elevated Privileges Access System (EPAS)<br>• Data is encrypted at rest and in transit |
| Vista Imaging | Yes | Yes | Name, Address, SSN, DOB, Physician name All data in DICOM DICOM Library - Anonymize, Share, View DICOM files ONLINE | To ingest veteran data into the SDP environment for data reporting and analytics purposes, and clinical care decision making. | Role-based access granted through the Elevated Privileges Access System (EPAS)<br>• Data is encrypted at rest and in transit |

**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.*

The Health and Data Analytics Platform is a multi-cloud data enterprise data management and analytics platform that aggregates Veteran data obtained from various disparate data sources across VA and one external source. Data on servers are copies of on-premises Corporate Data Warehouse (CDW) databases. The Power Business Intelligence (BI) gateways provide access from cloud-based systems to on premise CDW data.

**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.*

Veteran data is ingested into HDAP using the Golden Gate Replication, Azure Data Factory (ADF), Azure Copy, and SSH File Transfer Protocol (SFTP) The data sources are listed in response to question 1.2 above.

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

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

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

The system will undergo automated and manual test cases to ensure the validity of the data. Data comes straight from the CDW data sources which has its own data integrity controls and processes. If inconsistent files are found during the data movement, the copy activity is aborted.

**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 applicable legal authority falls under SORN: 23VA10NB3: Title 5 U.S.C 301, Title 26 U.S.C 61. Title 38, U.S.C. sections 31, 109, 111,501, 1151 1703, 1705, 1710, 1712, 1717,1720, 1721, 1724, 1725, 1727, 1728,1741–1743, 1781, 1786, 1787, 3102, 5701 (b) (6) (g) (2) (g) (4) (c) (1), 5724, 7105, 7332, and 8131–8137. 38 Code of Federal Regulations 2.6 and 45 CFR part 160 and 164. Title 44 U.S.C and Title 45 U.S.C. Veterans Access, Choice, and Accountability Act of 2014 and SORN 54VA10NB3: Title 38, United States Code, sections 501 (a), 501 (b), 1703, 1720G, 1724, 1725, 1728, 1781, 1787, 1802, 1803, 1812, 1813, 1821, Public Law 103–446 section 107 and Public Law 111–163 section 101. Title 38 United States Code Section 7304, Rules and Regulations -Title 38 United States Code Section 501(b), and Deputy Secretary of Veterans Affairs - Title 38 United States Code Section 304.

Patient Medical Record-VA'' (24VA10A7): https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf14/pdf/2014-19283.pdf

**1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information**

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

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

*Principle of Purpose Specification: 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:** PII of a Veteran may not be accurate, complete, and current in the HDAP system

**Mitigation:** HDAP is not a system of record and relies on the source (feeder) systems to ensure that PII collected is accurate, complete, and current. The following policies and procedures in the VA ensure that any PII collected and maintained by VA is accurate, relevant, timely, and complete for the purpose for which it is to be used
• requires a Veteran or an authorized representative to validate PII during the collection process
• when required, requests Veteran or an authorized representative to revalidate that PII collected is still accurate
• confirms to the greatest extent practicable upon collection or creation of personally identifiable information (PII), the accuracy, relevance, timeliness, and completeness of that information
• collects PII directly from the individual to the greatest extent practicable
• checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems; and
• issues guidelines ensuring and maximizing the quality, utility, objectivity, and integrity of disseminated information

## 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.*

HDAP is a central repository of integrated Veteran data from multiple data sources in the VA. HDAP will make health data more accessible to authorized users in a way that improves collaboration between many clinical stakeholders through enhanced knowledge sharing. It's open-architected, cloud-based data analytics platform enables for consolidating, curating, and analyzing data across the VA.

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

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

*If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.*
*This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information*

• HDAP is hosted in the Microsoft Azure GovCloud (MAG). Business Intelligence (BI) solutions from Microsoft are used to inspect, cleanse, transform and model Veteran data to support decision-making.
• Azure Data Factory brings together all structured, unstructured, and semi-structured data (logs, files, and media) to Azure Data Lake Storage.
• Structureless datasets are cleaned, transformed, and combined with structured data from operational databases or data warehouses in the VA with the help of Azure Databricks.
• Native connectors between Azure Databricks and Azure Synapse Analytics are leveraged to access and move data at scale.
• The Advanced Analytics Teams (data scientists and data analysts) take advantage of Azure Databricks to perform root cause determination and raw data analysis.
• Query and report Veteran data in Power BI and Microsoft SQL Services Management Studio
• Palantir, a data science tool, used for predictive modeling.

