Privacy Impact Assessment for the VA IT System called:

FSC Business Activity Monitoring (BAM)

Financial Services Center (FSC)

Veterans Affairs Central Office (VACO) eMASS ID #1483

Date PIA submitted for review:

02/27/2024

System Contacts

System Contacts:

	Name	E-mail	Phone Number
Privacy Officer	Pamela M. Smith	Pamela.Smith6@va.gov	512-386-2246
Information System Security Officer (ISSO)	Ronald Murray	Ronald.Murray2@va.gov	512-460-5081
Information System Owner	Jonathan Lindow	Jonathan.Lindow@va.gov	512-568-0626

Abstract

The abstract provides the simplest explanation for "what does the system do?".

FSC Business Activity Monitoring (BAM) is a web-based, modular, software-as-a-service used to identify improper payments. BAM identifies, prevents improper payments, and improves the efficiency and accuracy of the Do Not Pay (DNP) and Recapture and Recovery Program processes to comply with the Office of Management and Budget (OMB) A-123 of 2016, OMB A-136 of 2016, Improper Payments Elimination and Recovery Act (IPERA) of 2010, and Improper Payments Elimination and Recovery Improvement Act (IPERIA) of 2012.

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. What is the IT system name and the name of the program office that owns the IT system?

FSC Business Activity Monitoring owned by Financial Services Center

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

FSC BAM analyzes FMS and iFAMS vouchers and identifies potential improper payments for review. It improves the efficiency and accuracy of the Do Not Pay (DNP) and Recapture and Recovery Program processes to comply with the Office of Management and Budget (OMB), Improper Payments Elimination and Recovery Act (IPERA) of 2010, and Improper Payments Elimination and Recovery Improvement Act (IPERIA) of 2012.

C. Who is the owner or control of the IT system or project?

The system is VA Owned and Operated. Operational technical product management of the application and database is owned and controlled by the Financial Services Center (FSC), Financial Technology Center (FTC) Project Management Office (PMO). The virtual servers are managed by the FSC FTC IT Operations. The overall product ownership is owned by the FSC FOS COD group.

2. Information Collection and Sharing

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

The estimated number of 40 thousand vendors within the system is. No information is shared with other systems. The information is received from the Integrated Payment Processing System IPPS system, based upon preset criteria, for analysis.

E. *What is a general description of the information in the IT system and the purpose for collecting this information?*

The information BAM collects is sent to for analysis only. It receives invoice/voucher related information from Invoice Payment Processing System (IPPS) from Financial Management System (FMS) and Integrated Financial and Acquisition Management System (iFAMS). This information is analyzed within the parameters set by the business to determine if voucher related information is verified (within the parameters set by the business).

General info collects for analysis:

- Invoices that have been sent for payment
- Vendor information that corresponds to the invoices

This is part of maintaining adherence to the Do Not Pay (DNP) and Recapture and Recovery Program processes to comply with the Office of Management and Budget (OMB) A-123 of 2016, OMB A-136 of 2016, Improper Payments Elimination and Recovery Act (IPERA) of 2010, and Improper Payments Elimination and Recovery Improvement Act (IPERIA) of 2012.

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

No information is shared.

G. *Is 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?*

System is installed in an On-Prem environment and hosted within the ATIC data center.

3. Legal Authority and SORN

H. *What is the citation of the legal authority to operate the IT system?*

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

- Legal authority is: 5 CFR 1315 (b) (7), 31 U.S.C. chapter 39; Section 1010 of Public Law 106-398, 114 Stat. 1654
- Title 5 - Administrative Personnel, Chapter III - OFFICE OF MANAGEMENT AND BUDGET, Subchapter B - OMB DIRECTIVES
- Part 1315 - PROMPT PAYMENT
- 13VA047 - Individuals Submitting Invoices-Vouchers for Payment - 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?*

No changes needed.

4. System Changes

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

No changes needed.

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

No changes needed.

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. It must also match the information provided in question 3.4 of the PTA.

