Privacy Impact Assessment for the VA IT System called:

Quadient SMART

VA Corporate

OIT/QPR/Enterprise Mail Management

Date PIA submitted for review:

5/17/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	*Tonya Facemire*	*Tonya.Facemire@va.gov*	*202-632-8423*
Information System Security Officer (ISSO)	*Richard Alomar-Loubriel*	*Richard.Alomar-Loubriel@va.gov*	*787-696-4091*
Information System Owner	*Scottie Ross*	*Scottie.Ross@va.gov*	*478-595-1349*

Abstract

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

Quadient SMART is a Commercial-Off-The-Shelf (COTS) and Software-as-a-Service (SaaS). SMART is a Shipping, Mailing, Accounting, Reporting and Tracking mailing solution from a single dashboard. SMART provides detailed shipping and tracking notifications, chargeback accounting with postage meter reconciliation, and extensive reporting options. SMART generates postage expense reports by: mail class, weight break, presort, ascending and descending register values, account/department, operator, cost center, and predefined or custom time periods.

VA Mailing equipment, software collects mailing metrics (number of letters/packages mailed, cost for mailing) and collates the data within Quadient SMART to provide a single solution for sending mail and streamlining the mailing process.

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.

Quadient SMART and Enterprise Mail Management, Compliance, Risk and Remediation (CRR)

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

Quadient SMART provides a single solution for sending mail and streamlining the mailing process allowing mail management at the VA Enterprise Level. Quadient SMART provides best cost shipping options, allows for accurate reporting, accountability of volume and expenditures of mail and parcels.

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

The system is owned and operated by the providing SaaS vendor Quadient and will be controlled by the Enterprise Mail Management, Compliance, Risk and Remediation (CRR) program office.

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.

The expected number of individuals whose information is stored in the system could be in excess of 100,000. The typical client will be various mail centers in VA Medical Centers, VA Regional Offices and VA Staff Offices

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

Contact Name, Address, Phone Number, and Email data is being used to identify individuals who are receiving mail. Mail managers, Mailing metrics, To/From Names, To/From Addresses, Mail Postage Cost, Package Shipping Cost, Weight of Package, Date/Time Packages, Sent/Received Name, Login information data is being used to login and provides the ability to track postage cost and related mailing metrics.

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

Each site will have a global address book and an individual address book. The global will be shared across the enterprise. The address books are used to imprint addresses on envelops for mailing. No other information is shared. Expenditure mail data is transferred through the cloud to the United States Postal Service (USPS).

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.

The global address book is shared across all sites and the standard controls are used across all sites. No PII is shared. Expenditure mail data is transferred through the cloud to the United States Postal Service (USPS).

3. Legal Authority and SORN

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

VA's use of information in Quadient SMART is authorized by 5 U.S.C. 301 which permits agency heads to create the usual and expected infrastructure necessary for the organization to accomplish its purposes and mission. In addition, the security and privacy measures for the system are required by the Federal Information Security Management Act (FISMA) and the statutes underlying OMB Circular A-130 for the secure and efficient use of government systems and resources. SORN's applicable to the system include 24VA10A7 / 85 FR 62406 – Patient Medical Records-VA, OPM/GOVT-1 General Personnel Records, 41VA41 / 87 FR 10283 – Veterans and Dependents National Cemetery Gravesite Reservation Records-VA and 58VA21/22/28 / 86 FR 61858 – Compensation, Pension Education and Vocational Rehabilitation and Employment Records-VA.

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?

The Quadient SMART System is not in the process of being modified, so the SORNS do not require amendment or revision. The system does use cloud technology. Two of the 3 VA SORNS cover cloud usage. The NCA SORN (41VA41) does not currently address cloud technology.

D. System Changes

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

The completion of this PIA will not require changes to business processes.

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

The completion of this PIA will not result in technology changes.

