Privacy Impact Assessment for the VA IT System called:

Integrated Financial and Acquisition Management System (iFAMS)

VACO

Financial Management Business Transformation

Date PIA submitted for review:

07/05/2022

System Contacts:

<table>
<thead>
<tr>
<th>System Contacts</th>
<th>Name</th>
<th>E-mail</th>
<th>Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Officer</td>
<td>Princess Miller</td>
<td><a href="mailto:Princess.Miller@va.gov">Princess.Miller@va.gov</a></td>
<td>(512) 460-5148</td>
</tr>
<tr>
<td>Information System Security Officer</td>
<td>Rito-Anthony B. Brisbane</td>
<td><a href="mailto:Rito-Anthony.Brisbane@va.gov">Rito-Anthony.Brisbane@va.gov</a></td>
<td>(512) 460-5081</td>
</tr>
<tr>
<td>Information System Owner</td>
<td>Jonathan Lindow</td>
<td><a href="mailto:Jonathan.Lindow@va.gov">Jonathan.Lindow@va.gov</a></td>
<td>737-802-9565</td>
</tr>
</tbody>
</table>
Abstract

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

Integrated Financial Management and Acquisition System (iFAMS) is a cloud-based momentum application intended to revolutionize Veterans Affairs financial reporting, accounting, and delivery of benefits to veterans and their beneficiaries as well as facility. This application is located within the VA Enterprise Cloud Service enclave and cloud service provider is Microsoft Azure Government (MAG). MAG has been certified as a FedRAMP High cloud though iFAMS is categorized as a moderate impact system based on a security risk assessment on the bearing of VA data surrounding confidentiality, integrity, and access. iFAMS data is covered under the notice 13VA047, Individuals Submitting Invoices-Vouchers for Payment and Accounting Transactional Data. Its system of records comprises of financial, accounting, benefit and, transactional data across the VA enterprise nationwide. Use case constitutes VA meeting financial management objectives for veterans, veteran health providers, and dependents. Data from thousands of veterans and their dependents, VA employees, VA contractors, and members of the public are collected and stored in this system. VA retains ownership of the data use, storage, security, access, sharing, and controls all of engagement concerning data. iFAMS is replacing Financial Management System (FMS) a mainframe financial management system that interfaces with external and internal financial systems. iFAMS will interconnect to various systems and share data in the same manner. This modernization effort is expected to span until 2026. Currently, iFAMS has external interfaces with Department of Treasury, General Service Administration (GSA), US Bank, and Health and Human Services (HHS). iFAMS shares data internally to the following systems: FMS, Financial Reporting Data Warehouse (FRDW), Financial Reporting System (FRS), Human Resources – Payroll Application Services (HR-Pas), Credit Card System (CCS), and Invoice Payment Processing System (IPPS), AAMS/eCMS, ConcurGov, PCS Travel, FSC Vendor Portal, FSC Data Depot, Frontier, MCAP-DSS, MinX, and WebLGY.

Overview

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

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

MAG has been certified as a FedRAMP High cloud though iFAMS is categorized as a moderate impact system based on a security risk assessment on the bearing of VA data surrounding confidentiality, integrity, and access. iFAMSs data is covered under the notice 13VA047, Individuals Submitting Invoices-Vouchers for Payment and Accounting Transactional Data. Its system of records comprises of financial, accounting, benefit and, transactional data across the VA enterprise nationwide. Use case constitutes VA meeting financial management objectives for veterans, veteran health providers, and dependents. Data from thousands of veterans and their dependents, VA employees, VA contractors, and members of the public are collected and stored in this system. VA retains ownership of the data use, storage, security, access, sharing, and controls all of engagement concerning data.

iFAMS is replacing Financial Management System (FMS) a mainframe financial management system that interfaces with external and internal financial systems. iFAMS will interconnect to various systems and share data in the same manner. This modernization effort is expected to span until 2026. Currently, iFAMS has external interfaces with Department of Treasury, General Service Administration (GSA), US Bank, and Health and Human Services (HHS). iFAMS shares data internally to the following systems: FMS, Financial Reporting Data Warehouse (FRDW), Financial Reporting System (FRS), Human Resources – Payroll Application Services (HR-PAS), Credit Card System (CCS), and Invoice Payment Processing System (IPPS), AAMS/eCMS, ConcurGov, PCS Travel, FSC Vendor Portal, FSC Data Depot, Frontier, MCAP-DSS, MinX, and WebLYG.

Integrated Financial Acquisition Management System (iFAMS) is owned by Financial Service Center. iFAMS intends to provide a comprehensive financial management system that enables VA to meet financial management objectives and comply with VA financial management policies and federal regulations. As this is a national system, iFAMS will span across all administrations, facilities, and offices throughout VA that provide benefits to veterans, their beneficiaries, physicians for veteran care, vendors, and VA employee payments such as travel and/or HR related activities. This application will collect data from thousands of veterans and their dependents, VA employees, VA contractors, and members of the public are collected and stored in this system. iFAMS general description of PII being collected and maintained are as follows:

- Names of recipients
- Email address
- Mailing address
- Banking account number electronic funds transfer/Automated Clearing House (EFT/ACH) routing information from individual
- Financial account information
- Credit Card Numbers,
- Taxpayer Identification Number (TIN)
- Social security numbers/Tax ID of government employees,
- Credit card numbers
- Internet IP Addresses
- Retirement Information
- Life Insurance Information
- Medicare Information
- Health Insurance Information
- Voluntary Separation Information
• Incentive Award
• Senior Executive Service Award
• Travel Savings Award
• Relocation Incentive
• Recruitment Incentive
• Hazard Pay
• Student Loan Repayment
• Supervisory Differential
• Vendor ID

Veterans and vendors/customers that do business with Veterans Affairs sensitive information is required to execute legal required receivables and payments through the United States Treasury and financial system entities. Legal authorities for which this system collects SSN's Federal Managers Financial Act (FMFIA); OMB Circular A-130, A-127, and A-123; and Executive Order 9397. External information sharing of Integrated Financial Acquisition Management System (iFAMS) data will conducted through a connection to web-based portal System Award Management (SAM) through SMTP file transfer and this portal feeds the following sensitive vendor information:

• Sole proprietorship first name
• Last name
• Middle name
• Tax ID number
• Financial Institute
• Account number ABA Routing ID
• Account
• Lockbox number
• EFT Waiver
• Remittance Name
• Remittance Address
• Remittance City
• Remittance State
• Remittance Zip
• Remittance Country
• Accounts Receivable First Name
• Accounts Receivable Last Name
• Accounts Receivable Middle Name
• Merchant ID

iFAMS will not be operated in more than one site, this application is in the VA enterprise cloud (VAEC) within cloud service provider, Microsoft Azure. VA has ownership over the data in the VAEC. iFAMS will inherit all FedRAMP certification documentation, processes, and will follow all data custodial rights negotiated by VA when Microsoft Azure Cloud service provider was contracted by the department. iFAMS is categorized as high, Microsoft Azure is certified as a FedRAMP high cloud. Security controls protecting the environment are more in-depth than the application’s controls. The legal authority to operate this system is Public Law 100-527, 100th Congress. SORN VA13047 is being revised and is in concurrence for approval and subsequent publication in the Federal Register. As this is new system replacing the legacy system FMS, all processes and procedures are being reviewed and where responsibilities can be inherited, iFAMS will consume and where operations need to be revised and/or revamp, steps will be taken to proceed. By completing this PIA there are no technological or procedural 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://va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.

This question is related to privacy control AP-1, Authority To Collect, and AP-2, Purpose Specification.

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

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

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

- Names of recipients
- Email address
- Mailing address
- Banking account number electronic funds transfer/Automated Clearing House (EFT/ACH) routing information from individual
• Financial account information
• Credit Card Numbers,
• Taxpayer Identification Number (TIN)
• Social security numbers/Tax ID of government employees,
• Credit card numbers
• Internet IP Addresses
• Retirement Information
• Life Insurance Information
• Medicare Information
• Health Insurance Information
• Voluntary Separation Information
• Incentive Award
• Senior Executive Service Award
• Travel Savings Award
• Relocation Incentive
• Recruitment Incentive
• Hazard Pay
• Student Loan Repayment
• Supervisory Differential
• Vendor ID
• Sole proprietorship first name
• Last name
• Middle name
• Tax ID number
• Financial Institute
• Account number ABA Routing ID
• Account
• Lockbox number
• EFT Waiver
• Remittance Name
• Remittance Address
• Remittance City
• Remittance State
• Remittance Zip
• Remittance Country
• Accounts Receivable First Name
• Accounts Receivable Last Name
• Accounts Receivable Middle Name
• Merchant ID

PII Mapping of Components

iFAMS consists of 7 key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by iFAMS and the reasons for the collection of the PII are in the table below.
## PII Mapped to Components

<table>
<thead>
<tr>
<th>Database Name of the information system collecting/storing PII</th>
<th>Does this system collect PII? (Yes/No)</th>
<th>Does this system store PII? (Yes/No)</th>
<th>Type of PII (SSN, DOB, etc.)</th>
<th>Reason for Collection/Storage of PII</th>
<th>Safeguards</th>
</tr>
</thead>
</table>
| Integrated Financial Acquisition Management System (iFAMS) Production Production | Yes | Yes | Name, SSN(s), email address, mailing address, financial account information, banking account number from individual, banking account number from Vendor, Agency banking account number, Electronic Funds Transfer / Automated Clearing House routing information, Credit Card Numbers, Taxpayer Identification Number (TIN), and data required to process receivables and payments through the United States Treasury and financial system entities. | iFAMS is VA’s implementation of the CGI Momentum Financials® product. Momentum is a commercial off-the-shelf (COTS) software solution. The product provides budgeting, acquisition and financial management capabilities specifically designed for the Federal Government. | MOU/ISA in place between iFAMS and:  
  - Department of Treasury  
  - System for Awards Management - General Services Administration (GSA-SAM)  
  - US Bank  
  - Health and Human Services – Payment Management System (HHS-PMS)  
  - mLINQS Hosting Service (MHS) (iMove) |
| Integrated Financial Acquisition Management System (iFAMS) Production Standby | Yes | Yes | Name, SSN(s), email address, mailing address, financial account information, banking account number from individual, banking account number from Vendor, Agency banking account number, Electronic Funds Transfer / Automated Clearing House routing information, Credit Card Numbers, Taxpayer Identification Number (TIN), and data required to process receivables and payments through the United States Treasury and financial system entities. | iFAMS is VA’s implementation of the CGI Momentum Financials® product. Momentum is a commercial off-the-shelf (COTS) software solution. The product provides budgeting, acquisition and financial management capabilities specifically designed for the Federal Government. | MOU/ISA in place between iFAMS and:  
  - Department of Treasury  
  - System for Awards Management - General Services Administration (GSA-SAM) |
<table>
<thead>
<tr>
<th>Service</th>
<th>Use Case</th>
<th>Details</th>
<th>MOU/ISA in place between iFAMS and:</th>
<th>MOU/ISA in place between iFAMS and:</th>
</tr>
</thead>
</table>
| Financial Management Service (FMS) | Yes      | Identification Number (TIN), and data required to process receivables and payments through the United States Treasury and financial system entities. Provides budgeting, acquisition and financial management capabilities specifically designed for the Federal Government. | • US Bank  
• Health and Human Services – Payment Management System (HHS-PMS)  
• mLINQS Hosting Service (MHS) (iMove) | |
| Human Resources – Payroll Application Services (HR-PAS) | Yes      | Identification Number (TIN), and data required to process receivables and payments through the United States Treasury and financial system entities. Name, SSN(s), email address, mailing address, financial account information, banking account number from individual, banking account number from Vendor, Agency banking account number, Electronic Funds Transfer / Automated Clearing House routing information, Credit Card Numbers, Taxpayer Identification Number (TIN), and data required to process receivables and payments through the United States Treasury and financial system entities. iFAMS is VA’s implementation of the CGI Momentum Financials® product. Momentum is a commercial off-the-shelf (COTS) software solution. The product provides budgeting, acquisition and financial management capabilities specifically designed for the Federal Government. | MOU/ISA in place between iFAMS and:  
• Department of Treasury  
• System for Awards Management - General Services Administration (GSA-SAM)  
• US Bank  
• Health and Human Services – Payment Management System (HHS-PMS)  
• mLINQS Hosting Service (MHS) (iMove) | |
<table>
<thead>
<tr>
<th>Service Description</th>
<th>MOU/ISA in place between iFAMS and:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recruitment Incentive</td>
<td>Department of Treasury</td>
</tr>
<tr>
<td>Retention Incentive</td>
<td>System for Awards Management - General Services Administration (GSA-SAM)</td>
</tr>
<tr>
<td>Hazard Pay</td>
<td></td>
</tr>
<tr>
<td>Student Loan Rayment Incentive</td>
<td>US Bank</td>
</tr>
<tr>
<td>Incentive Supervisory Differential</td>
<td>Health and Human Services – Payment Management System (HHS-PMS)</td>
</tr>
<tr>
<td>Director Pay</td>
<td>mLINQS Hosting Service (MHS) (iMove)</td>
</tr>
<tr>
<td>Software solution. The product provides budgeting,</td>
<td></td>
</tr>
<tr>
<td>acquisition and financial management capabilities</td>
<td></td>
</tr>
<tr>
<td>specifically designed for the Federal Government.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Financial Reporting Data Warehouse (FRDW)</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>SSN</td>
<td></td>
</tr>
<tr>
<td>Stub Name</td>
<td></td>
</tr>
<tr>
<td>iFAMS is VA’s implementation of the CGI Momentum</td>
<td></td>
</tr>
<tr>
<td>Financials® product. Momentum is a commercial off-the</td>
<td></td>
</tr>
<tr>
<td>shelf (COTS) software solution. The product provides</td>
<td></td>
</tr>
<tr>
<td>budgeting, acquisition and financial management</td>
<td></td>
</tr>
<tr>
<td>capabilities specifically designed for the Federal</td>
<td></td>
</tr>
<tr>
<td>Government.</td>
<td></td>
</tr>
<tr>
<td>MOU/ISA in place between iFAMS and:</td>
<td></td>
</tr>
<tr>
<td>Department of Treasury</td>
<td></td>
</tr>
<tr>
<td>System for Awards Management - General Services</td>
<td></td>
</tr>
<tr>
<td>Administration (GSA-SAM)</td>
<td></td>
</tr>
<tr>
<td>US Bank</td>
<td></td>
</tr>
<tr>
<td>Health and Human Services – Payment Management System</td>
<td></td>
</tr>
<tr>
<td>(HHS-PMS)</td>
<td></td>
</tr>
<tr>
<td>mLINQS Hosting Service (MHS) (iMove)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Charge Card Services (CCS)</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>User ID</td>
<td></td>
</tr>
<tr>
<td>Title</td>
<td></td>
</tr>
<tr>
<td>Vendor Address Code</td>
<td></td>
</tr>
<tr>
<td>Vendor Code</td>
<td></td>
</tr>
<tr>
<td>iFAMS is VA’s implementation of the CGI Momentum</td>
<td></td>
</tr>
<tr>
<td>Financials® product. Momentum is</td>
<td></td>
</tr>
<tr>
<td>MOU/ISA in place between iFAMS and:</td>
<td></td>
</tr>
<tr>
<td>Department of Treasury</td>
<td></td>
</tr>
<tr>
<td>Invoice Payment Processing System</td>
<td>Yes</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-----</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
1.2 What are the sources of the information in the system?