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[1]
☐ Vehicle License Plate Number
☒ Internet Protocol (IP) Address Numbers
☒ Medications
☒ Medical Records
☒ Race/Ethnicity

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

☒ Tax Identification Number
☒ Medical Record Number
☒ Gender
☒ Integrated Control Number (ICN)
☒ Military History/Service Connection
☒ Next of Kin
☒ Other Data Elements (list below)

- VENDORNAME
- ADDRESS1
- ADDRESS2
- CITY
- STATE
- ZIP
- PHONE
- CONTACT
- CUSTACCT
- SSNTAXID
- BANKNUMB
- BANKNAME
- CORRBANKNUMB
- CORRBANK
- ACCTNUMB
- BANKACCTYPE
- BANKCITY
- BANKSTATE
- BANKZIP

- Financial Institute, Account number ABA Routing ID, Account, Sole proprietorship first name, Last name, Middle name, Financial Institute, Account number ABA Routing ID, Account, User ID

PII Mapping of Components (Servers/Database)

BAM Data Warehouse (BAM DW) consists of 2 – BAM Entity Service, BAM Analytics, and BAM Database key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by BAM Data Warehouse (BAM DW) 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 server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	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

Database Names: • **Vafscdbsfos510a** • **Vafscdbsfos510b**	Yes	Yes	•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	Vendor identification and analysis	Data Encrypted at rest.

			•Tax Identification Number •Medical Record Number •Gender •Integrated Control Number (ICN) •Military History/Service Connection •Next of Kin **BAM Vendor fields:** • VENDORNAME • ADDRESS1 • ADDRESS2 • CITY • STATE • ZIP • VENDTYPE • PHONE • CONTACT • CUSTACCT • SSNTAXID • BANKNUMB • BANKNAME • CORRBANKNUMB • CORRBANK • ACCTNUMB • BANKACCTYPE • BANKCITY • BANKS • BANKZIP • SSNTAX		

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 BAM Oversight application does not collect information from a commercial data aggregator. It does not collect the information directly from the individual.

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.

The BAM Oversight application does not collect information from a commercial data aggregator. It does not collect the information directly from the individual.

1.2c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?

BAM Oversight provides an analysis of a voucher presented for payment to a workbench for the station user to review. Once reviewed the decision information is received into IPPS.

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?

BAM does not collect directly from the individual. It receives FMS and iFAMS data via electronic transmission from Vendor File, Data Depot, and IPPS. Data is not bi-directional.

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

N/A - All information is digital. No information sent to BAM uses a form in the physical characteristics of paper.

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.

BAM only collects information from other systems and sources that have their own ATO and information validation checks and controls. The information is received from IPPS. The accuracy of the information is managed by IPPS. If there is missing or incorrect data IPPS will place the invoice in an exception workbasket for a technician to perform an action. The action would be to either find/correct the data or return the invoice to the vendor for missing information that is required in the prompt payment act for payment processing.

1.4b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?

N/A – Commercial aggregators are not used.

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

Budget and Accounting Act of 1950, General Accounting Office, Title 8, chapter 3; Full SSN is used for payment and accounting purposes to index, and store pay affecting documents. Also required for IRS tax reporting. System of Records Notice SORN is clear about the use of the information, specifically SORN: 13VA047 Individuals Submitting Invoices-Vouchers For Payment-VA 2020-08611.pdf (govinfo.gov)

- Legal authority is: 5 CFR 1315 (b) (7), 31 U.S.C. chapter 39; Section 1010 of Public Law 106-398, 114 Stat. 1654
- Title 5 - Administrative Personnel, Chapter III - OFFICE OF MANAGEMENT AND BUDGET, Subchapter B - OMB DIRECTIVES
- Part 1315 - PROMPT PAYMENT

Legal Authority 31 U.S.C. 3512—Executive Agency Accounting and other Financial Management Reports and Plans; Federal Managers' Financial Integrity Act Section 2 of 1982; Federal Financial Management Improvement Act of 1996; E-Government Act of 2002 Title III., Federal Information Security Management Act (FISMA); Clinger Cohen Act of 1996; 38 CFR part 17 §§ 17.120–17.132.

OMB Circular A–123, Management's Responsibility for Internal Control; and OMB Circular A–127, Financial Management Systems. 5 CFR 1315 (b)(7)

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

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk:

- Sensitive Personal Information may be released to unauthorized individuals.

Mitigation:

- BAM adheres to information security requirements instituted by the VA Office of Information Technology (OIT).
- BAM relies on information previously collected by the VA from the individuals.
- Both contractors and VA employees are required to take Privacy, HIPAA, and information security training annually.
- File access granted only to those with a valid need to know.

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 that 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.

PII/PHI Data Element	Internal Use	External Use
• Name • Social Security Number • Date of Birth • Mother's Maiden Name	Analysis performed within the application only.	Not used or shared with another VA database or externally with other government organizations.