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)

VA personnel user logon info (username and password)

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

PII Mapping of Components (Servers/Database)

Quadient SMART consists of **one** key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **Quadient SMART** 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
MongoDB Atlas	Yes	Yes	• To/From Names • To/From Addresses • Mail Postage Cost • Package Shipping Cost • Weight of Package • Date/Time Packages are sent/Received	Comply with UPS, USPS regulations General Service Administration (GSA) Schedule 48, Next Generation Delivery Service (NGDS)	User training, system document; implementation role-based access settings, firewalls, passwords, (NIST's) Special Publication 800-53, as determined using Federal Information Processing (FIPS) 199.

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?

The source of information is collected by Hardcopy directly from the individual about whom the information pertains, the Government Sources are collected within the Enterprise Mail Management

program office and the Non-Government Sources are collected from the public. The information originates from VA business systems, address books, directories, and other programs supplying name and addresses and is entered into the system and subsequently provided to Quadient SMART. Quadient does not need the information. The VA SMART ADMIN will import all the Address Book into the SMART system.

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.

Information from sources other than the individual is not required.

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

The system does not create information (for example, a score, analysis, or report).

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?

The SaaS mailing solution (SMART) doesn't retrieve users mailing addresses, the envelops/packages come to the mail center pre-addressed by the service to run through the mail machine to have postage printed to the letter or package. As the letter is run through the mailing machine the address is checked by the United States Post Office data base (CASS) for accuracy and validity. The addresses are not collected or stored.

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.

Information is not collected on a form.

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.

The Agency has an option to require the ship to address to be validated before shipping a package. The SMART application utilizes a USPS CASS certified solution. CASS is a tool created and used by the United States Postal Service to ensure the accuracy of any software that taps into their database. A CASS-certified service provider that processes addresses will fill in information missing from an address, standardize it, and update it, giving you the most current and most accurate address.

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.

Postal address verification (also known as address, address validation, address verification and Coding Accuracy Support System (CASS) certification) is the process used to check the validity and deliverability of a physical mailing address. According to the United States Postal Service, an address is valid (or mailable) if it is CASS-certified, meaning that it exists within the comprehensive list of mailable addresses in their Address Management System. CASS enables the United States Postal Service (USPS) to evaluate the accuracy of software that corrects and matches street addresses. CASS certification is offered to all mailers, service bureaus, and software vendors that would like the USPS to evaluate the quality of their address-matching software and improve the accuracy of their ZIP+4, carrier route, and five-digit coding.

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

VA's use of information in Quadient SMART by 5 U.S.C. 301 which permits agency heads to create the usual and expected infrastructure necessary for the organization to accomplish its purposes and mission. In addition, the security and privacy measures for the system are required by the Federal Information Security Management Act (FISMA) and the statutes underlying OMB Circular A-130 for the secure and efficient use of government systems and resources. SORN's applicable to the system include 24VA10A7 / 85 FR 62406 – Patient Medical Records-VA, OPM/GOVT-1 General Personnel Records, 41VA41 / 87 FR 10283 – Veterans and Dependents National Cemetery Gravesite Reservation Records-VA and 58VA21/22/28 / 86 FR 61858 – Compensation, Pension Education and Vocational Rehabilitation and Employment Records-VA.

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: Name and mailing address are well established publicly accepted standard PII elements needed to send parcels, letters, and flats via US mail with USPS or shipping vendors. Members of the public are aware of and voluntarily provide their name and address when corresponding with the VA. There's no privacy risk related to the data collected. The data is the mail spend by the individual VA mail center and is not shared.

Mitigation: The system only collects PII in accordance with shipping vendor and USPS regulations. The VA relies on shipping vendor and USPS to adequately communicate any changes in their regulations to the public.

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.

- To/From Names: Listed on the envelope or package for mailing.
- To/From Addresses: Listed on the envelope or package for mailing.

- Mail Postage Cost: How much the particular mailing cost to send through the postal system (an example is a stamp)
- Package Shipping Cost: How much the particular mailing cost to send through the postal system (an example is a stamp)
- Weight of Package: The weight of the letter or package. This dictates how much it cost to send through the mail.
- Date/Time Packages are sent/Received: Date/Time Packages are sent/Received is a tracking mechanism to make sure the package is delivered and the length of time it takes for delivery.

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.