List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

Describe why information from sources other than the individual is required. For example, if a program’s system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question 1.3 indicate why the system is using this source of data.

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

This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

Information is provided by the individual or legal representative as part of an application for a benefit, contract or reimbursement. Data could potentially be obtained from a VA administration, facility and/or medical center; vendor for which VA is doing business; Department of Treasury; Internal Revenue Service; and other Federal entities. Also, sensitive data is shared from SAM system which is a one-way interfacing system through SMTP transfer.

1.3 How is the information collected?

This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technology used in the storage or transmission of information in identifiable form?

If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form’s OMB control number and the agency form number.

This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

Data is being collected by interfacing system, SAM, for iFAMS. SAM is the Commercial Off The Shelf (COTS) product, Momentum’s Central Contractor Registry Connector (CCRC) module. Data is obtained from a VA administration, facility and/or medical center; vendor for which VA is doing business; Department of Treasury; Internal Revenue Service; and other Federal entities. Also, sensitive data is shared from SAM system which is a one-way interfacing system through SMTP transfer. Data collections are listed in section 5.1.

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

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

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

VA will take reasonable steps through system configurations and administrative processes and procedures to confirm and affirming the accuracy of PII being collected. The types of measures taken to protect data quality will be based on the nature and context of the PII, how it is to be used, and how it was obtained. Measures taken to validate the accuracy of PII that is used to make determinations about the rights, benefits, or privileges of individuals under federal programs will be more comprehensive than those used to validate less sensitive PII. Additional steps will be necessary to validate PII that is obtained from sources other than individuals or the authorized representatives of individuals.

Information is checked for accuracy on a continuous basis, per VA’s established policies for Assessment & Authorization and Continuous Monitoring.

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

- Department of Veterans Affairs Act, Public Law 100-527, 100th Congress
- Federal Managers Financial Act (FMFIA);
- OMB Circular A-130, A-127, and A-123;
- Executive Order 9397, Numbering System for Federal Accounts Relating to Individual Persons; and
- VA financial related policies and procedures.
- SORN notice 13VA047, Individuals Submitting Invoices-Vouchers for Payment and Accounting Transactional Data

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

Consider the following Fair Information Practice Principles (FIPPs) when assessing the risk to individual privacy:
Principle of Purpose Specification: Explain how the collection ties with the purpose of the underlying mission of the organization and its enabling authority.

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

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

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

Follow the format below when entering your risk assessment:

**Privacy Risk:** Information being collected, used, stored, and disseminated is directly related to rendering payment, benefits, and accounting purposes which directly supports iFAMS. Privacy risks are surrounding the sensitivity of the information being collected, maintained and stored. Also, there is a breach risk in the volume of data being stored. If data is exposed the department would be in grave risk for financial hardship and damaged reputation.

**Mitigation:** iFAMS is being hosted in Microsoft Azure certified as a high impact cloud. FedRAMP High impact controls surrounding the environment will add on an extra layer of protection through confidentiality, integrity, and availability for iFAMS information. Additionally, as an agency requirement all employees with access to this application would have to complete the VA Privacy and Information Security Awareness Training and Rules of Behavior and Departmental Privacy training.

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.
Information collected is being used to support dissemination of benefits, financial, accounting required receivables and payments through the United States Treasury, Internal Revenue Service, and other financial system entities.

<table>
<thead>
<tr>
<th>IDENTIFIER</th>
<th>PURPOSE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of recipients</td>
<td>Used to identify individual / Sole proprietor</td>
</tr>
<tr>
<td>Email address</td>
<td>Used to contact individual</td>
</tr>
<tr>
<td>Mailing Address</td>
<td>Used to locate individual</td>
</tr>
<tr>
<td>Bank Account Number EFT/ACH</td>
<td>Used for benefit / invoicing / payment distribution</td>
</tr>
<tr>
<td>Financial Account Information</td>
<td>Used for benefit / invoicing / payment distribution</td>
</tr>
<tr>
<td>Credit Card Number</td>
<td>Used for benefit / invoicing / payment distribution</td>
</tr>
<tr>
<td>TIN</td>
<td>Used for benefit / invoicing / payment distribution</td>
</tr>
<tr>
<td>SSN</td>
<td>Used to identify individual / Sole Proprietor</td>
</tr>
<tr>
<td>Internet IP Address</td>
<td>Used to identify individual / Sole Proprietor</td>
</tr>
<tr>
<td>Sole Proprietor First Name</td>
<td>Used to identify individual / Sole Proprietor</td>
</tr>
<tr>
<td>Sole Proprietor Last Name</td>
<td>Used to identify individual / Sole Proprietor</td>
</tr>
<tr>
<td>Sole Proprietor Middle Name</td>
<td>Used to identify individual / Sole Proprietor</td>
</tr>
<tr>
<td>Sole Proprietor TIN</td>
<td>Used for benefit / invoicing / payment distribution</td>
</tr>
<tr>
<td>Sole Proprietor Financial Institute</td>
<td>Used for benefit / invoicing / payment distribution</td>
</tr>
<tr>
<td>Sole Proprietor Account Number Routing ID</td>
<td>Used for benefit / invoicing / payment distribution</td>
</tr>
<tr>
<td>Sole Proprietor Account</td>
<td>Used for benefit / invoicing / payment distribution</td>
</tr>
<tr>
<td>Sole Proprietor Lockbox Number</td>
<td>Used for benefit / invoicing / payment distribution</td>
</tr>
<tr>
<td>Sole Proprietor EFT Waiver</td>
<td>Used for benefit / invoicing / payment distribution</td>
</tr>
<tr>
<td>Sole Proprietor Remittance Name</td>
<td>Used to identify individual / Sole Proprietor</td>
</tr>
<tr>
<td>Sole Proprietor Remittance Address</td>
<td>Used to locate individual</td>
</tr>
<tr>
<td>Sole Proprietor Remittance City</td>
<td>Used to locate individual</td>
</tr>
<tr>
<td>Sole Proprietor Remittance State</td>
<td>Used to locate individual</td>
</tr>
<tr>
<td>Sole Proprietor Zip</td>
<td>Used to locate individual</td>
</tr>
<tr>
<td>Sole Proprietor Country</td>
<td>Used to locate individual</td>
</tr>
<tr>
<td>Accounts Receivable First Name</td>
<td>Used to identify individual / Sole Proprietor</td>
</tr>
<tr>
<td>Accounts Receivable Last Name</td>
<td>Used to identify individual / Sole Proprietor</td>
</tr>
<tr>
<td>Accounts Receivable Middle Name</td>
<td>Used to identify individual / Sole Proprietor</td>
</tr>
<tr>
<td>Merchants ID</td>
<td>Used for benefit / invoicing / payment distribution</td>
</tr>
</tbody>
</table>

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

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

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

This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

At this stage in the development of the system, there are no data analytic tools and/or business intelligence used. In future system implementations, tools to perform predictive analytics, data analysis, data matching, relational analysis, scoring, and reporting will be utilized.

2.3 How is the information in the system secured?

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

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

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

This question is related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest

Microsoft Azure Government (MAG) Infrastructure that iFAMS leverages: This is inherited from FedRAMP JAB authorized package ID F1603087869 for Microsoft - Azure Government (High-IaaS). Communications through VAEC are inherited. Additionally, all commercial databases and applications (e.g., Oracle databases, IBM Tivoli suite, CA Product suite, etc.) conform to the mandates of FIPS 140-2 in regard to encrypting data at rest.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information. How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. Example: Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.

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

Principle of Transparency: Is the PIA and SORN, if applicable, clear about the uses of the information?

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?

This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.
Access control to PII is determined by system security roles and responsibilities created in system configuration and determined and assigned by programmatic offices. Through the assigned security roles individuals will only have access to information that they have been designated “need to know.” Additionally, programmatic offices/administrations/facilities will only have access to their assigned locations and other locations are segregated by firewall configuration. These safeguards are in place to control access. Additionally, iFAMS has robotic monitoring tools connecting to the system to manage and track security anomalies. iFAMS data is covered under the notice 13VA047, Individuals Submitting Invoices-Vouchers for Payment and Accounting Transactional Data. Its system of records comprises of financial, accounting, benefit and, transactional data across the VA enterprise nationwide. Use case constitutes VA meeting financial management objectives for veterans, veteran health providers, and dependents.