• 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 BAM Vendor Fields: • VENDORNAME • ADDRESS1 • ADDRESS2 • CITY • STATE • ZIP • VENDTYPE • PHONE • CONTACT • CUSTACCT • SSNTAXID • BANKNUMB • BANKNAME • CORRBANKNUMB • CORRBANK • ACCTNUMB • BANKACCTYPE • BANKCITY		Data is sent to the application’s database for analysis only.

• BANKS • BANKZIP • SSNTAX		

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?

BAM reviews invoices and maintains only (does not distribute or merge) the information sent to it via Enterprise Service Bus (ESB) in a separate data base for analysis. BAM responds with the recommended action. It will analyze the data sent to it based on the criteria required by the business (consumers of the data). It will perform complex AI analysis and deliver the results to the business in the form of a case that is displayed in a Work Bench.

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.

Not applicable to BAM.

2.3 How is the information in the system secured?
These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

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

The data is encrypted in transit and at rest. SSNs are not shared with other government organizations or externally.

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

Masking of SSNs is used to protect the information. SSNs are not shared with other government organizations or externally.

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

All employees and contractors are required to participate in general and role-based privacy training annually, all appropriate administrative, technical and safeguards have been implemented to protect IPPS, data accessed and displayed by the system and users of the system and these controls are reviewed regularly.

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 is determined by the business and station. It is controlled through the approval of an OFS 9957 digital form.

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

- Both contractor and VA employees are required to take Privacy, HIPAA, and information security training annually.
    - System of Records Notice SORN is clear about the use of the information, specifically SORN: 13VA047 Individuals Submitting Invoices-Vouchers for Payment-VA
    - Disciplinary actions, depending on the severity of the offense, include counseling, loss of access, suspension and possibly termination.
    - The information is required to process payments; without this information, we would not be able to accomplish our mission.

2.4c Does access require manager approval?

Yes

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

Information gathered is only used to verify vendor and invoice information. Both contractor and VA employees are required to take Privacy, HIPAA, and information security training annually. The System of Records Notice (SORN) is clear about the use of the information, specifically SORN: 13VA047 Individuals Submitting Invoices-Vouchers for Payment-VA. Disciplinary actions, depending on the severity of the offense, include counseling, loss of access, suspension and possibly termination. The information is required to process payments; without this information, we would not be able to accomplish our mission.

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

As a Product Owner the FOS COD Operational Team is responsible for this requirement. As a Product's technical management team, the FSC FTC PMO, working with FTC Operations, are responsible for assuring safeguards are technically in place.

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 data is retained and analyzed but is not transmitted, shared, or exchanged.

Name
Business Name
Vendor ID number
Social Security Number: (Only if used instead of Vendor ID number) Mailing Address
Zip Code
Phone Number
Email Address
Financial Account Information
Vendor Invoice Information
Vendor invoice information

3.2 How long is information retained?

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

BAM does not retain information outside the existing policies stated in sections 3.3 and 3.4. Records are retained as long as required per National Archivist and Records Administration

(NARA) standards (Reference: GRS Schedule 1.1, Item #10). Destroyed 6 years after final payment or cancellation 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)?

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

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

Yes, GRS Schedule 1.1, Item #10, Disposition Authority DAA-GRS-2013-0003-0001.
grs1-1.pdf (archives.gov)

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

It is governed by General Accounting Office Regulations which require retention for records created prior to July 2,1975: 10 years and 3 months after the period of the account; records created on and after July 2, 1975: 6 years and 3 months after the period of the account. Records are normally retired to Federal Record Centers within 1 or 2 years after payment and audit.

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.

3.4 What are the procedures for the elimination or transfer of SPI?

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

Electronic records are retained if required (GRS Schedule 1.1, Item #10), and are destroyed IAW NARA disposition instructions. [Destroy 6 years after final payment or cancellation, but longer retention is authorized if required for business use.] Nightly job that removes data outside of retention period deletes / destroys metadata and image to re-use file storage. If there are paper records needed to be destroyed, they are placed into large, locked bins throughout the facility. They are destroyed each Friday by a contracted shredder company.

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.

BAM follows VA policy to minimize the use of PII during testing or training. The VA Financial Services Center uses techniques to minimize the risk to privacy be disallowing the use of PII for research/testing/training. Our Information System Owner (ISO) and Information System Security Officers (ISSOs) enforce the policy that the only environments that can have live data is pre-prod and prod. No exceptions.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

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

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

Follow the format below:

Privacy Risk:

- If information is retained longer than specified, privacy information may be released to unauthorized individuals.

