Privacy Impact Assessment for the VA IT System called:

Enterprise Event Bus (EEB)

VACO

Veteran Experience Services (VES)

Date PIA submitted for review:

9/7/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Lynn Olkowski	Lynn.Olkowski@va.gov	(202) 632-8405
Information System Security Officer (ISSO)	Andrew Vilailack	Andrew.Vilailack@va.gov	(813) 970-7568
Information System Owner	Andrew Fichter	Andrew.Fichter@va.gov	(240) 274-4459

Abstract

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

The Enterprise Event Bus (EEB) is an asynchronous event processing system spanning systems and lines of business at the VA that allows producers to publish business events based on data changes and consumers to subscribe to those events. The system uses Kafka as its core event streaming platform, with AWS MSK (Managed Streaming for Apache Kafka) as the management layer.

Overview

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

1 General Description

A. The IT system name and the name of the program office that owns the IT system.

The Enterprise Event Bus (EEB) is part of the Veteran Experience Services (VES) portfolio.

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

Our hypothesis is that this system will reduce the complexity that is currently inherent in the direct coupling between VA systems that need to (or would benefit from) sharing data. With the Event Bus approach, event producers don't need to have direct connections with event consumers, and multiple event consumers may receive and act on a single event; i.e., it's not just an asynchronous queue sitting between a single producer and consumer. It should be noted that the Enterprise Event Bus is not intended to subsume or replace any existing API or eventing ecosystems; its focus is to provide access to events from existing systems that are of interest to a wider audience by filtering, enriching, or transforming the event payload to make it easier for other systems to work with.

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

Veteran Experience Services (VES)

2. Information Collection and Sharing

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

No information is stored in the Enterprise Event Bus itself; this is system of transport, not a system of record. See Section 4.1 of this document for a listing of the information transported by the system. For the Decision Letter Availability event, which is the only one that we have developed to the point where we have some sense of the production volume, there has been an average of 3,035 events per day over the last 6 weeks (8/25/23 – 10/5/23). Each event contains data for an individual who has a new claim decision letter to review. Note that we plan to submit a revised PIA document during Q1 2024 with additional details on the data sources we expect to go to production with.

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

The Enterprise Event Bus does not directly collect any information. As a system of transport, it acts as conduit through which information collected by VA systems can be more efficiently shared with other VA systems.

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

Anticipated types of information to be shared through the Enterprise Event Bus in its initial implementation include VistA appointment data (date and time, data file number, name, possibly SSN [we are actively working to exclude this, if possible]), and Veteran Participant ID as part of claim status information.

G. Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.

The Enterprise Event Bus only operates within the VA's AWS VAEC environment.

3. Legal Authority and SORN

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

The legal authorities to operate the system are 38 U.S.C. 7601-7604 and U.S.C 7681-7683. The system will be covered under the AWS-GovCloud ATO as a Moderate Impact system. (a) Title 40 U.S.C. § 1401 (3), Clinger-Cohen Act of 1996, which directs the development and maintenance of IT architectures by federal agencies to maximize benefits within the federal government (b) Government Performance and Results Act of 1993, designed to improve federal program effectiveness, enhance Congressional decision-making, and strengthen internal controls.

- Veterans Health Information Systems and Technology Architecture (VistA) Records-VA (79VA10), 2020-28340.pdf (govinfo.gov)
- Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records—VA (58VA21/22/28), 2021-24372.pdf (govinfo.gov)

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

The system is not in the process of being modified. The SORNs listed above reference system locations in the VA Enterprise Cloud (VAEC).

D. System Changes

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

No. There were no findings from the PTA that required a change to how the system operates.

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

No. There were no findings from the PTA that required technology changes.

Section 1. Characterization of the Information

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

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

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

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

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

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

- ☒ Name
- ☒ Social Security Number
- ☒ Date of Birth
- ☐ Mother's Maiden Name
- ☐ Personal Mailing Address
- ☐ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☐ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☐ Financial Information
- ☐ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers*
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☐ Medications
- ☐ Medical Records
- ☐ Race/Ethnicity
- ☐ Tax Identification Number
- ☒ Medical Record Number
- ☐ Gender
- ☒ Integrated Control Number (ICN)

☐ Military History/Service Connection
☐ Next of Kin
☒ Other Data Elements (list below)

<<Add Additional Information Collected But Not Listed Above Here (For Example, A Personal Phone Number That Is Used As A Business Number)>>

- Appointment Date and Time
- Patient Data File Number (DFN)
- Veteran Participant ID
- Account numbers

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

PII Mapping of Components (Servers/Database)

The Enterprise Event Bus (EEB) consists of zero key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by the Enterprise Event Bus (EEB) and the reasons for the collection of the PII are in the table below.

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

Internal Database Connections

This is not applicable – there are no direct database connections between the Enterprise Event Bus system and any other systems, VA or otherwise.

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
N/A	N/A	N/A	N/A	N/A	N/A

1.2 What are the sources of the information in the system?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.2a List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

The Enterprise Event Bus does not directly collect any information from any individuals, it only works with data that already exists within VA systems. Currently, data included in the one event that is produced for the Event Bus comes from the Benefits Integration Platform (BIP) Kafka cluster. Specifically, BIP has made Version 1 of the ClaimLifecycleStatusUpdatedEvent available in their dev, staging, and production environments. The data for the event is consumed from two CorpDB

tables: Benefit Claim Lifecycle Status (BNFT_CLAIM_LC_STATUS) and Benefit Claim (BNFT_CLAIM).

1.2b Describe why information from sources other than the individual is required. For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question indicate why the system is using this source of data.