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

- Names of recipients
- Email address
- Mailing address
- Banking account number EFT/ACH routing information from individual
- Financial account information
- Credit Card Numbers,
- Taxpayer Identification Number (TIN)
- Social security numbers/Tax ID of government employees,
- Credit card numbers
- Internet IP Addresses
- Sole proprietorship first name
- Last name
- Middle name
- Tax ID number
- Financial Institute
- Account number ABA Routing ID
- Account
- Lockbox number
- EFT Waiver
- Remittance Name
• Remittance Address
• Remittance City
• Remittance State
• Remittance Zip
• Remittance Country
• Accounts Receivable First Name
• Accounts Receivable Last Name
• Accounts Receivable Middle Name
• Merchant ID
• SSN
• Stub Number
• Retirement Indicator
• Retirement
• OASDI or Social Security
• Life Insurance
• Medicare
• Health Insurance
• Voluntary Separation Incentive Award
• Incentive Award
• Senior Executive Service Award
• Travel Savings Award
• Relocation Incentive
• Recruitment Incentive
• Retention Incentive
• Hazard Pay
• Student Loan Repayment Incentive
• Supervisory Differential

3.2 How long is information retained?

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

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

iFAMS data is retained in the current application for three years after date of creation. Data will then be archived to a data lake for hot storage for two years and transferred into cold storage until it meets the disposition date documented in the records control schedule, 10-1 VHA RCS.
3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so please indicate the name of the records retention schedule.

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner.

This question is related to privacy control DM-2, Data Retention and Disposal.

PII maintained in iFAMS has a data retention period notated in the Financial Management and Reporting Records, MP-4, Part X Change 2, dated May 26, 1982. Also, 10-1 VHA RCS contains retention and disposition requirements for Office of Finance records which have been authorized by NARA or have been assigned a General Record Schedule (GRS) disposal authority. The VHA RCS 10-1, until MP-4, Part X Change 2 is revised, is the main authority for the retention and disposition requirements of Office of Finance records. It provides a brief description of the records, states the retention period and disposition requirements. The actual defined period will be different depending on the specific record type. This requirement is also documented in the newly revised SORN 13VA047 Individuals Submitting Invoices-Vouchers for Payment and Accounting.

3.4 What are the procedures for the elimination of SPI?

Explain how records are destroyed or eliminated at the end of the retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc?

This question is related to privacy control DM-2, Data Retention and Disposal.

In accordance with VA Directive 6371 Destruction of Temporary Records, it is VA policy that all Federal records contained on paper, electronic, or other medium are properly managed from their creation through their final disposition, in accordance with Federal laws, the GRS and VHA Records Control Schedule (RCS) 10-1. GRS can be found at www.archives.gov. VA Directive 6300, Records and Information Management contains the policies and responsibilities for VA’s Records and Information Management program. VA Handbook 6300.1, “Records Management Procedures”, Section 3.2, contains mandatory procedures for the proper management of eliminating data at the end of the retention period. Procedures are enforced by Records Management Staff and VA Records Officers.

Additionally, iFAMS will comply with VA Directive 6500 Control DM-2

- VA will retain PII and/or PHI for the minimum amount of time to fulfill the purpose(s) identified in the notice or as required by law;
- Dispose of, destroy, erase, and/or anonymize the PII and/or PHI, regardless of the method of storage in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and
- Use approved records disposition schedules to ensure secure deletion or destruction of PII and/or PHI (including originals, copies, and archived records).
• Program officials coordinate with records officers and with NARA to identify appropriate retention periods and disposal methods.

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

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

Financial Management Business Transformation (FMBT) has developed programmatic policies that discuss minimalization of PII within test data. Privacy and Security training was developed and conducted on June 15, 2020, that discussed the use of Mock data when appropriate and only using live data within an accredited site. Additional, reminders have been sent through mass emails to the project personnel including contractor and government staff that reiterate the importance of using deidentified and/or mock data to test within non-accredited site. All Financial Management Business Transformation (FMBT) program activities e.g. analysis, testing, UAT, etc. (with the exception of ‘go live’ production migration) shall use data that has been masked or processed into synthetic data to safeguard PII sensitive data. All FMBT requests to system owners for data examples, test data, etc. shall explicitly specify the data to be provided by the request recipient has been appropriately masked prior to transfer to the requestor. In cases where system owners, representatives, etc. are unable or data volume considerations make it unapproachable to perform masking of sample and/or test data, the data cleansing/ETL team shall be engaged for assistance before the data is transferred. All sensitive data transferred for subsequent masking by the data cleansing/ETL team shall be encrypted in transit.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

Consider the following FIPPs below to assist in providing a response:
Principle of Minimization: Does the project retain only the information necessary for its purpose? Is the PII retained only for as long as necessary and relevant to fulfill the specified purposes?

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

Follow the format below:

**Privacy Risk:** If information maintained by iFAMS is retained for longer than is necessary to fulfill the VA mission, records held longer than required are at greater risk of being unintentionally released or breached.

**Mitigation:** To mitigate the risk posed by information retention, the iFAMS adheres to the VA RCS schedules for each category or data it maintains. When the retention data is reached for a record, the medical center will carefully dispose of the data by the determined method as described in question 3.4. VA Handbook 6500.2, “Management of Data Breaches Involving Sensitive Personal Information (SPI),” contains the policies and responsibilities that VA components are required to follow to manage data breaches, including detection, correlation, notification, remediation, and reporting.

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

<table>
<thead>
<tr>
<th>List the Program Office or IT System information is shared/received with</th>
<th>List the purpose of the information being shared /received with the specified program office or IT system</th>
<th>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</th>
<th>Describe the method of transmittal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office of Financial Services (FSC)</td>
<td>Human Resources – Payroll Application Services (HR-PAS)</td>
<td>SSN, Stub Name, Retirement Indicator, Retirement, Social Security, Life Insurance, Medicare, Health Insurance, Voluntary Separation Incentive Award, Incentive Award, Senior Executive Service Award, Travel Savings Award, Relocation Incentive, Recruitment Incentive, Hazard Pay, student Loan Repayment, Supervisory Differential</td>
<td>Secure File Transfer Protocol server (SFTP)</td>
</tr>
<tr>
<td>Office of Finance/Financial Management Services (FMS)</td>
<td>FMS is the legacy system of iFAMS</td>
<td>Name, SSN(s), email address, mailing address, financial account information, banking account number from individual, banking account number from Vendor, Agency banking account number, Electronic Funds Transfer/Automated Clearing House routing information, Credit Card Numbers, Taxpayer Identification Number (TIN), and data required to process receivables and payments through the United States Treasury and financial system entities.</td>
<td>SFTP server</td>
</tr>
<tr>
<td>Financial Service Center (FSC)/Financial Reporting Data</td>
<td>Financial Reporting Data Warehouse (FRDW) – an Oracle-based data</td>
<td>Stub Name, SSN</td>
<td>SFTP server/File Splitting</td>
</tr>
<tr>
<td>List the Program Office or IT System information is shared/received with</td>
<td>List the purpose of the information being shared/received with the specified program office or IT system</td>
<td>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</td>
<td>Describe the method of transmittal</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Warehouse (FRDW)</td>
<td>repository that provides a system for reporting financial data from iFAMS. FRDW stores summary financial data from iFAMS and detail data from the payroll system, and is used for reporting, financial statement creation, and reconciliation of summarized data back to the details.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FSC/ Charge Card System (CCS)</td>
<td>Charge Card Services (CCS) - is a set of services that provide information to CCS for data storage and reporting purposes through the delivery of an iFAMS extract and transmission of the daily US Bank SBF statement file.</td>
<td>User ID, Title, User ID, Vendor Address Code, Vendor Code</td>
<td>Webservices</td>
</tr>
<tr>
<td>FSC/ Financial Report System (FRS)</td>
<td>Financial Report System (FRS) - FRS uses General Ledger and String Trial Balance data extracted from iFAMS into an Oracle database in the form of a text file. FRS loads (weeknights and at month end) budget</td>
<td>User ID, Vendor Address Code, Vendor Code, Vendor Name</td>
<td>SFTP server</td>
</tr>
<tr>
<td>List the Program Office or IT System information is shared/received with</td>
<td>List the purpose of the information being shared/received with the specified program office or IT system</td>
<td>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</td>
<td>Describe the method of transmittal</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>and spending transaction data extracted from iFAMS into an Oracle database.</td>
<td>Invoice Payment Processing System (IPPS) - is a web enabled VA enterprise payment system that is primarily used to issue VA payments to commercial vendors. IPPS is an internet portal that processes invoices after receipt of electronic invoice data and provides approval/acceptance workflow and FMS payment transaction creation.</td>
<td>Vendor Name</td>
<td>SFTP server</td>
</tr>
<tr>
<td>Office of Acquisitions (OAL)</td>
<td>Automated Acquisition Management System / Electronic Contract Management System (AAMS/eCMS) – Near-real time interface contains the data elements required to establish or modify a Contract Award or Contract Order.</td>
<td>Vendor, Vendor Address Code, Email, Duns, Login ID, Contract Number, OEM Duns Number</td>
<td>WebService</td>
</tr>
<tr>
<td>Office of Financial Services (FSC)</td>
<td>ConcurGov - used to obligate, pay and Report VA</td>
<td>Organization Fund, Vendor Code</td>
<td>Hybrid – Batch and WebService</td>
</tr>
<tr>
<td>List the Program Office or IT System information is shared/received with</td>
<td>List the purpose of the information being shared /received with the specified program office or IT system</td>
<td>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</td>
<td>Describe the method of transmittal</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>temporary duty travel (TDY) and Local Travel.</td>
<td>Vendor Address Code</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Office of Financial Services (FSC)</td>
<td>Permanent Change of Station (PCS) Travel - streamlines the process for initiating and approving documents required by employees who are relocating and are authorized to receive PCS travel reimbursements during their permanent change of station travel.</td>
<td>Vendor Code Vendor Address</td>
<td>WebService</td>
</tr>
<tr>
<td>Office of Financial Services (FSC)</td>
<td>FSC Vendor Portal - streamlines the 10-091 vendor form and enable an automated process to handle requests to create vendor records in iFAMS, specifically VA employees and non-SAM commercial vendors.</td>
<td>Vendor Remittance Address Vendor Name Contracting Officer Email Address Contracting Officer Representative Email Address Receipt Vendor Name Vendor SSN Tax Identification Number Vendor Bank ABA/BIC Bank Account Number Vendor Bank Name SSN</td>
<td>WebService</td>
</tr>
<tr>
<td>Office of Financial Services (FSC)</td>
<td>FSC Data Depot - data repository that stores IPPS related data from FMS for the exchange of order, commitment, receipt, and vendor data information.</td>
<td>Vendor Remittance Address Vendor Name Contracting Officer Email Address Contracting Officer Representative Email Address Receipt Vendor Name Vendor SSN Tax Identification Number Vendor Bank ABA/BIC Bank Account Number Vendor Bank Name SSN</td>
<td>Data Extract</td>
</tr>
<tr>
<td>List the Program Office or IT System information is shared/received with</td>
<td>List the purpose of the information being shared/received with the specified program office or IT system</td>
<td>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</td>
<td>Describe the method of transmittal</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
</tbody>
</table>
| Financial Accounting Services (FAS) | Frontier - Used to reconcile VA General Ledger entry data against corresponding Treasury system information (Intra-Governmental Payment and Collection (IPAC), Collections Information Repository (CIR), and Central Accounting Reporting System (CARS)). | Vendor Code  
Vendor Type  
Used ID  
Accounting Period  
Dollar Amount  
Check Number | Data Extract |
| Managerial Cost Accounting Office (MCAO) | Managerial Cost Accounting Program / Decision Support System (MCAP-DSS) - is used to conduct financial management and perform cost accounting and performance measurement. Since the system contains a rich repository of clinical information it is used to promote a more proactive approach to the care of high risk and high cost patients. | Organization Accounting Period | Data Extract |
| Office of Financial Services (FSC) | MinX - Hyperion-based reporting system that automates the | Trading Partner  
Dollar Amount  
Fund | Data Extract |
### 4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

*Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks. This question is related to privacy control UL-1, Internal Use.*

Follow the format below:

**Privacy Risk:** There is a risk that information may be shared with unauthorized VA program or system or that data could be shared.

<table>
<thead>
<tr>
<th>List the Program Office or IT System information is shared/received with</th>
<th>List the purpose of the information being shared/received with the specified program office or IT system</th>
<th>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</th>
<th>Describe the method of transmittal</th>
</tr>
</thead>
<tbody>
<tr>
<td>preparation of the consolidated financial statement. It is used for annual reporting, specifically reporting GL/accounting data.</td>
<td>Payment Amount, Payment Date, Payment Amount, Transaction Type</td>
<td>Hybrid – Batch and WebService</td>
<td></td>
</tr>
<tr>
<td>OFM VBAVACO (ALAC)</td>
<td>Web Loan Guaranty (WebLGY) - is responsible for managing the core processes and data involved with the VA Home Loan program. It incorporates functionality supporting the VA home loan guaranty benefit to include Eligibility, Loan Processing, Construction and Valuation, Loan Review, Property Management and Oversight.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Version Date: October 1, 2021  
Page 25 of 61
Mitigation: Safeguards implemented to ensure data is not sent to the wrong VA organization are employee security and privacy training and awareness and required reporting of suspicious activity. Agency implementation and use of two factor authentication, encryption, built in firewalls, user access according to granted permissions, and access authorization.