**2.3 How is the information in the system secured?**

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

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

*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 data are encrypted and transmitted through a secure network. The entire SSN is hidden from users, and HDAP ensures that PII data is only released to the intended individual.

**2.4 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.*

Add answer here:

A role-based access control (RBAC) security approach is used to limit users only to the information needed to do their job and prevent them from accessing information that doesn't pertain to them. A variety of user roles and Active Directory user groups, ranging from administrators to supervisors and DAPL stakeholders (consume reports) will exist in the system. Data owners are responsible for authorizing access to PII and leverage the safeguards implemented by HDAP DevSecOps.

## 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 PII information is retained by the HDAP system –

- Name
- Social Security Number
- Mailing Address
- Personal Phone Number
- Personal Email Address
- Demographics
- Date of Birth
- Electronic Data Interchange Personal Identifier (EDIPI)
- Usernames
- Biometrics

**3.2 How long is information retained?**

*In some cases VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. If the system is using cloud technology, will it be following the NARA approved retention length and schedule?*

*The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.*
*This question is related to privacy control DM-2, Data Retention and Disposal.*

Per the National Archives and Records Administration Request for Records Disposition Authority Records Schedule: DAA-GRS-2013-0005, Item 51, data is destroyed 5 years after the project/activity/transaction is completed or superseded, or the associated system is terminated, or the associated data is migrated to a successor system, but longer retention is authorized if required for business use.

**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.*

Yes, VHA Record Control Schedule 10-1: https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

**3.4 What are the procedures for the elimination of SPI?**

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

HDAP data will be deleted after decommissioning, following the Records Control Schedule (RCS 10-1), in compliance with VA policy, by logically deleting the stored data then overwriting the virtual drives with generic/dummy data to ensure no previous ghost/residual data can be restored.

**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*

Yes, access control policies and procedures implemented in VAEC MAG to minimize the use of PII for testing, training, and research.

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

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

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

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

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

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

Follow the format below:
**Privacy Risk:** Possibility of data breach is higher if retention of PII is longer.

**Mitigation:** To combat a data breach, HDAP implements the same retention schedule as the source record. HDAP relies on the data ingested from data sources. Old data are automatically archived based on retention schedule requirements.

HDAP data will be deleted after decommissioning, following the Records Control Schedule (RCS 10-1), in compliance with VA policy, by physically deleting the stored data then overwriting the drives with generic/dummy data to ensure no previous ghost/residual data can be restored.

## 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*** |
|---|---|---|---|
| Corporate Data Warehouse (CDW) | CDW<br>For data reporting and analytics purposes, and clinical care decision making. | Name, Social Security Number, Email, Biometrics, Financial Information, Health Information, Benefits Information, Claims Decision, DD-214, Mailing Address, Phone Number, Date of Birth | TLS/SSL over communication HTTPS |
| Quality, Performance, and Risk (QPR), Data Management and Analytics Directorate | Data Centralization and Business Intelligence Platform (DCBI)<br>For Audit, oversight, tracking of yearly budget execution by vendor, and Resource allocation, workload management, and staffing model | Name, Address, Phone Number, VA & personal email address Vendor Taxpayer ID Number (TIN), Email address | HTTPS & Azure Data Factory (ADF) |
| Office of Healthcare Innovation & Learning (OHIL) | Digital Health Platform (DHP) | Name, Integration Control Number (ICN), Patient Generated Data (PGD) from Fitbit device | HTTPS |
| Palantir | One-stop view of VA Veteran data across multiple lines of business to aid in predictive and prescriptive modeling and providing Veteran common model. | Name, SSN, Mailing Address, Physical Address, Next-of-kin information, COVID case information, Patient ID, VA Identifier, Phone Number, Email, Health Information, Benefits Information, Claims Decision, DD-214, & Date of Birth | HTTPS |

**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:** If access to the system is not monitored, there may be unauthorized use or disclosure of the information in HDAP

**Mitigation:** All organizational use of HDAP data is routinely monitored, tracked, and logged by the HDAP technical team. VA personnel are trained on the authorized uses of HDAP information as well as consequences of unauthorized use or sharing of PII. Related controls: Accountability, Audit, And Risk Management AR-3, AR-4, AR-5, AR-8, Authority And Purpose AP-2, Data Minimization And RetentionDI-1, DI-2, Individual Participation And Redress IP-1, TransparencyTR-1 are implemented to protect and ensure the proper handling of PII.