The system meters mail, provides best cost shipping options, allows for accurate reporting, accountability of volume and expenditures of mail and parcels. Mailing equipment, products and services collect mailing metrics (number of letters/packages mailed, cost for mailing) and collates the data within the SaaS tool to provide a single solution for viewing aggregate mail data at the VA Enterprise Level.

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.

Logon credentials remain available as long each user has authorized access to the system. Credentials are revoked when access is no longer needed, including if individual moves a different office within VA or leaves employment.

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?

All information flow is encrypted within the Quadient SMART solution using FIPS 140-2 validated cryptography 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?

The system does not collect, process, or retain SSNs.

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

Access to the PII is determined by Business System owner who will review all user account request, which contain justification, and utilize their subject matter expertise to determine in a "need to know" before granting access. Administrative safeguards include user training; system documentation that advises on proper use; implementation of Need to Know and Minimum Necessary principles when awarding access, and others. Technical safeguards include role-based access settings, firewalls, and passwords. Other appropriate controls have been selected from the National Institute of Standards and Technology's (NIST's) Special Publication 800-53, as determined using Federal Information Processing Standard (FIPS) 199. Technical settings ensure that only Administrators are allowed to reset the password for users if needed.

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?

Access to the PII is determined by Business System owner who will review all user account request, which contain justification, and utilize their subject matter expertise to determine in a "need to know" before granting access.

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

Administrative safeguards include user training; system documentation that advises on proper use; implementation of Need to Know and Minimum Necessary principles when awarding access, and others.

2.4c Does access require manager approval?

Access requires local administrator manager approval.

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

All PII Data is being monitor & track per the FedRAMP NIST 800-53 Controls

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

The vendor is responsible for assuring safeguards for the PII

Section 3. Retention of Information

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

3.1 What information is retained?

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

The information that is retained in the system is Name, Mailing Address, Phone Numbers, weight date and time of the package, letter, or flat, and VA personnel (user) logon information (Username and Password).

3.2 How long is information retained?

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

The retention schedule has been approved by the NARA. The guidance for retention of records is found in the Records Control Schedule 10-1 http://www.va.gov/vhapublications/rcs10/rcs10-1.pdf and NARA: https://www.archives.gov/records-mgmt/grs.htmlOfficial record held in the office of record. Temporary; destroy 6 years after final payment or cancellation, but longer retention is authorized if required for business use. (GRS 1.1, Item 010 https://www.archives.gov/)) (DAA-GRS-2013-0003-0001) According to VA Handbook 6500, once records are entered into the system they remain as part of the protected system information. System logs are maintained for one year and then flagged for deletion by their automated processes. System logs are not retained after one year and any SPI containing them will be overwritten as part of the process for audit management. When virtual machines are no longer required to support the system, they are wiped clean, and the data overwritten. Paper documents are destroyed to an unreadable state in accordance with the Department of Veterans' Affairs VA Directive 6371, (April 8, 2014), https://www.va.gov/digitalstrategy/docs/VA_Directive_6500_24_Jan_2019.pdf In addition, any equipment that is decommissioned and is leaving the controlled data center will be sanitized (e.g., degaussing) or destroyed in accordance with VA Handbook 6500 and the Veterans Affairs Dedicated Cloud Media Sanitization Procedure. VA Dedicated Cloud Media Sanitization policy outlines the VA Dedicated Cloud policy and procedure for tracking, documentation, and disposal of storage media within the environment and their return to the VA, in accordance with VA Handbook 6500. Logon credentials remain available as long each user has authorized access to the system. Credentials are revoked when access is no longer needed, including if individual moves a different office within VA or leaves employment.

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

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

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

Yes, all records are stored within the system of record indicated on an approved disposition authority. 005-1 is the Records Control Schedule for all of OIT that is approved by NARA.

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

The Records Retention Schedule is DAA-GRS-2016-0003. Sequence Number 1 - Privacy Act System of Records Notices (SORNs). Disposition Authority Number: DAA-GRS-2016-0003-0002. Sequence Number 2 - Records analyzing Personally Identifiable Information (PII). Sequence Number 2.1 - Records of Privacy Threshold Analyses (PTAs) and Initial Privacy Assessments (IPAs). Disposition Authority Number: DAA-GRS-2016-0003-0003. Sequence Number 2.2 - Records of Privacy Impact Assessments (PIAs). Disposition Authority Number: DAA-GRS-2016-0003-0004. Sequence Number 3 - Computer matching program notices and agreements. Disposition Authority Number: DAA-GRS-2016-0003-0005.