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

<table>
<thead>
<tr>
<th>List External Program Office or IT System information is shared/received with</th>
<th>List the purpose of information being shared / received / transmitted with the specified</th>
<th>List the specific PII/PHI data element that are processed (shared/received/transmitted) with the Program or IT system</th>
<th>List the legal authority, binding agreement, SORN routine use, etc. that permit</th>
<th>List the method of transmission and the measures in place to secure data</th>
</tr>
</thead>
</table>

Version Date: October 1, 2021
Page 26 of 61
<table>
<thead>
<tr>
<th>Program Office or IT System</th>
<th>Information Sharing</th>
<th>External Sharing (Can Be More Than One)</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Award Management (SAM) shares information with iFAMS for iFAMS use. Sharing is one-way and not bidirectional.</td>
<td>- Sole proprietorship first name&lt;br&gt;- Last name&lt;br&gt;- Middle name&lt;br&gt;- Tax ID number&lt;br&gt;- Financial Institute&lt;br&gt;- Account number ABA Routing ID&lt;br&gt;- Account&lt;br&gt;- Lockbox number&lt;br&gt;- EFT Waiver&lt;br&gt;- Remittance Name&lt;br&gt;- Remittance Address&lt;br&gt;- Remittance City&lt;br&gt;- Remittance State&lt;br&gt;- Remittance Zip&lt;br&gt;- Remittance Country&lt;br&gt;- Sole proprietorship first name&lt;br&gt;- Last name&lt;br&gt;- Middle name&lt;br&gt;- Tax ID number&lt;br&gt;- Financial Institute&lt;br&gt;- Account number ABA Routing ID&lt;br&gt;- Account&lt;br&gt;- Lockbox number&lt;br&gt;- EFT Waiver&lt;br&gt;- Remittance Name&lt;br&gt;- Remittance Address&lt;br&gt;- Remittance City&lt;br&gt;- Remittance State&lt;br&gt;- Remittance Zip&lt;br&gt;- Remittance Country</td>
<td>SORN notice 13VA047, Individuals Submitting Invoices-Vouchers for Payment and Accounting Transactional Data, MOU/ISA</td>
</tr>
<tr>
<td>HHS Payment Management System (PMS)</td>
<td>This information is collected for grants management and to pay vendors for services rendered.</td>
<td>The transmitted data contains PII which includes vendor financial data (Taxpayer Identification Number [TIN]/Employer Identification Number [EIN]/Social Security Number [SSN]) without individual’s name or company name.</td>
</tr>
</tbody>
</table>

Simple Mail Transfer Protocol (SMTP)
<table>
<thead>
<tr>
<th>US Bank (data from US Bank. No VA data is sent to US Bank from the VA.)</th>
<th>The information is collected to fulfill the function of storing and utilizing the information to pay vendors for services rendered. It is also used for employee travel budget reconciliation</th>
<th>USBconur_weekly_filelayout</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Account number</strong></td>
<td><strong>Reference Number</strong></td>
<td><strong>Posting Date</strong></td>
</tr>
<tr>
<td><strong>Passenger Name</strong></td>
<td><strong>Ticket Number</strong></td>
<td><strong>Travel Agency Code</strong></td>
</tr>
<tr>
<td><strong>Travel Agency Name</strong></td>
<td><strong>Source Amount</strong></td>
<td><strong>Obligation</strong></td>
</tr>
<tr>
<td><strong>Passenger specific data</strong></td>
<td><strong>USBANK-CCS-001-PowerTrack_filelayout</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Account number</strong></td>
<td><strong>Posting Date</strong></td>
<td><strong>Transaction Date</strong></td>
</tr>
<tr>
<td><strong>Merchant Name</strong></td>
<td><strong>Merchant City</strong></td>
<td><strong>Merchant State</strong></td>
</tr>
<tr>
<td><strong>Merchant Zip</strong></td>
<td><strong>Station</strong></td>
<td><strong>Billing Amount</strong></td>
</tr>
<tr>
<td><strong>P.O. Number</strong></td>
<td><strong>Invoice Number</strong></td>
<td><strong>Fee</strong></td>
</tr>
<tr>
<td><strong>Line item amount</strong></td>
<td><strong>Line item units</strong></td>
<td><strong>smry_amt</strong></td>
</tr>
<tr>
<td><strong>smry_amt</strong></td>
<td><strong>File_total</strong></td>
<td><strong>Dt_cr_flag</strong></td>
</tr>
<tr>
<td><strong>shipto_name</strong></td>
<td><strong>shipto_address</strong></td>
<td><strong>shipto_city</strong></td>
</tr>
<tr>
<td><strong>shipto_state</strong></td>
<td><strong>shipto_zip</strong></td>
<td></td>
</tr>
</tbody>
</table>

| Bureau of Fiscal Service Treasury Web Application Infrastructure | The information is collected to fulfill the function of payment for | The data that traverses this connection contains federal financial information as well as Privacy Act data and is classified Sensitive but Unclassified (SBU) PII data | SORN notice 13VA047, Individuals Submitting Invoices-Vouchers for Payment and Accounting Transactional Data, MOU/ISA |

| Data, MOU/ISA | SFTP (SSH File Transfer Protocol) |
| mLINQS Hosting Service (MHS), (iMOVE) | Purpose for Data Transfer: To record obligation and liquidations for taxable travel in the financial accounting system of record. | Data transmitted from MHS to Integrated Financial, and Acquisition Management System (iFAMS) will include financial information. Taxable Travel data is entered into MHS where it is processed and stored in support of taxable relocation travel. Relevant financial data is transmitted to the VA for the purpose of recording financial transaction in the VA’s financial accounting system of record. | SORN notice 13VA047, Individuals Submitting Invoices-Vouchers for Payment and Accounting Transactional Data, MOU/ISA | Data will be transmitted synchronously using SOAP over HTTPS from mLINQS, LLC to VA. |

### 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:** There is a risk that the data could be shared with an inappropriate and/or unauthorized external organization or institution.
Mitigation: The potential harm is mitigated by access control, configuration management, media protection, system and service acquisition, audit and accountability measures, contingency planning, personnel security, system and communication protection, awareness and training, identification authentication, physical and environmental protection, system information integrity, security assessment and authorization, incident response, risk assessment, planning and maintenance.

Section 6. Notice

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

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

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

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

Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

This question is related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

SORN NOTICE 13VA047, INDIVIDUALS SUBMITTING INVOICES-VOUCHERS FOR PAYMENT AND ACCOUNTING TRANSACTIONAL DATA PROVIDES NOTICE OF INFORMATION AND DATA USE OF INFORMATION. THIS SORN IS UNDER REVISION AND HAS BEEN CONCURRED ON BY OFFICE OF GENERAL COUNSEL, OFFICE OF CONGRESSIONAL AFFAIRS, PRIVACY SERVICE AND IFAMS AUTHORIZING OFFICIAL. IT IS WAITING ON CHIEF INFORMATION OFFICER APPROVAL IN ORDER TO MOVE OUTSIDE THE AGENCY. SORN PACKAGE DOCUMENTS ARE WITHIN THE APPENDIX OF THIS DOCUMENT.

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.
iFAMS does not collect directly from the individual. There is no ability for an individual to decline to provide information.

6.3 Do individuals have the right to consent to 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

iFAMS collects directly from the individual. There is no ability for an individual to decline to provide information.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?

This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use

Follow the format below:

Privacy Risk: There is a risk that individuals who provide information to the VA interfacing application will not know how their information is being shared and used internal to the Department of Veterans Affairs.

Mitigation: PIA and SORN corresponding to the legacy system FMS for which iFAMS will comply with serves to a notification for use.
Section 7. Access, Redress, and Correction

The following questions are directed at an individual’s ability to ensure the accuracy of the information collected about him or her.

7.1 What are the procedures that allow individuals to gain access to their information?

Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency’s FOIA/Privacy Act practices, but may also include additional access provisions. For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency’s procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.

If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR).

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

This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

SORN notice 13VA047, Individuals Submitting Invoices-Vouchers for Payment and Accounting Transactional Data, details the processes and procedures behind requesting and retrieving Privacy Act covered records. An individual wanting notification or access, including contesting the record, should mail or deliver a request to the office identified in the SORN. If an individual does not know the “office concerned,” the request may be addressed to the following with below requirements:

- PO or FOIA/PO of any VA field station or the Department of Veterans Affairs Central Office, 810 Vermont Avenue, NW, Washington, DC 20420.
- The receiving office must promptly forward the mail request received to the office of jurisdiction clearly identifying it as “Privacy Act Request” and notify the requester of the referral. Approved VA authorization forms may be provided to individuals for use.

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.
SORN notice 13VA047, Individuals Submitting Invoices-Vouchers for Payment and Accounting Transactional Data, details the processes and procedures behind correcting and contesting inaccurate or erroneous information. An individual may request amendment of a record pertaining to him or her contained in a specific VA system of records by mailing or delivering the request to the office concerned. The request must be in writing and must conform to the following requirements:

- It must state the nature of the information in the record the individual believes to be inaccurate, irrelevant, untimely, or incomplete; why the record should be changed; and the amendment desired. The requester must be advised of the title and address of the VA official who can assist in preparing the request to amend the record if assistance is desired.
- Not later than business 10 days after the date of a request to amend a record, the VA official concerned will acknowledge in writing such receipt. If a determination for correction or amendment has not been made, the acknowledgement will inform the individual of when to expect information regarding the action taken on the request. VA will complete a review of the request to amend or correct a record within 30 business days of the date of receipt.

Where VA agrees with the individual’s request to amend his or her record(s), the requirements of 5 U.S.C. § 552a(d) will be followed. The record(s) will be corrected promptly, and the individual will be advised promptly of the correction.

If the record has previously been disclosed to any person or agency, and an accounting of the disclosure was made, prior recipients of the record will be informed of the correction. An approved VA notification of amendment form letter may be used for this purpose.

An individual wanting notification or access, including contesting the record, should mail or deliver a request to the Privacy Office or FOIA/Privacy Office of any VA field station or the Department of Veterans Affairs Central Office, 810 Vermont Avenue, NW, Washington, DC 20420.

### 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.*

SORN notice 13VA047, Individuals Submitting Invoices-Vouchers for Payment and Accounting Transactional Data, details the processes and procedures behind correcting and contesting inaccurate or erroneous information. An individual may request amendment of a record pertaining to him or her contained in a specific VA system of records by mailing or delivering the request to the office concerned.
NOTIFICATION PROCEDURES: Notification for correcting the information will be accomplished by informing the individual to whom the record pertains by mail. The individual making the amendment must be advised in writing that the record has been amended and provided with a copy of the amended record. System Manager for the concerned VA system of records, Privacy Officer, or their designee, will notify the relevant persons or organizations who had previously received the record about the amendment.

If 38 U.S.C. § 7332-protected information was amended, the individual must provide written authorization to allow the sharing of the amendment with relevant persons or organizations request to amend a record must be acknowledged in writing within 10 workdays of receipt. If a determination has not been made within this time, the System Manager for the concerned VA system of records or designee, and/or the facility Privacy Officer, or designee, must advise the individual when the facility expects to notify the individual of the action taken on the request. The review must be completed as soon as possible, in most cases within 30 workdays from receipt of the request. If the anticipated completion date indicated in the acknowledgment cannot be met, the individual must be advised, in writing, of the reasons for the delay and the date action is expected to be completed. The delay may not exceed 90 calendar days from receipt of the request.

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 by other processes specific to a program, system, or group of systems.

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

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

If the individual discovers that incorrect information was provided during intake, they simply follow the same contact procedures as before, and state that the documentation they are now providing supersedes that previously provided.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department’s access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program’s effectiveness because the individuals involved might change their behavior.