Mitigation:

- BAM adheres to information security requirements instituted by the VA Office of Information Technology (OIT).
- Both contractor and VA employees are required to take Privacy, HIPAA, and information security training annually.
- We are also finalizing procedures to automate the destruction of media at the

appropriate time based on published NARA and VA instructions.

- access granted only to those with a valid need to know Access to the records is restricted to VA Finance employees. These records are protected from outside access by Federal Protective Service
- File access granted only to those with a valid need to know Access to the records is restricted to VA Finance employees. These records are protected from outside access by Federal Protective Service

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***
FSC Data Depot	Invoice analysis for errors and fraud.	Business Name First name Last name	Encrypted network traffic only within

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*
		Middle name Tax ID number Financial Institute Account number ABA Routing ID Account Sole proprietorship first name Last name Middle name Tax ID number Financial Institute Account number ABA Routing ID Account Vendor Code Vendor Type Used ID Account User ID BAM Vendor fields: VENDORNAME ADDRESS1 ADDRESS2 CITY, STATE, ZIP VENDTYPE PHONE CONTACT CUSTACCT CREDITCARD SSNTAXID BANKNUMB BANKNAME CORRBANKNUMB CORRBANK ACCTNUMB BANKACCTYPE BANKCITY BANKSTATE BANKZIP SSNTAXIDIND EMAIL	boundary through the Enterprise Service Bus (ESB)

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:
BAM does not share information directly with internal organizations and there are no connections to external organizations. Only statistics regarding how many invoices checked and the dollar amount is pulled for operational review. VendorFile/ESB provides access to large amount of Vendor data which is necessary for the purpose of providing services to the VA and billing for those services. The compromise of this information would constitute a breach of confidence with the Vendors served by VA.

Mitigation:
BAM does not share information directly with internal organizations and there are no connections to external organizations. Only statistics regarding how many invoices checked and the dollar amount is pulled for operational review.

The source data used already exists in the other systems, and the electronic transfers of information are secure. All access is done through secure internal VA networks. Only selected users have access to PHI data.

- IBM's Enterprise Content Management system (FileNet is the Financial Service Center's new electronic records management system. It adheres to information security requirements instituted by the VA Office of Information Technology (OIT).
- Both contractor and VA are required to take Privacy, HIPAA, and information security training annually.
- Information is shared in accordance with VA Handbook 6500.
- File access granted only to those with a valid need to know.

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				

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.

*If no External Sharing listed on the table above, **(State there is no external sharing in both the risk and mitigation fields).***

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: No Privacy risk

Mitigation: No Mitigation necessary.

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.

BAM does not collect data from a veteran or vendor. This is done within other System ATOs. All data used by BAM is collected by other systems and these systems have responsibility for notification per policy.

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

N/A - The data analyzed is managed by other system ATOs. This section would be considered not applicable.

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 data analyzed is managed by other system ATOs. This section would be considered not applicable.

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.

A notice was not provided. BAM does not collect information directly from the Veteran, but instead from the source applications listed in section 1.2 of this PIA. The source systems collecting the information would provide the notice. The System of Record Notice (SORN) Sorn 13VA047 Individuals Submitting Invoices-Vouchers for Payment-VA 2020-08611.pdf (govinfo.gov) indicates all purposes of use and records categories stored in the BAM system.

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.

Not applicable to BAM.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (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 Transparency: *Has sufficient notice been provided to the individual?*

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

Privacy Risk: Any right to consent to use the information would be handled by the source systems that collect the information from the Veteran and feed BAM with information.

Mitigation: The VA mitigates this risk by providing the public with notice that the system exists, as discussed in detail in Question 6.1 under the System of Record Notice.

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.***

Veterans can correct/update their information online via the VA's eBenef itswebsite. https://www.ebenefits.va.gov VA employees may access their information by contacting their servicing HR office Additionally, any Veteran may request access to one's own health documents by completing VA Form 10-5345a, (Individuals' Request for a Copy of their Own Health Information) which can be obtained online at http://www.va.gov/vaforms/medical/pdf/vha-10-5345a-fill.pdf

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)?

Not applicable to BAM.

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?

Veterans can correct/update their information online via the VA's eBenefitswebsite. https://www.ebenefits.va.gov VA employees may access their information by contacting their servicing HR office Additionally, any Veteran may request access to one's own health documents by completing VA Form 10-5345a, (Individuals' Request for a Copy of their Own Health Information) which can be obtained online at https://www.va.gov/vaforms/medical/pdf/VHA%20Form%2010-5345a%20Fill-revision.pdf

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.