## Section 5. External Sharing/Receiving and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to VA, which includes Federal, State, and local governments, and the private sector.

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

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

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

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

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

*What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a*

*Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?*

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

*Data Shared with External Organizations*

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

**5.2 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:** N/A, there are no external connections in HDAP

**Mitigation:** N/A

## Section 6. Notice

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

**6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?**

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

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

*Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection. This question is related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.*

HDAP is a central repository of integrated data from the one or more disparate sources. Data does not originate in the HDAP data warehouse. Information is collected, or copied, from systems of record (SOR) across the VA such as CDW and brought into the data warehouse. The source system is responsible for providing a Privacy Act statement anytime information is collected on a paper or electronic form, on a website, on a mobile application, over the telephone, or through some other medium. This requirement ensures that the individual is provided with sufficient information about the request for information to make an informed decision on whether to respond.

Refer to –
VHA Privacy Notice of Privacy Practices:
https://vaww.va.gov/vhapublications/ViewPublication.asp?pub_ID=1090VA
Privacy Impact Assessment: https://www.oprm.va.gov/privacy/pia.aspx
VHA HANDBOOK 1605.04, Notice of Privacy Practices
VHA Directive 1605.01, Privacy and Release of Information

**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*

At the time of collection, individuals can decline a request to provide information. For instance, individuals have the right to refuse to disclose their SSNs to the VHA. The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VHA an SSN.

The VHA Notice of Privacy Practices provides information to a patient (i.e., Veteran) on their patient rights (i.e., to request a restriction).

**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*

VHA Directive 1605.01, Privacy and Release Information directive list the rights to request that the VHA restrict the uses and/or disclosures of individually identifiable health information to carry out treatment, payment, or health care operations.

The VHA Notice of Privacy Practices provides information on the uses and disclosures of information that require their authorization.

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

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

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

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

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

Follow the format below:

**Privacy Risk:** If a privacy notice is not provided to the subject of the records, the public would not be aware of the information collected about the subject of the record.

**Mitigation:** The VA mitigates this risk by ensuring that this PIA – which serves as notice that a HDAP exists, what information it contains, and the procedures in managing the information – is available online per the requirements of the eGovernment Act of 2002, Publication. L. 107–347 §208 (b) (1) (B) (iii).

## 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.*

Patient requests for information are governed by VHA health information management and privacy policy with respect to right to access one's own health record upon receipt of a written and signed request. All requests for copies of health records are processed by Release of Information staff at each VA medical center or accessed through the My HealtheVet premium account.

**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.*

Procedures for an individual submitting an amendment to their health records are addressing VHA Directive 1907.01 and 1605.01. Both policies outline the rights of an individual to request an amendment to any information or records retrieved by the individual's name or other individually identifiable information contained in a VA system of records, as provided in 38 CFR 1.579 and 45 CFR. The request must be in writing over the signature of the individual and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the facility Privacy Officer, or designee, to be date stamped; and filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579.

**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 are made aware of the procedures for correcting her or his information through the Privacy Act statement provided at the time of information collection.

See record access procedure from SORN: Individuals seeking information regarding access to and contesting of records in this system may write, call, or visit the VA facility location where they are or were employed or made contact.

**7.4 If no formal redress is provided, what alternatives are available to the individual?**

*Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems.*
*This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.*

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

The VHA Notice of Privacy Practices provides information on the patients (e.g., Veteran) right to request and amendment of their health record. Amendment requests must be submitted to the VHA facility where the Veteran received his/her healthcare.

**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:** The HDAP system denies a Veteran direct access, redress and correction of their record maintained in the system. This may result in inaccurate Veteran information making its way into the system.

**Mitigation:** A Veteran who wishes to determine whether a record is being maintained in this system under his or her name or other personal identifier, or who wants to review the contents of such a record, should submit a written request or apply in person to the VA health care facility (or directly to the VHA) where care was rendered. Inquiries should include the patient's full name, date of birth, and return address. The SSN may be required as an additional identity verification method.

## 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.*

All HDAP users must obtain VA clearance. Direct access to HDAP data is strictly prohibited for external agencies.