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

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

Principle of Individual Participation: Is there a mechanism by which an individual can 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: Because there is no direct way for individuals to review or correct their information within iFAMS, there is a risk that the system may use inaccurate data when creating reports.

Mitigation: iFAMS system configuration encompasses an Enterprise Service Bus that will orchestrate the migration, analysis, and cleansing of the data before it is transmitted from an interfacing system to iFAMS.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system, and are they documented?

Describe the process by which an individual receives access to the system.

Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

Describe the different roles in general terms that have been created to provide access to the system. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.

An individual is provided access to the system by their system administrator within their organization. Each organization has their own criteria; however, access control to PII is determined by system security roles and responsibilities created in system configuration and determined and assigned by programmatic offices. Through the assigned security roles individuals will only have access to information that they have been designated “need to know.” Additionally, programmatic offices/administrations/facilities will only have access to their assigned locations and other locations are segregated by firewall configuration. These safeguards are in place to control access.
Additionally, iFAMS has robotic monitoring tools connecting to the system to manage and track security anomalies. iFAMs data is covered under the notice 13VA047, Individuals Submitting Invoices-Vouchers for Payment and Accounting Transactional Data. Its system of records comprises of financial, accounting, benefit and, transactional data across the VA enterprise nationwide. Use case constitutes VA meeting financial management objectives for veterans, veteran health providers, and dependents. 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 any access is granted, this request must be approved by the supervisor, Information Security Officer (ISO), and OIT.

Privacy and Information Security Awareness and Rules of Behavior (Talent Management System 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 monitored for compliance:
VA 10203: Privacy and HIPAA Training
VA 3812493: Annual Government Ethics

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.

Yes, contractors will have access to the information within iFAMS and through the contracting process, contractors are required to sign non-disclosure agreements. Contractors are working on the engineering, architecture, configuration, management of the environment, and will monitor the system for performance and security anomalies. Contractors are required to have corresponding clearances at the level and access appropriate. Contractors need to access PII is determined by the business need and the need to know. Contractors will be granted access to iFAMS if their VA manager and Privacy Officer approval. A contracting systems engineer does not have the same level or access to data as a contracted data analyst working to study legacy system data and cleansing data.
8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately. This question is related to privacy control AR-5, Privacy Awareness and Training.

iFAMS follow agency protocols. In accordance with VA Directives 6500 and 6502, VA personnel and/or any individual that has access to the network must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. Rules are included as part of the VA Privacy and Security Awareness training which all personnel must complete via the VA’s Talent Management System (TMS). After the user’s initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system.

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

If yes, provide:

1. The Security Plan Status,
2. The Security Plan Status Date,
3. The Authorization Status,
4. The Authorization Date,
5. The Authorization Termination Date,
6. The Risk Review Completion Date,
7. The FIPS 199 classification of the system (LOW/MODERATE/HIGH).

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

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

1. The Security Plan Status - Approved
2. The Security Plan Status Date – 22nd June 2022
3. The Authorization Status – Authorization to Operate (ATO)
4. The Authorization Date - 22nd July 2021
5. The Authorization Termination Date, NA – 21st July 2024
6. The Risk Review Completion Date - 15th July 2021
7. The FIPS 199 classification of the system is HIGH.
Section 9 – Technology Usage

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

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

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

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

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

iFAMS utilizes the VA Enterprise Cloud (VAEC).

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

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

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.
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.

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).
### Section 10. References

**Summary of Privacy Controls by Family**

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

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

PRINCESS MILLER
Digitally signed by PRINCESS MILLER
Date: 2022.09.01 07:07:40 -05'00'

Privacy Officer, Princess Miller

RITO-ANTHONY BRISBANE
Digitally signed by RITO-ANTHONY BRISBANE
Date: 2022.08.24 19:59:37 -05'00'

Information System Security Officer, Rito-Anthony B. Brisbane

JONATHAN LINDOW
Digitally signed by JONATHAN LINDOW
Date: 2022.08.24 08:37:12 -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).

DEPARTMENT OF VETERANS AFFAIRS

PRIVACY ACT OF 1974; SYSTEM OF RECORDS

AGENCY: Department of Veterans Affairs (VA), Office of Information of Technology

ACTION: Notice of Modified System of Records

SUMMARY: Individuals Submitting Invoices-Vouchers for Payment and Accounting Transactional Data-VA is a compilation of records received, controlled, managed, and employed for payment processing; general accounting; benefit payment distribution to veterans and their families; commercial vendor invoices for contract and reimbursement expenditures; and payroll payments.

DATES: Comments on this modified system of records must be received no later than 30 days after date of publication in the Federal Register. If no public comment is received during the period allowed for comment or unless otherwise published in the Federal Register by VA, the modified system of records will become effective a minimum of 30 days after date of publication in the Federal Register. If VA receives public comments, VA shall review the comments to determine whether any changes to the notice are necessary.

ADDRESSES: Written comments may be submitted through www.Regulation.gov; by mail or hand-delivery to Director, Regulation Policy and Management (00REG), Department of Veterans Affairs, 810 Vermont Ave. NW, Room 1064, Washington, DC 20420; or by fax to (202) 273-9026 (not a toll-free number). Comments should indicate that they are submitted in response to 13-VA047 Individuals Submitting Invoices-Vouchers for Payment and Accounting Transactional Data-VA. Copies of comments received will be available for public inspection in the Office of Regulation Policy and Management, Room 1063B, between the hours of 8:00 a.m. and 4:30 p.m., Monday through Friday (except holidays). Please call (202) 461 4902 for an appointment. (This is not a toll-free number.) In addition, comments may be viewed online at www.Regulations.gov.

FOR FURTHER INFORMATION CONTACT: Tammy Watson, Tammy.Watson@va.gov, (202) 461-6126,
SUPPLEMENTARY INFORMATION: Individuals Submitting Invoices-Vouchers for Payment and Accounting Transactional Data-VA is a VA-wide financial management system of records utilized in VA’s IT accounting systems for payment of benefits, vendor payments, invoice payment processing, and payroll purposes. Information is collected from recipients, vendors, VA administrations, medical centers, and other Federal entities for rendering payment.


Additional Routine Uses were added based on revised guidelines to A-108 and updated standards for agency breach notification. Moreover, VA must be able to provide its own initiative information that pertains to a violation of laws to law enforcement authorities for them to investigate and enforce those laws. Under 38 U.S.C. § 5701(a) and (f), VA may only disclose the names and addresses of veterans and their dependents to Federal entities with law enforcement responsibilities. This is distinct from the authority to disclose records in response to a qualifying request from a law enforcement entity, as authorized by Privacy Act subsection 5 U.S.C. § 552a(b)(7). VA will administer financial and transactional information through benefit disbursement consuming HIPPA related data thus amending the routine uses to include: 14. Federal Agencies, Hospitals, for Referral by VA.; 15. Non-VA Doc, for Referral to VA; 18. Researchers, for Research; 25. Claims Representatives; and 26. Third Party, for Benefit or Discharge. Location of the system of records is a notable change to being stored, managed, and secured within a momentum cloud application. Numerical order of routine uses from original SORN listing to revised version is amended to the below agency standardized format including the first ten routine uses:

1. Congress.
2. Data breach response and remedial efforts.
3. Data breach response and remedial efforts with another Federal agency.
4. Law Enforcement.
5. Litigation.
6. Contractors.
7. EEOC.
8. FLRA.
9. MSPB.
10. NARA & GSA.

Congress. VA may disclose information from the record of an individual in response to an inquiry from the congressional office made at the request of that individual. VA must be able to provide information about individuals to adequately respond to inquiries from Members of Congress at the request of constituents who have sought their assistance.

Justification – VA established standardized Routine Use. Disclosures may be made to a congressional office from the record of an individual in response to an inquiry from the
congressional office made at the request of the individual to whom the record pertains. The 
disclosure must be within the scope of the individual’s request and release of individually 
identifiable treatment records relating to alcohol, drug abuse, sickle cell anemia, or human 
immunodeficiency virus/AIDS must be specifically addressed in the individual’s request to 
the congressional office for assistance. In those cases, however, where the congressional 
quiry indicates that the request is being made on behalf of a person other than the 
individual whose record is to be disclosed, the congressional office should be advised that 
the written consent of the subject of the record is required. The Privacy Act limitation on 
disclosure of personal information contained in any VA system of records shall not apply to 
any Chairman/Head of a committee in the House of Representatives or the United States 
Senate Veterans’ Affairs or Appropriations Committees (including the Subcommittees on 
VA, HUD, and Independent Agencies) if an official request for the disclosure has been 
made for an oversight purpose on a matter within the jurisdiction of the Committee or 
Subcommittee. Use case -- Use of information is necessary and proper to ensure the 
veteran and whom they entrust and deem necessarily have access to advocate on their behalf.

Data breach response and remedial efforts. VA may, on its own initiative, disclose 
information from this system to appropriate agencies, entities, and persons when (1) VA 
suspects or has confirmed that there has been a breach of the system of records; (2) the 
Department has determined that as a result of the suspected or confirmed compromise 
there is a risk of harm to individuals, the Department (including its information systems, 
programs, and operations), the Federal Government, or national security; and (3) the 
disclosure is to agencies, entities, or persons whom VA determines are reasonably 
necessary to assist or carry out the Department’s efforts to respond to the suspected or 
confirmed compromise and prevent, minimize, or remedy such harm. Justification – VA 
established standardized Routine Use. This routine use permits disclosures by the 
Department to respond to a suspected or confirmed data breach, including the conduct of 
any risk analysis or provision of credit protection services as provided in 38 U.S.C. § 5724 
and, in accordance with Veterans Benefits, Health Care, and Information Technology Act of 
2006 §§ 5723 – 5724. VA may notify officials other than officials within the Department of 
data breaches when required. In the instance of 20 or more individuals affected, VA may 
provide notice to Director of Office of Management and Budget and other such Federal 
entities as determined relevant through quantitative and qualitative risk analyses whether 
independent or internal on a confirmed data breach. Specifically, VA may authorize an 
independent risk analysis by a non-VA entity and/or Office of Inspector General in cases 
involving PII and/or PHI. Findings of such risk analysis may endorse and invoke 
provisioning of credit monitoring for all those affected. Use Case - Use of information is 
necessary and proper to mitigate the effect of a confirmed data breach through provisioning 
credit monitoring. Notification of non-federal entities in compliance and risk assessment 
capacity to perform prevention strategies.

Data breach response and remedial efforts with another Federal agency. VA may, on its 
own initiative, disclose information from this system to another Federal agency or Federal 
entity, when VA determines that information from this system of records is reasonably 
necessary to assist the recipient agency or entity in (1) responding to a suspected or 
confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, 
the recipient agency or entity (including its information systems, programs, and operations),
the Federal Government, or national security, resulting from a suspected or confirmed breach. Justification – VA established standardized Routine Use: In accordance with U.S.C 38§ 5723, (7) VA will ensure that the Assistant Secretary for Information and Technology, in coordination with the Under Secretaries, Assistant Secretaries, and other key officials of the Department report to Congress, the Office of Management and Budget, and other entities as required by law and this section of the regulation to cooperate with notify and cooperate with officials other than officials of the Department of data breaches when required. Use Case - Use of information is necessary and proper to initiate investigations into confirmed data breaches involving other executive branch agencies.

Law Enforcement. VA may, on its own initiative, disclose information in this system, except the names and home addresses of veterans and their dependents, which is relevant to a suspected or reasonably imminent violation of law, whether civil, criminal or regulatory in nature and whether arising by general or program statute or by regulation, rule or order issued pursuant thereto, to a Federal, State, local, Tribal, or foreign agency charged with the responsibility of investigating or prosecuting such violation, or charged with enforcing or implementing the statute, regulation, rule or order. Justification – VA established standardized Routine Use: VA may also disclose the names and addresses of veterans and their dependents to a federal agency charged with the responsibility of investigating or prosecuting civil, criminal or regulatory violations of law, or charged with enforcing or implementing the statute, regulation, rule or order. Use Case - Use of information is necessary and proper to cooperate with other federal agencies while prosecuting civil, criminal or regulatory violations of law. Litigation. VA may disclose information from this system of records to the Department of Justice (DoJ), either on VA’s initiative or in response to DoJ’s request for the information, after either VA or DoJ determines that such information is relevant to DoJ’s representation of the United States or any of its components in legal proceedings before a court or adjudicative body, provided that, in each case, the agency also determines prior to disclosure that release of the records to the DoJ is a use of the information contained in the records that is compatible with the purpose for which VA collected the records. Justification – VA established standardized Routine Use: VA, on its own initiative, may disclose records in this system of records in legal proceedings before a court or administrative body after determining that the disclosure of the records to the court or administrative body is a use of the information contained in the records that is compatible with the purpose for which VA collected the records. Use Case - Use of information is necessary and proper to disclose records in this system of records in legal proceedings before a court or administrative body.