- Veterans can correct/update their information online via the VA's eBenefits website. https://www.ebenefits.va.gov
- VA employees may access their information by contacting their servicing HR office.

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.

These SORNs associated with the data available via the other ATO portal can be found on-line at: http://www.oprm.va.gov/privacy/systems_of_records.aspx . If the invoice has erroneous or incomplete information the then vendor will be notified of what is missing or incomplete via snail mail or email if we have that on file.

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

*Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. **Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

- BAM does not collect PII/PHI information directly from individuals. Nevertheless, Veterans can correct/update their information online via the VA's eBenefits website. http://benefits.va.gov/benefits/offices.asp
- These payment records are compiled from documentation from the vendor, contractor, and employee; Dun and Bradstreet (identifying numbers); and procurement and authorization documentation generated by the Veterans Administration.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?

This question is related to privacy control IP-3, Redress.

Follow the format below:

Privacy Risk:
Inaccurate data may be used to process payments. There is a risk that individuals whose records contain incorrect information may not receive timely correspondence or services.

Mitigation:
The information in BAM is obtained via the vendor sending in an invoice as previously stated. If there is erroneous or inaccurate information, the vendor may need to submit a corrected invoice. Any validation performed would merely be the Vendor personally reviewing the information before they provide it. Individuals can provide updated information for their records by submitting new forms or correspondence and indicating to the VA that the new information supersedes the previous data. See answer under 7.1 for the vendors outlet to call regarding their information.

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?

- Individuals must take and pass training on Privacy, HIPAA, information security, and government ethics.
- Individuals must have a completed security investigation.
- Once training and the security investigation are complete, a request is submitted for access…before access is granted; this request must be approved by the supervisor, Information Security Officer (ISO), and OIT.
- Site administrator(s) established at each VA location and grant access to the appropriate people. They can grant a read only access or certifying official access. When access is granted or removed **9957** security forms are generated.

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?

N/A – Other agencies do not have access to this system.

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.

There are only two roles. Read Only and Read-Write.

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 are required to sign an NDA or confidentiality agreement. Contractors will have access to the system and their contracts are reviewed on an annual basis.
- Contractors must take and pass training on Privacy, HIPAA, information security, and government ethics.
- Contractors must have a completed security investigation.
- Once training and the security investigation are complete, a request is submitted for access before access is granted, this request must be approved by the government supervisor, Information Security Officer (ISO), and Office of Information & Technology (OIT).
- Site administrator(s) established at each VA location and grant access to the appropriate people. They can grant a read only access or certifying official access. When access is granted or removed 9957 security forms are generated.

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.

Privacy and Information Security Awareness and Rules of Behavior (TMS course # 10176) is required for all Federal and Contractor personnel that require access to the VA Network. Annual training compliance is closely monitored.

Other required Talent Management System courses are provided monitored for compliance: VA 10203: Privacy and HIPAA Training VA 3812493: Annual Government Ethic

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* July 1st, 2022
3. *The Authorization Status:* Approved
4. *The Authorization Date:* Sept 27th, 2022
5. *The Authorization Termination Date:* March 26th, 2023
6. *The Risk Review Completion Date:* August 16, 2022
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

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

Not applicable.

Section 9 – Technology Usage

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

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

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

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

N/A – BAM does not use the cloud model

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

N/A – BAM does not use cloud technology.

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.

No CSP data collected.

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.

Not applicable to BAM

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).

Not applicable to BAM.

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**
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.

PAMELA SMITH

Digitally signed by PAMELA SMITH
Date: 2024.04.01 16:17:46 -05'00'

Privacy Officer, Pamela M. Smith

RONALD MURRAY

Digitally signed by RONALD MURRAY
Date: 2024.04.02 09:17:01 -05'00'

Information System Security Officer, Ronald Murray

JONATHAN LINDOW

Digitally signed by JONATHAN LINDOW
Date: 2024.04.02 13:59:22 -05'00'

Information System Owner, Jonathan Lindow

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; screen shot of a website collection privacy notice).

HELPFUL LINKS:

General Records Schedule
https://www.archives.gov/records-mgmt/grs.html

National Archives (Federal Records Management):
https://www.archives.gov/records-mgmt/grs

VA Publications:
https://www.va.gov/vapubs/

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