A role-based access control (RBAC) security approach is used to limit users only to the information needed to do their job and prevent them from accessing information that doesn't pertain to them. A variety of user roles, ranging from administrators to supervisors and DAPL stakeholders (consume reports) will exist in the system. The HDAP user profiles identified to date are listed in Section 2.4 above.

**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.*

The HDAP data management implementation is a collaborative effort involving the Data and Analytics Product Line (DAPL) , contractors, data scientists, system owners, and data analysts. Contractors have access to the system and its PII to support their duties that include but are not limited to big data ingestion, preparation, orchestration, and management.

DAPL is responsible for ensuring that all contractors working on the HDAP system are cleared using the VA background investigation process and obtain a Minimum Background Investigation (MBI). Contractors must sign Non-Disclosure Agreements (NDA) and necessary contractual requirements governing access and handling of Veteran data.

**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.*

Department of Veterans Affairs (VA) offers privacy and security training through a state-of-the-art online Talent Management System (TMS). Veterans Health Administration (VHA) and Veterans Benefit Administration (VBA) employees and contractors who have access to Protected Health Information (PHI) are required to complete

1. VA Privacy and Information Security Awareness and Rules of Behavior (TMS ID: 10176)
2. HVA Privacy and Health Insurance Portability and Accountability (HIPAA) Focused Training (TMS ID: 10203)

VA requires all users to take these courses, so they would know what to do to keep information safe and help VA comply with federal laws about privacy and information security. These courses help users understand their roles and responsibilities for keeping information safe and ensure that individual who have access to PII are trained to handle it appropriately.

All VA personnel must read and acknowledge their receipt and acceptance of the VA Information Security Rules of Behavior (ROB). Acceptance obtained through electronic acknowledgment is tracked through the TMS system.

Role-based Training includes but is not limited to and based on the role of the user.
1. Information Assurance for Software Developers IT Software Developers (TMS ID: 1016925)
2. Information Security Role-Based Training for Data Managers (TMS ID: 1357084)
3. Information Security Role-Based Training for IT Project Managers (TMS ID: 64899)
4. Information Security Role-Based Training for IT Specialists (TMS ID: 3197)
5. Information Security Role-Based Training for Network Administrators (TMS ID: 1357083)
6. Information Security Role-Based Training for System Administrators (TMS ID: 1357076)
7. Information Security Role-Based Training for System Owners (TMS ID: 3867207)

VA contractors must complete the privacy and security training courses to gain access to VA information systems or VA sensitive information. To maintain their access, contractors must complete this training each year.

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

*If Yes, provide:*

1. *The Security Plan Status,*
2. *The Security Plan Status Date,*
3. *The Authorization Status,*
4. *The Authorization Date,*

5. *The Authorization Termination Date,*
6. *The Risk Review Completion Date,*
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH).*

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

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

Yes, HDAP has an Authorization to Operate (ATO) with an authorization date of March 10, 2022, authorization termination date (ATD) of March 10, 2023. The FIPS 199 classification of SDP system is MODERATE. The security plan was approved January 3, 2022, and the risk review was completed January 27, 2022.

## Section 9 – Technology Usage

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

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

*If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS).*

*This question is related to privacy control UL-1, Information Sharing with Third Parties.*

*Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1.*

Yes, through VAEC Azure MAG

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

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

N/A System is going through VAEC

**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 System is going through VAEC

**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 System is going through VAEC

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

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

N/A

## Section 10. References

Summary of Privacy Controls by Family

*Summary of Privacy Controls by Family*

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

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

**Signature of Responsible Officials**

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

Phillip Cauthers 255139

Digitally signed by Phillip Cauthers 255139
Date: 2022.10.26 06:43:37 -07'00'

**Privacy Officer, Phillip Cauthers**

Albertino M. Estacio 119921

Digitally signed by Albertino M. Estacio 119921
Date: 2022.10.25 07:39:46 -07'00'

**Information System Security Officer, Albert Estacio**

Michelle E. Clark 304622

Digitally signed by Michelle E. Clark 304622
Date: 2022.10.25 20:55:58 -04'00'

**Information System Owner, Michelle Clark**

## 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).

https://vaww.va.gov/vhapublications/ViewPublication.asp?pub_ID=1090VA

https://www.oprm.va.gov/privacy/pia.aspx