Contractors. VA may disclose information from this system of records to individuals, organizations, private or public agencies, or other entities or individuals with whom VA has a contract or agreement to perform such services as VA may deem practicable for the purposes of laws administered by VA, for the contractor, subcontractor, public or private agency, or other entity or individual with whom VA has a contract or agreement to perform services under the contract or agreement. This routine use includes disclosures by an individual or entity performing services for VA to any secondary entity or individual to perform an activity that is necessary for individuals, organizations, private or public agencies, or other entities or individuals with whom VA has a contract or agreement to provide the service to VA. This routine use also applies to agreements that do not qualify as contracts defined by Federal procurement laws and regulations. Justification – VA established standardized Routine Use: VA may disclose information from this system of
records to individuals, organizations private or public agencies, or other entities or individuals with whom VA has a contract or agreement to perform such services on behalf of VA acting in such capacity as an agent of VA on a need-to-know basis. Use Case - Use of information is necessary and proper to disclose records from this system of records for entities contracted, entered into an agreement, and performing duties on behalf of VA.

EEOC. VA may disclose information from this system to the Equal Employment Opportunity Commission (EEOC) when requested in connection with investigations of alleged or possible discriminatory practices, examination of Federal affirmative employment programs, or other functions of the Commission as authorized by law or regulation. Justification – VA established standardized Routine Use: VA must be able to provide information to EEOC to assist it in fulfilling its duties to protect employees’ rights, as required by statute and regulation. Use Case - Use of information is necessary and proper to disclose records from this system of records to protect VA employee rights.

FLRA. VA may disclose information from this system to the Federal Labor Relations Authority (FLRA), including its General Counsel, information related to the establishment of jurisdiction, investigation, and resolution of allegations of unfair labor practices, or in connection with the resolution of exceptions to arbitration awards when a question of material fact is raised; for it to address matters properly before the Federal Services Impasses Panel, investigate representation petitions, and conduct or supervise representation elections. Justification – VA established standardized Routine Use: VA must be able to provide information to FLRA to comply with the statutory mandate under which it operates. Use Case - Use of information is necessary and proper to cooperate in labor relation investigations.

MSPB. VA may disclose information from this system to the Merit Systems Protection Board (MSPB), or the Office of the Special Counsel, when requested in connection with appeals, special studies of the civil service and other merit systems, review of rules and regulations, investigation of alleged or possible prohibited personnel practices, and such other functions promulgated in 5 U.S.C. §§ 1205 and 1206, or as authorized by law. Justification – VA established standardized Routine Use: VA must be able to provide information to MSPB to assist it in fulfilling its duties as required by statute and regulation. Use Case - Use of information is necessary and proper to cooperate with Merit Systems Protection Board and/or Office of Special Counsel concerning allegations of prohibited personnel practices.

Disclosure may be made to a congressional office from the record of an individual in response to an inquiry from the congressional office made at the request of that individual. Disclosure may be made to NARA (National Archives and Records Administration) GSA (General Services Administration) in records management inspections conducted under authority of 44 U.S.C. 2904 and 2906. (In present SORN and will not Change)

Transfer payment information necessary to complete payment of claims and to furnish income data Form 1099 to the Treasury Department to effect payment of claims to vendors and to furnish income information. (In present SORN and will not Change)
In the event that a system of records maintained by this agency to carry out its functions indicates a violation or potential violation of law, whether civil, criminal or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule or order issued pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the appropriate agency, whether Federal, State, local or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, or rule, regulation or order issued pursuant thereto. (Deleted and replaced with more up to date)

A record from this system of records may be disclosed as a ‘routine use’ to a Federal, State or local agency or to a non-governmental organization maintaining civil, criminal or other relevant information, such as current licenses, registration or certification, if necessary to obtain information relevant to an agency decision concerning the hiring or retention of an employee, the use of an individual as a consultant, attending or to provide fee basis health care, the issuance of a security clearance, the leting of a contract, or the issuance of a license, grant or other benefits. These records may also be disclosed as part of an ongoing computer matching program to accomplish these purposes. (Deleted and updated by – In Original SORN – Deleted or Replaced by updated Routine Use detailed below)

A record from this system of records may be disclosed to a Federal, State or local agency, in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the leting of a contract, or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency’s decision on the matter. (Deleted and updated by – In Original SORN – Deleted or Replaced by updated Routine Use detailed below)

Relevant information from this system of records, including the nature and amount of financial obligation, may be disclosed as a routine use, to assist the Veterans Administration in the collection of unpaid financial obligations owed the VA, to a debtor’s employing agency or commanding officer so that the debtor-employee may be counseled by his or her federal employer or commanding officer. This purpose is consistent with 5 U.S.C. 5514, 4 CFR 102.5, and section 206 of Executive Order 11222 of May 8, 1965 (30 FR 6469). (Deleted and updated by – In Original SORN – Deleted or Replaced by updated Routine Use detailed below)

Relevant information from this system of records, including available identifying data regarding the debtor, such as name of debtor, last known address of debtor, name of debtor’s spouse, social security account number of debtor, VA insurance number, VA loan number, VA claim number, place of birth and date of birth of debtor, name and address of debtor’s employer or firm and dates of employment, may be disclosed to other Federal agencies, State probate courts, State driver’s license bureaus, and State automobile title and license bureaus as a routine use in order to obtain current address, locator and credit report assistance in the collection of unpaid financial obligations owed the U.S. This purpose is consistent with the Federal Claims Collection Act of 1966 (Pub.L. 89-508, 31
U.S.C. 951-953) and 4 CFR parts 101-105. (Deleted and updated by – In Original SORN – Deleted or Replaced by updated Routine Use detailed below)

Records from this system of records may be disclosed to a Federal Agency or to a State or local government licensing board and/or to the Federation of State Medical Boards or a similar nongovernment entity which maintains records concerning individuals’ employment histories or concerning the issuance, retention or revocation of licenses, certifications, or registration necessary to practice an occupation, profession or specialty, in order for the Agency to obtain information relevant to an Agency decision concerning the hiring, retention or termination of an employee or to inform a Federal Agency or licensing boards or the appropriate nongovernment entities about the health care practices of a terminated, resigned or retired health care employee whose professional health care activity so significantly failed to conform to generally accepted standards of professional medical practice as to raise reasonable concern for the health and safety of patients in the private sector or from another Federal Agency. These records may also be disclosed as part of an ongoing computer matching program to accomplish these purposes. (Deleted and updated by – In Original SORN – Deleted or Replaced by updated Routine Use detailed below)

Relevant information (excluding medical treatment information related to drug or alcohol abuse, infection with the human immunodeficiency virus or sickle cell anemia) may be disclosed to the Department of Health and Human Services (HHS) for the purpose of identifying improper duplicate payments made by Medicare fiscal intermediaries where VA authorized and was responsible for payment for medical services obtained at non-VA health care facilities. The purpose of the review is for HHS to identify duplicate payments and initiate recovery of identified overpayments and, where warranted, initiate fraud investigations, or, to seek reimbursement from VA for those services which were authorized by VA and for which no payment, or partial payment, was made by VA. HHS will provide information to identify the patient to include the patient name, address, Social Security number, date of birth, and information related to the period of medical treatment for which payment was made by Medicare to include the name and address of the hospital, the admission and discharge dates, the services for which payment was made, and the dates and amounts of payment. Information disclosed from this system of records will be limited to that information that is necessary to confirm or disprove an inappropriate payment by Medicare. These records may also be disclosed as part of an ongoing computer matching program to accomplish these purposes. (Deleted and updated by – In Original SORN – Deleted or Replaced by updated Routine Use detailed below)

Identifying information in this system, including name, address, social security number and other information as is reasonably necessary to identify such individual, may be disclosed to the National Practitioner Data Bank at the time of hiring and/or clinical privileging/deprivileging of health care practitioners, and other times as deemed necessary by VA, in order for VA to obtain information relevant to a Department decision concerning the hiring, privileging/deprivileging, retention or termination of the applicant or employee. (Deleted and updated by – In Original SORN – Deleted or Replaced by updated Routine Use detailed below)

Relevant information from this system of records may be disclosed to the National Practitioner Data Bank and/or State Licensing Board in the State(s) in which a practitioner is
licensed, in which the VA facility is located, and/or in which an act or omission occurred upon which a medical malpractice claim was based when VA reports information concerning: (1) Any payment for the benefit of a physician, dentist, or other licensed health care practitioner which was made as the result of a settlement or judgment of a claim of medical malpractice if an appropriate determination is made in accordance with agency policy that payment was related to substandard care, professional incompetence or professional misconduct on the part of the individual; (2) a final decision which relates to possible incompetence or improper professional conduct that adversely affects the clinical privileges of a physician or dentist for a period longer than 30 days; or, (3) the acceptance of the surrender of clinical privileges or any restriction of such privileges by a physician or dentist either while under investigation by the health care entity relating to possible incompetence or improper professional conduct, or in return for not conducting such an investigation or proceeding. These records may also be disclosed as part of a computer matching program to accomplish these purposes. (Deleted and updated by – In Original SORN – Deleted or Replaced by updated Routine Use detailed below)

Federal Agencies, for Computer Matches. VA may disclose identifying information, including social security number, concerning veterans, spouses of veterans, and the beneficiaries of veterans to other federal agencies for the purpose of conducting computer matches to obtain information to determine or verify eligibility of veterans receiving VA medical care under Title 38, U.S.C. Office Enterprise Integration (OEI) may disclose limited individual identification information to another Federal agency for the purpose of matching and acquiring information held by that agency for OPP to use for the purposes stated for this system of records. Justification – VA established standardized Routine Use: VA must be able to provide limited personally identifiable information to other federal agencies for computer matching activities for the purpose of benefit payments to veterans and beneficiaries. Use Case - Use of information is necessary and proper to conduct computer matching activities with regards to payments and verification of VA payment if VA is considered a Source Agency. (New Routine Use)

Federal Agencies, for Litigation. VA may, on its own initiative, disclose information to another federal agency, court, or party in litigation before a court or other administrative proceeding conducted by an agency, if VA is a party to the proceeding and needs to disclose the information to protect its interests. Justification – VA established standardized Routine Use: VA, on its own initiative, may disclose records in this system of records in legal proceedings another federal agency, court, or party in litigation before a court or other administrative proceeding conducted by an agency if VA is a party to the proceeding and needs to disclose the information to protect its interests. Use Case - Use of information is necessary and proper to disclose records in this system of records in legal proceedings before a court or administrative body. (New Routine Use)

Federal Agencies, Hospitals, for Referral by VA. VA may disclose relevant health care information to: (1) a federal agency or non-VA health care provider or institution when VA refers a patient for hospital or nursing home care or medical services, or authorizes a patient to obtain non-VA medical services and the information is needed by the federal agency or non-VA institution on provider to perform the services; or (2) a federal agency or to a non-VA hospital (federal, state, and local public or private) or other medical installation having hospital facilities, organ banks, blood banks, or similar institutions, medical schools
or clinics, or other groups or individuals that have contracted or agreed to provide medical services or share the use of medical resources under the provisions of 38 U.S.C. §§ 513, 7409, 8111, or 8153, when treatment is rendered by VA under the terms of such contract or agreement or the issuance of an authorization, and the information is needed for purposes of medical treatment and/or follow-up, determining entitlement to a benefit, or for VA to effect recovery of the costs of the medical care. Justification – VA established standardized Routine Use: VA must be able to provide patient referral information for authorized hospital and/or nursing home care to a non-VA medical services provider for recovery of the costs of the medical care. Use Case - Use of information is necessary and proper as data within this system does not exclusively include financial, transactional, and benefit payout data it also includes VHA PHI information that is funneled in by VISTA. (New Routine Use)