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.

Based on the MOU/ISA contract, the VA records office will be consulted, and process for destroying or eliminating records will be documented as requested. More information on how to reach out can be found at https://www.va.gov/records/.

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.

All personnel will take mandatory annual Information Security Awareness and Records Management Training. In addition, administrators with privileged accounts will be required to take role-based training annually to maintain account access. The Quadient SMART system provides training for proper use of the system. VA personnel may take advantage of information security and privacy awareness events and workshops held within VA.

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

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

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

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

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

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: Quadient SMART only the minimum amount of information necessary in order to mail documents which are name, mailing address, and phone numbers for recipients. Logon credentials remain available as long as each user has authorized access to the system. Credentials are revoked when access is no longer needed.

Mitigation: Records are maintained under NARA GRS 20, Item 1c; superseded by the new GRS 3.2, item 030, which is for records created as part of their user identification and authorization process to gain access to systems. Retention is until "business use ceases". NARA concurs that agencies may dispose of these records as soon as they are no longer needed. NARA Approved citation GRS 23-8. Disposition: Temporary, destroy or delete when 2 years old, or 2 years after the date of the latest entry, whichever is applicable.

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***
Enterprise Mail Management Program Office	VA Mail Operations	Name, Mailing Address, Phone Numbers, Logon Information (Username and Password)	Electronically (HTTPS)
Veterans Benefits Administration (VBA)	VA Mail Operations	Name, Mailing Address, Phone Numbers, Logon Information (Username and Password)	Electronically (HTTPS)
Veterans Health Administration (VHA)	VA Mail Operations	Name, Mailing Address, Phone Numbers, Logon Information (Username and Password)	Electronically (HTTPS, SFTP)
National Cemetery Administration (NCA)	VA Mail Operations	Name, Mailing Address, Phone Numbers, Logon Information (Username and Password)	Electronically (HTTPS)
Staff Offices	VA Mail Operations	Name, Mailing Address, Phone Numbers, Logon Information (Username and Password)	Electronically (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. (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: The information used and stored in the application includes United States Postal Service (USPS), FedEx, DHL, and United Parcel Service (UPS) Tracking Number, USPS/shipping vendor service type (e.g., First Class mail, Priority Mail, etc.), USPS/shipping vendor service type add-on information (e.g., Registered Mail, Certified Mail, etc.) mail recipient (addressee) name, mail recipient mailing street address and zip code, and value of postage used to send a parcel. The mailing COTS equipment and SaaS software application the VA uses to provide the solution for sending mail and streamlining the mailing processing. The application will handle, and store mail and delivery service labeling associated with VA's use of United Parcel Service (UPS), United States Postal Service (USPS) and other like delivery services. The application will also store tracking information and system user authentication information. The types of information the application collects, maintains and shares are the names, addresses and phone numbers for members of the public who receive mail from the VA's mail operations. They will also track the number of pieces mailed costs by piece and overall costs. The system will also hold the VA office mailing address for agency offices sending mail and in some cases the names of individual employees sending outbound mail, in addition to username and login information for VA employees using the system. No personal information is shared externally. Mail recipient (addressee) name, mail recipient mailing street address and zip code are public information.

Mitigation: The system has the minimum amount of information necessary to mail documents which are the name, mailing address, and phone number for recipients. This information is required in printing shipping vendors compliant postage labels. Access to the PII is determined Business System owner who will review all user account request, which contain justification, and utilize their subject matter expertise to determine in a "need to know" exist before granting access. Administrative safeguards include user training; system documentation that advises on proper use; implementation of Need to Know and Minimum Necessary principles when awarding access, and others. Technical safeguards include role-based access settings, firewalls, and passwords. Other appropriate controls have been selected from the National Institute of Standards and Technology's (NIST's) Special Publication 800-53, as determined using Federal Information Processing Standard (FIPS) 199. Technical settings ensure that only Administrators are allowed to reset the password for users if needed.