Federal Agencies, for Recovery of Medical Care Costs. VA may disclose patient identifying information to federal agencies and VA and government-wide third-party insurers responsible for payment of the cost of medical care for the identified patients, for VA to seek recovery of the costs of the medical care. These records may also be disclosed as part of a computer matching program to accomplish this purpose. Justification – Use of information is necessary and proper as data within this system does not exclusively include financial, transactional, and benefit payout data it also includes VHA PHI information that is funneled in by VISTA. (New Routine Use) Use Case - Use of information is necessary and proper as data within this system does not exclusively include financial, transactional, and benefit payout data it also includes VHA PHI information that is funneled in by VISTA. (New Routine Use)

Researchers, for Research. VA may disclose information from this system, except the names and home addresses of veterans and their dependents (unless name and address is furnished by the requester), for research purposes determined to be necessary and proper, to epidemiological and other research facilities approved by the Under Secretary for Health. Justification -- The data within this system does not just include financial, transactional, and benefit payout data it also includes VHA PHI information that is funneled in by VISTA. Use Case - Use of information is necessary and proper as data within this system does not exclusively include financial, transactional, and benefit payout data it also includes VHA PHI information that is funneled in by VISTA. (New Routine Use)

Treasury, IRS. VA may disclose the name of a veteran or beneficiary, other information as is reasonably necessary to identify such individual, and any other information concerning the individual's indebtedness by virtue of a person's participation in a benefits program administered by VA, may be disclosed to the Department of the Treasury, Internal Revenue Service, for the collection of Title 38 benefit overpayments, overdue indebtedness, and/or costs of services provided to an individual not entitled to such services, by the withholding of all or a portion of the person's Federal income tax refund. The purpose of this disclosure is to collect a debt owed the VA by an individual by offset of his or her Federal income tax refund. Justification – VA established standardized Routine Use: VA must be able to provide information to MSPB to assist it in fulfilling its duties as required by statute and
regulation. Use Case - Use of information is necessary and proper to cooperate with Merit Systems Protection Board and/or Office of Special Counsel concerning allegations of prohibited personnel practices. (New Routine Use)

Treasury, to Report Waived Debt as Income. VA may disclose an individual's name, address, social security number, and the amount (excluding interest) of any indebtedness which is waived under 38 U.S.C. § 3102, compromised under 4 C.F.R. Part 103, otherwise forgiven, or for which the applicable statute of limitations for enforcing collection has expired, to the Department of the Treasury, Internal Revenue Service, as a report of income under 26 U.S.C. § 61(a)(12). Justification – VA established standardized Routine Use: VA must be able to provide information to MSPB to assist it in fulfilling its duties as required by statute and regulation. Use Case - Use of information is necessary and proper to cooperate with Merit Systems Protection Board and/or Office of Special Counsel concerning allegations of prohibited personnel practices. (New Routine Use)

Treasury, for Payment or Reimbursement. VA may disclose information to the Department of the Treasury to facilitate payments to physicians, clinics, and pharmacies for reimbursement of services rendered, and to veterans for reimbursements of authorized expenses, or to collect, by set off or otherwise, debts owed the United States. Justification – VA established standardized Routine Use: VA must be able to provide information to MSPB to assist it in fulfilling its duties as required by statute and regulation. Use Case - Use of information is necessary and proper to cooperate with Merit Systems Protection Board and/or Office of Special Counsel concerning allegations of prohibited personnel practices. (New Routine Use)

Guardians Ad Litem, for Representation. VA may disclose information to a fiduciary or guardian ad litem in relation to his or her representation of a claimant in any legal proceeding, but only to the extent necessary to fulfill the duties of the fiduciary or guardian ad litem. This disclosure permits VA to provide individual information to an appointed VA Federal fiduciary or to the individual’s guardian ad litem that is needed to fulfill appointed duties. Justification – VA established standardized Routine Use: VA must be able to provide information to MSPB to assist it in fulfilling its duties as required by statute and regulation. Use Case - Use of information is necessary and proper to cooperate with Merit Systems Protection Board and/or Office of Special Counsel concerning allegations of prohibited personnel practices. (New Routine Use)

Guardians, for Incompetent Veterans. VA may disclose relevant information from this system of records while presenting evidence to a court, magistrate, or administrative tribunal; in matters of guardianship, inquests, and commitments; to private attorneys representing veterans rated incompetent in conjunction with issuance of Certificates of Incompetency; and to probation and parole officers in connection with court-required duties. Justification – VA established standardized Routine Use: VA must be able to provide information to MSPB to assist it in fulfilling its duties as required by statute and regulation. Use Case - Use of information is necessary and proper to cooperate with Merit Systems Protection Board and/or Office of Special Counsel concerning allegations of prohibited personnel practices. (New Routine Use)
Claims Representatives. VA may disclose information from this system of records relevant to a claim of a veteran or beneficiary, such as the name, address, the basis and nature of a claim, amount of benefit payment information, medical information, and military service and active duty separation information, at the request of the claimant to accredited service organizations, VA-approved claim agents, and attorneys acting under a declaration of representation, so that these individuals can aid claimants in the preparation, presentation, and prosecution of claims under the laws administered by VA. The name and address of a claimant will not, however, be disclosed to these individuals under this routine use if the claimant has not requested the assistance of an accredited service organization, claims agent or an attorney. VA must be able to disclose this information to accredited service organizations, VA-approved claim agents, and attorneys representing veterans so they can assist veterans by preparing, presenting, and prosecuting claims under the laws administered by VA. Justification – VA established standardized Routine Use: VA must be able to provide information to MSPB to assist it in fulfilling its duties as required by statute and regulation. Use Case - Use of information is necessary and proper to cooperate with Merit Systems Protection Board and/or Office of Special Counsel concerning allegations of prohibited personnel practices. (New Routine Use)

Third Party, for Benefit or Discharge. Health care information concerning a non-judicially declared incompetent patient may be disclosed to a third party upon the written authorization of the patient's next of kin for the patient, or, consistent with the best interest of the patient, a member of the patient's family, to receive a benefit to which the patient or family member is entitled, or, to arrange for the patient's discharge from a VA medical facility. Sufficient data to make an informed determination will be made available to such next of kin. If the patient's next of kin are not reasonably accessible, the Chief of Staff, Director, or designee of the custodial VA medical facility may disclose health information for these purposes. Justification – VA established standardized Routine Use: VA must be able to provide information to MSPB to assist it in fulfilling its duties as required by statute and regulation. Use Case - Use of information is necessary and proper to cooperate with Merit Systems Protection Board and/or Office of Special Counsel concerning allegations of prohibited personnel practices. (New Routine Use)

Signing Authority

The Senior Agency Official Privacy, or designee, approved this document and authorized the undersigned to sign and submit the document to the Office of the Federal Register for publication electronically as an official document of the Department of Veterans Affairs.
SYSTEM NAME: Individuals Submitting Invoices-Vouchers for Payment and Accounting Transactional Data-VA 13VA047

SECURITY CLASSIFICATION: The information in this system is unclassified.

SYSTEM LOCATION: VA Data Processing Center, Austin, Texas and fiscal offices of Central Office; field stations where fiscal transactions are processed; and application server located in the VA managed enterprise service cloud enclave.

SYSTEM MANAGER(S): Tammy Watson, System Owner, VA Financial Services Center (FSC), Austin, TX 78741


PURPOSE(S) OF THE SYSTEM: Individuals Submitting Invoices-Vouchers for Payment and Accounting Transactional Data-VA is a VA-wide financial management system of records utilized in VA’s IT accounting systems for payment of benefits, vendor payments, invoice payment processing, and payroll purposes. Information is collected from recipients, vendors, VA administrations, medical centers, and other Federal entities for rendering payment.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Contractors, vendors, salaried employees, non-salaried employees, consultants, physicians and dentists, and patients and veterans.

CATEGORIES OF RECORDS IN THE SYSTEM: Commercial Vendor identification listings, invoiced payment records, claimant information, and banking and financial accounting information

RECORD SOURCE CATEGORIES: commercial vendors; individual or legal representative as part of an application for a benefit, contract or reimbursement; Data could potentially be obtained from a VA administration, facility and/or medical center; Department of Treasury; Internal Revenue Service; and other Federal entities.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

To the extent that records contained in the system include information protected by 45 CFR parts 160 and 164, i.e., individually identifiable health information, and 38 U.S.C. § 7332, i.e., medical treatment information related to drug abuse, alcoholism or alcohol abuse,
sickle cell anemia or infection with the human immunodeficiency virus, that information cannot be disclosed under a routine use unless there is also specific statutory authority in 38 U.S.C. § 7332 and regulatory authority in 45 CFR parts 160 and 164 permitting disclosure.

1. Congress. VA may disclose information from the record of an individual in response to an inquiry from the congressional office made at the request of that individual. VA must be able to provide information about individuals to adequately respond to inquiries from Members of Congress at the request of constituents who have sought their assistance.

2. Data breach response and remedial efforts. VA may, on its own initiative, disclose information from this system to appropriate agencies, entities, and persons when (1) VA suspects or has confirmed that there has been a breach of the system of records; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to individuals, the Department (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure is to agencies, entities, or persons whom VA determines are reasonably necessary to assist or carry out the Department’s efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm. This routine use permits disclosures by the Department to respond to a suspected or confirmed data breach, including the conduct of any risk analysis or provision of credit protection services as provided in 38 U.S.C. § 5724.

   a. Effective Response. A federal agency’s ability to respond quickly and effectively in the event of a breach of federal data is critical to its efforts to prevent or minimize any consequent harm. An effective response necessitates disclosure of information regarding the breach to those individuals affected by it, as well as to persons and entities in a position to cooperate, either by assisting in notification to affected individuals or playing a role in preventing or minimizing harms from the breach.

   b. Disclosure of Information. Often, the information to be disclosed to such persons and entities is maintained by federal agencies and is subject to the Privacy Act (5 U.S.C. § 552a). The Privacy Act prohibits the disclosure of any record in a system of records by any means of communication to any person or agency absent the written consent of the subject individual unless the disclosure falls within one of the twelve statutory exceptions. To ensure an agency is in the best position to respond in a timely and effective manner, in accordance with 5 U.S.C. § 552a(b)(3) of the Privacy Act, agencies should publish a routine use for appropriate systems specifically applying to the disclosure if information in connection with response and remedial efforts in the event of a data breach.

3. Data breach response and remedial efforts with another Federal agency. VA may, on its own initiative, disclose information from this system to another Federal agency or Federal entity, when VA determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations),
the Federal Government, or national security, resulting from a suspected or confirmed breach.

4. Law Enforcement. VA may, on its own initiative, disclose information in this system, except the names and home addresses of veterans and their dependents, which is relevant to a suspected or reasonably imminent violation of law, whether civil, criminal or regulatory in nature and whether arising by general or program statute or by regulation, rule or order issued pursuant thereto, to a Federal, State, local, Tribal, or foreign agency charged with the responsibility of investigating or prosecuting such violation, or charged with enforcing or implementing the statute, regulation, rule or order. On its own initiative, VA may also disclose the names and addresses of veterans and their dependents to a federal agency charged with the responsibility of investigating or prosecuting civil, criminal or regulatory violations of law, or charged with enforcing or implementing the statute, regulation, rule or order issued pursuant thereto.

5. Litigation. VA may disclose information from this system of records to the Department of Justice (DoJ), either on VA’s initiative or in response to DoJ’s request for the information, after either VA or DoJ determines that such information is relevant to DoJ’s representation of the United States or any of its components in legal proceedings before a court or adjudicative body, provided that, in each case, the agency also determines prior to disclosure that release of the records to the DoJ is a use of the information contained in the records that is compatible with the purpose for which VA collected the records. VA, on its own initiative, may disclose records in this system of records in legal proceedings before a court or administrative body after determining that the disclosure of the records to the court or administrative body is a use of the information contained in the records that is compatible with the purpose for which VA collected the records.