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?

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***
Quadient-SMART	Sending Parcels/Mail	The COTS/SaaS tools collect the following mail information for each individual letter/package (postal charges, date package sent, tracking numbers and amount of postage paid).	National MOU/ISA	Site to Site
United States Postal Service (USPS)	Sending Parcels/Mail	Name, Mailing Address, Phone Numbers, Logon Information (Username and Password)	5, U.S.C. 301 Federal Information Security Management Act (FISMA) OMB Circular A-130	HTTPS User Training System Documentation Need to Know Minimum Necessary Principles Role-based Access Settings Firewalls
United Parcel Service (UPS)	Sending Parcels/Mail	Name, Mailing Address, Phone Numbers, Logon Information (Username and Password)	5, U.S.C. 301 Federal Information Security Management Act (FISMA) OMB Circular A-130	HTTPS User Training System Documentation Need to Know Minimum Necessary Principles

				Role-based Access Settings Firewalls
Federal Express (FedEx)	Sending Parcels/Mail	Name, Mailing Address, Phone Numbers, Logon Information (Username and Password)	5, U.S.C. 301 Federal Information Security Management Act (FISMA) OMB Circular A-130	HTTPS User Training System Documentation Need to Know Minimum Necessary Principles Role-based Access Settings Firewalls

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

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: The mailing COTS equipment and SaaS software application uses cloud technology to provide a single solution for sending mail and streamlining the mailing process. The system has the minimum amount of information necessary to mail documents which are the name, mailing address, and phone number for recipients. This information is required in printing shipping vendors compliant postage labels and is Public information and carries no risk.

Mitigation: Quadient has developed a System Security Plan for SMART and supporting documents that comply with 325 FedRAMP Moderate controls across 17 control families plus additional VA-Specific controls. These include comprehensive access and audit families of controls. Quadient SMART will undergoing rigorous, independent third-party audit that includes testing, examination,

evidence, and pen testing. FedRAMP access, audit, and other controls are followed and evidenced continually, weekly, monthly, quarterly, etc. as prescribed by the FedRAMP Moderate impact SSP statements.

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.

No prior notice is provided. The related SORNs are:

- 24VA10A7 / 85 FR 62406 – Patient Medical Records-VA - 2020-21426.pdf (govinfo.gov)
- OPM/GOVT-1 General Personnel Records - 2012-29777.pdf (govinfo.gov), modification 2015-30309.pdf (govinfo.gov)
- 41VA41 / 87 FR 10283 – Veterans and Dependents National Cemetery Gravesite Reservation Records-VA - 2022-03795.pdf (govinfo.gov)
- 58VA21/22/28 / 86 FR 61858 – Compensation, Pension Education and Vocational Rehabilitation and Employment Records-VA - 2021-24372.pdf (govinfo.gov)

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

Name and mailing address are well established publicly accepted standard PII elements needed to send parcels, letters, and flats via US mail with shipping vendors. Members of the public are aware of and voluntarily provide their name and address when corresponding with the VA.

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.

The submission of PII is Voluntary and if the recipient would like to request to opt-out of receiving mail from the VA, they may notify the VA sender to not send them mail via US Mail or shipping vendor.

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.

The submission of information is Voluntary and if the recipient would like to request to opt-out of receiving mail from the VA, they may notify the VA sender via mail or contact number to not send them mail via US Mail or delivery service and 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.

The submission of information is Voluntary and if the recipient would like to request to opt-out of receiving mail from the VA, they may notify the VA sender via mail or contact number to not send them mail via US Mail or other delivery services.

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:

<u>Privacy Risk:</u> The system only collects information in accordance with shipping vendor and USPS regulations. The system has the minimum amount of information necessary to mail

documents which are the name, mailing address, and phone number for recipients. This information is required in printing shipping vendors compliant postage labels and is Public information and carries no risk.

Mitigation: The VA relies on shipping vendor and USPS to adequately communicate any changes in their regulations to the public.

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.***

The submission of information is Voluntary and if the recipient would like to request to opt-out of receiving mail from the VA, they may notify the VA sender via mail or contact number to not send them mail via US Mail or other delivery services.

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).

The system is not exempt from the access of provisions of the Privacy Act.

7.1c If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information.

The system is a Privacy Act system.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed. If the correction procedures are the same as those given in question 7.1,

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

The submission of information is Voluntary and if the recipient would like to request to opt-out of receiving mail from the VA, they may notify the VA sender via mail or contact number to not send them mail via US Mail or other like delivery services. The system only collects information in accordance with shipping vendor and USPS regulations. The VA relies on USPS and shipping vendors to adequately communicate any changes in their regulations to the public.

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.

The system only collects information in accordance with shipping vendor and USPS regulations. The VA relies on shipping vendor and USPS to adequately communicate any changes in their regulations to the public.

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.

Individuals may contact VA using contact information available on VA.gov and by phone.

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: The submission of information is Voluntary, and the system only collects information in accordance with shipping vendor and USPS regulations.

Mitigation: If the recipient would like to request to opt-out of receiving mail from the VA, they may notify the VA sender via mail or contact number to not send them mail via US Mail or other shipping vendors. The system only collects information in accordance with shipping vendor and USPS regulations. The VA relies on shipping vendors and USPS to adequately communicate any changes in their regulations to the public. 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.

To access the S.M.A.R.T. Application the Agency Customer Admin must assign credentials to a user that need to ship and track packages. In addition, SSO can be available to provide additional safeguards.

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?

Users from other agencies will not have access.

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.

All users have "full" access.

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 will have access to the Quadient SMART system. The PII access is the same as they currently hold while performing mail duties as a mail clerk or mail supervisor in a VA Mail Center. Contractors have NDAs in place already.

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.

Per the FedRAMP NIST 800-53 Moderate controls requirements all personnel must take mandatory Information Security Awareness and Records management Training. Administrators with privileged accounts are required to take role-based training annually to maintain account access.

8.4 Has Authorization and Accreditation (A&A) been completed for the system? No

8.4a If Yes, provide:

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

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.***

VA Sponsored FedRAMP ATO process is the initial A&A process for the Quadient SMART SaaS application and is In Process. The following items are included in this process: Security Plan, Authorization, and Risk Review. The estimated IOC date is December 2023. The system is currently classified as Moderate Impact.

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)*

This system is a Software as a Service (SaaS) that uses cloud technology. There is no current agency authorization or FedRAMP Authorization for the solution, but it is currently in process of pursuing a VA-Sponsored FedRAMP Authorization. The system has a current data security categorization of Moderate from VA's Digital Transformation Center. Both a PIA and PTA have been completed and approved by the VA Privacy Office.

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.*

Contract does not establish ownership rights over data. The contract number is 36Cl0Xl9D0019. Section 5.11 of the contract states, "The contractor shall provide 100% of government owned data at the end of each thirty-day billing cycle and a comprehensive consolidated file with 100% of all government data acquired throughout the life of the contract. The comprehensive consolidated data file shall be delivered NLT thirty days prior to the end of the contract's POP. Both the thirty-day cycle data and the comprehensive consolidated file shall be in a government designated medium, format and configuration for delivery."

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.

CSP will not collect any ancillary data.

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.

Overall, protection of privacy data is the responsibility of VA. Privacy and data protections policies are documented in the approved VA and CSP security policies. These protections are also included in the contractual requirement for FedRAMP authorization. The SaaS system receives a full risk assessment annually with any remediations overseen by CSP ISO and VA ISOs.

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).

The system does not use RPA.

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 they provided in this Privacy Impact Assessment is true and accurate.

Tonya L. Facemire 234776

Digitally signed by Tonya L. Facemire 234776
Date: 2023.05.31 08:57:28 -04'00'

Privacy Officer, Tonya Facemire

RICHARD ALOMAR-LOUBRIEL 139039

Digitally signed by RICHARD ALOMAR-LOUBRIEL 139039
Date: 2023.05.31 11:40:57 -04'00'

Information System Security Officer, Richard Alomar-Loubriel

SCOTTIE ROSS

Digitally signed by SCOTTIE ROSS
Date: 2023.05.31 12:01:28 -04'00'

Information System Owner, Scottie Ross

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