6. Contractors. VA may disclose information from this system of records to individuals, organizations, private or public agencies, or other entities or individuals with whom VA has a contract or agreement to perform such services as VA may deem practicable for the purposes of laws administered by VA, for the contractor, subcontractor, public or private agency, or other entity or individual with whom VA has a contract or agreement to perform services under the contract or agreement. This routine use includes disclosures by an individual or entity performing services for VA to any secondary entity or individual to perform an activity that is necessary for individuals, organizations, private or public agencies, or other entities or individuals with whom VA has a contract or agreement to provide the service to VA. This routine use also applies to agreements that do not qualify as contracts defined by Federal procurement laws and regulations.

7. EEOC. VA may disclose information from this system to the Equal Employment Opportunity Commission (EEOC) when requested in connection with investigations of alleged or possible discriminatory practices, examination of Federal affirmative employment programs, or other functions of the Commission as authorized by law or regulation. VA must be able to provide information to EEOC to assist it in fulfilling its duties to protect employees’ rights, as required by statute and regulation.
8. FLRA. VA may disclose information from this system to the Federal Labor Relations Authority (FLRA), including its General Counsel, information related to the establishment of jurisdiction, investigation, and resolution of allegations of unfair labor practices, or in connection with the resolution of exceptions to arbitration awards when a question of material fact is raised; for it to address matters properly before the Federal Services Impasses Panel, investigate representation petitions, and conduct or supervise representation elections. VA must be able to provide information to FLRA to comply with the statutory mandate under which it operates.

9. MSPB. VA may disclose information from this system to the Merit Systems Protection Board (MSPB), or the Office of the Special Counsel, when requested in connection with appeals, special studies of the civil service and other merit systems, review of rules and regulations, investigation of alleged or possible prohibited personnel practices, and such other functions promulgated in 5 U.S.C. §§ 1205 and 1206, or as authorized by law. VA must be able to provide information to MSPB to assist it in fulfilling its duties as required by statute and regulation.

10. NARA & GSA. VA may disclose information from this system to the National Archives and Records Administration (NARA) and General Services Administration (GSA) in records management inspections conducted under Title 44, U.S.C. NARA is responsible for archiving old records which are no longer actively used but may be appropriate for preservation, and for the physical maintenance of the Federal government's records. VA must be able to provide the records to NARA to determine the proper disposition of such records.

11. Federal Agencies, for Computer Matches. VA may disclose identifying information, including social security number, concerning veterans, spouses of veterans, and the beneficiaries of veterans to other federal agencies for the purpose of conducting computer matches to obtain information to determine or verify eligibility of veterans receiving VA medical care under Title 38, U.S.C. Office Enterprise Integration (OEI) may disclose limited individual identification information to another Federal agency for the purpose of matching and acquiring information held by that agency for OPP to use for the purposes stated for this system of records.

12. Federal Agencies, for Litigation. VA may, on its own initiative, disclose information to another federal agency, court, or party in litigation before a court or other administrative proceeding conducted by an agency, if VA is a party to the proceeding and needs to disclose the information to protect its interests.

13. Federal Agencies, Hospitals, for Referral by VA. VA may disclose relevant health care information to: (1) a federal agency or non-VA health care provider or institution when VA refers a patient for hospital or nursing home care or medical services, or authorizes a patient to obtain non-VA medical services and the information is needed by the federal agency or non-VA institution on provider to perform the services; or (2) a federal agency or to a non-VA hospital (federal, state, and local public or private) or other medical installation having hospital facilities, organ banks, blood banks, or similar institutions, medical schools or clinics, or other groups or individuals that have contracted or agreed to provide medical services or share the use of medical resources under the provisions of 38 U.S.C. §§ 513,
7409, 8111, or 8153, when treatment is rendered by VA under the terms of such contract or agreement or the issuance of an authorization, and the information is needed for purposes of medical treatment and/or follow-up, determining entitlement to a benefit, or for VA to effect recovery of the costs of the medical care.

14. Federal Agencies, for Recovery of Medical Care Costs. VA may disclose patient identifying information to federal agencies and VA and government-wide third-party insurers responsible for payment of the cost of medical care for the identified patients, for VA to seek recovery of the medical care costs. These records may also be disclosed as part of a computer matching program to accomplish this purpose.

15. Researchers, for Research. VA may disclose information from this system, except the names and home addresses of veterans and their dependents (unless name and address is furnished by the requester), for research purposes determined to be necessary and proper to epidemiological and other research facilities approved by the Under Secretary for Health.

16. Treasury, IRS. VA may disclose the name of a veteran or beneficiary, other information as is reasonably necessary to identify such individual, and any other information concerning the individual's indebtedness by virtue of a person's participation in a benefits program administered by VA, may be disclosed to the Department of the Treasury, Internal Revenue Service, for the collection of Title 38 benefit overpayments, overdue indebtedness, and/or costs of services provided to an individual not entitled to such services, by the withholding of all or a portion of the person's Federal income tax refund. The purpose of this disclosure is to collect a debt owed the VA by an individual by offset of his or her federal income tax refund.

17. Treasury, to Report Waived Debt as Income. VA may disclose an individual's name, address, social security number, and the amount (excluding interest) of any indebtedness which is waived under 38 U.S.C. § 3102, compromised under 4 C.F.R. Part 103, otherwise forgiven, or for which the applicable statute of limitations for enforcing collection has expired, to the Department of the Treasury, Internal Revenue Service, as a report of income under 26 U.S.C. § 61(a)(12).

18. Treasury, for Payment or Reimbursement. VA may disclose information to the Department of the Treasury to facilitate payments to physicians, clinics, and pharmacies for reimbursement of services rendered, and to veterans for reimbursements of authorized expenses, or to collect, by set off or otherwise, debts owed the United States.

19. Guardians Ad Litem, for Representation. VA may disclose information to a fiduciary or guardian ad litem in relation to his or her representation of a claimant in any legal proceeding, but only to the extent necessary to fulfill the duties of the fiduciary or guardian ad litem. This disclosure permits VA to provide individual information to an appointed VA Federal fiduciary or to the individual's guardian ad litem that is needed to fulfill appointed duties.

20. Guardians, for Incompetent Veterans. VA may disclose relevant information from this system of records while presenting evidence to a court, magistrate, or administrative tribunal; in matters of guardianship, inquests, and commitments; to private attorneys
representing veterans rated incompetent in conjunction with issuance of Certificates of Incompetency; and to probation and parole officers in connection with court-required duties.

21. Claims Representatives. VA may disclose information from this system of records relevant to a claim of a veteran or beneficiary, such as the name, address, the basis and nature of a claim, amount of benefit payment information, medical information, and military service and active duty separation information, at the request of the claimant to accredited service organizations, VA-approved claim agents, and attorneys acting under a declaration of representation, so that these individuals can aid claimants in the preparation, presentation, and prosecution of claims under the laws administered by VA. The name and address of a claimant will not, however, be disclosed to these individuals under this routine use if the claimant has not requested the assistance of an accredited service organization, claims agent or an attorney. VA must be able to disclose this information to accredited service organizations, VA-approved claim agents, and attorneys representing veterans so they can assist veterans by preparing, presenting, and prosecuting claims under the laws administered by VA.

22. Third Party, for Benefit or Discharge. Health care information concerning a non-judicially declared incompetent patient may be disclosed to a third party upon the written authorization of the patient’s next of kin in order for the patient, or, consistent with the best interest of the patient, a member of the patient’s family, to receive a benefit to which the patient or family member is entitled, or, to arrange for the patient’s discharge from a VA medical facility. Sufficient data to make an informed determination will be made available to such next of kin. If the patient’s next of kin are not reasonably accessible, the Chief of Staff, Director, or designee of the custodial VA medical facility may disclose health information for these purposes.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Records are stored electronically on a VA server, in paper folders, magnetic discs, magnetic tape, and in a momentum cloud application. Paper documents may be scanned/digitized and stored for viewing electronically.


POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Individuals Submitting Invoices-Vouchers for Payment and Accounting Transactional Data-VA system of records is retained as defined by its NARA approved Records Control Schedule, MP-4, Part X and within rules of the General Records Schedule (GRS). Unscheduled records within this System of Records are indefinitely retained within the rules GRS, ERA Number DAA-GRS-2013-005-002 (Permanent Retention). Per NARA practice, documentation for permanent electronic records must be transferred with the related
records using the disposition authority of the related electronic records rather than the GRS disposition authority.

Agency policy and responsibility for media and electronic sanitization is explicated in VA Handbook 6500.1, Electronic Media Sanitization. This Handbook sets forth policies and responsibilities for the proper sanitization of electronic media prior to repair, disposal, reuse, or recycling. These guidelines are in accordance with Federal Information Processing Standard (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems; and NIST Special Publication 800-88 Revision 1, Guidelines for Media Sanitization.


ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: VA will store records produced within this system of records in an area that is physically and technologically secure from access by unauthorized persons at all times. Only authorized personnel will transport records within this system of records. VA will process records produced within this system of records under immediate supervision and control of authorized personnel in a manner that will protect the confidentiality of the records, so that unauthorized persons cannot retrieve any records by computer, remote terminal, or other means. VA will store records using FIPS 140-2 compliant encryption. Systems personnel must enter personal identification numbers when accessing records on the agencies’ systems. VA will strictly limit authorization to those electronic records areas necessary for the authorized analyst to perform his or her official duties.

RECORD ACCESS PROCEDURES: An individual wanting notification or access, including contesting the record, should mail or deliver a request to the office identified in the SORN. If an individual does not know the “office concerned,” the request may be addressed to the following with below requirements: PO or FOIA/PO of any VA field station or the Department of Veterans Affairs Central Office, 810 Vermont Avenue, NW, Washington, DC 20420. The receiving office must promptly forward the mail request received to the office of jurisdiction clearly identifying it as “Privacy Act Request” and notify the requester of the referral. Approved VA authorization forms may be provided to individuals for use.

CONTESTING RECORD PROCEDURES: An individual may request amendment of a record pertaining to him or her contained in a specific VA system of records by mailing or delivering the request to the office concerned. The request must be in writing and must conform to the following requirements: It must state the nature of the information in the record the individual believes to be inaccurate, irrelevant, untimely, or incomplete; why the record should be changed; and the amendment desired. The requester must be advised of the title and address of the VA official who can assist in preparing the request to amend the record if assistance is desired. Not later than business 10 days after the date of a request to amend a record, the VA official concerned will acknowledge in writing such receipt. If a
determination for correction or amendment has not been made, the acknowledgement will inform the individual of when to expect information regarding the action taken on the request. VA will complete a review of the request to amend or correct a record within 30 business days of the date of receipt. Where VA agrees with the individual’s request to amend his or her record(s), the requirements of 5 U.S.C. § 552a(d) will be followed. The record(s) will be corrected promptly, Tow and the individual will be advised promptly of the correction.

If the record has previously been disclosed to any person or agency, and an accounting of the disclosure was made, prior recipients of the record will be informed of the correction. An approved VA notification of amendment form letter may be used for this purpose. An individual wanting notification or access, including contesting the record, should mail or deliver a request to the Privacy Office or FOIA/Privacy Office of any VA field station or the Department of Veterans Affairs Central Office, 810 Vermont Avenue, NW, Washington, DC 20420.

NOTIFICATION PROCEDURES: Notification for correcting the information will be accomplished by informing the individual to whom the record pertains by mail. The individual making the amendment must be advised in writing that the record has been amended and provided with a copy of the amended record. System Manager for the concerned VA system of records, Privacy Officer, or their designee, will notify the relevant persons or organizations who had previously received the record about the amendment. If 38 U.S.C. § 7332-protected information was amended, the individual must provide written authorization to allow the sharing of the amendment with relevant persons or organizations. A request to amend a record must be acknowledged in writing within 10 workdays of receipt. If a determination has not been made within this time period, the System Manager for the concerned VA system of records or designee, and/or the facility Privacy Officer, or designee, must advise the individual when the facility expects to notify the individual of the action taken on the request. The review must be completed as soon as possible, in most cases within 30 workdays from receipt of the request. If the anticipated completion date indicated in the acknowledgment cannot be met, the individual must be advised, in writing, of the reasons for the delay and the date action is expected to be completed. The delay may not exceed 90 calendar days from receipt of the request.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: N/A

HISTORY: VA 13VA047, Individuals Submitting Invoices-Vouchers for Payment-VA – published prior to 1995