Not applicable – the Enterprise Event Bus does not directly collect any information from any individuals, it only works with data that already exists within VA systems.

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

Not applicable. The system does not create any information; it only moves information from one system to another.

1.3 How is the information collected?

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.3a This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technologies used in the storage or transmission of information in identifiable form?

Not applicable – the Enterprise Event Bus does not directly collect any information from any individuals, it only works with data that already exists within VA systems.

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

Not applicable – the Enterprise Event Bus does not directly collect any information from any individuals, it only works with data that already exists within VA systems.

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

These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

Apache Kafka, the technology that underpins the Enterprise Event Bus, provides delivery guarantees that producing systems can leverage to ensure data is correctly pushed into the Event Bus system. The configuration that will be applied to the data stream will be selected based on the needs of that system and the nature of the data stream. For data streams which can tolerate the risk of duplicate messages, at-least-once delivery will be selected; with this configuration, the push of data is not considered complete until the Event Bus system has acknowledged that the event has been received – triggering retries in the event of failures. For data streams which cannot tolerate duplicate messages, the stream can be configured for exactly once delivery. With this configuration option, the system assigns each event a unique sequence number based on the data and producer. The stream will only accept the push if this number is unique, and the write will not be considered complete until the Event Bus system has acknowledged that the event has been received. Of note, the Enterprise Event Bus is not to be considered an authoritative data source and data streams are not intended for long-term storage of data.

1.4b If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

Not applicable, no outside sources are used by the Enterprise Event Bus.

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

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

The legal authorities to operate the system are 38 U.S.C. 7601-7604 and U.S.C 7681-7683. The system will be covered under the AWS-GovCloud ATO as a Moderate Impact system. (a) Title 40 U.S.C. § 1401 (3), Clinger-Cohen Act of 1996, which directs the development and maintenance of IT architectures by federal agencies to maximize benefits within the federal government (b) Government Performance and Results Act of 1993, designed to improve federal program effectiveness, enhance Congressional decision-making, and strengthen internal controls.

- Veterans Health Information Systems and Technology Architecture (VistA) Records-VA (79VA10), 2020-28340.pdf (govinfo.gov)
- Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records—VA (58VA21/22/28), 2021-24372.pdf (govinfo.gov)

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Privacy Risk: The system transports PII and PHI on Veterans, and potentially other people who may be eligible for or are receiving benefits and/or health care from VA, from one internal VA system to another. **The system does not directly collect data from any individual**, and thus does not provide any policies and procedures to ensure that personally identifiable information is accurate, complete, and current.

If Event Bus information was breached or accidentally disclosed to inappropriate parties or the public, limited appointment and claims data for an individual could be exposed. For appointment data, this could potentially include a unique identifier for the individual and some identifying details about the type of appointment. For claims data, this could potentially include a unique identifier for the individual, a unique identifier for a claim, and some basic information about the claim.

Mitigation: The Enterprise Event Bus follows best practices regarding encrypting data in transit and at rest throughout our system. The system is located on the VA network and can only be accessed by other internal-to-VA systems. When considering which information passes through the system, we seek to minimize sensitive data. Individuals are not permitted direct access to the data that passes through the Event Bus, as the Event Bus is intended for system-to-system transit of data. These systems follow the principles of least privilege, which means that each system is only allowed to access a specific subset of the data as deemed necessary for their functionality. In the event of a security incident resulting from a misconfiguration in permissions, members of the Enterprise Event Bus Administrative team are trained to respond to security incidents in accordance with VA best practices defined in (VA Privacy and Information Security Awareness TMS 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.

All use of information by the Enterprise Event Bus is internal to VA. Our anticipated uses for the first iteration of the system include: An "appointment firehose" of VistA appointment data that clinician facing applications can use to show current appointment status and any other relevant applications can take appropriate follow-up actions; and a claim decision letter availability event that will trigger an email notification to a Veteran to view the letter in the Claim Status Tool. See the table below for details about each of the PII/SPI selected in Question 1.1. NOTE that PII/SPI associated with Appointment Firehose Events is subject to change; we are still in the process of finalizing the payload definition for those events. This will be updated when we submit a revised PIA document during Q1 2024.

Name: Internal, used as a patient identifier in Appointment Firehose Events.

Social Security Number: Internal, used as a patient identifier in Appointment Firehose Events (tentative; we will be working with the data source provider to eliminate this if possible).

Date of Birth: Internal, used as a patient identifier in Appointment Firehose Events.

Medical Record Number: Internal, used as a patient identifier in Appointment Firehose Events.

Integrated Control Number (ICN): Internal, used as a patient and/or appointment identifier in Appointment Firehose Events.

Appointment Date and Time: Internal, appointment detail in Appointment Firehose Events to be displayed by a consuming application.

Patient Data File Number (DFN): Internal, used as a patient identifier in Appointment Firehose Events.

Veteran Participant ID: Internal, used as a beneficiary identifier in the Claim Decision Letter Availability Event.

2.2 What types of tools are used to analyze data and what type of data may be produced?
These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis.

The Enterprise Event Bus does not currently perform complex meta-analysis on the data that we ingest. However, our Decision Letter Availability engine generates a data stream of events that are triggered in response to an ingested stream of events from the Benefits Integration Platform. When

events in the stream for the ClaimLifecycleStatusUpdated event are either Authorized or Continued at Authorization and the ClaimTypeCode starts with 01, 02, 03, 04, 08, 11, 12, 17, 18 or 40, our system generates a decision letter availability event.

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

Not applicable. The Enterprise Event Bus only works with existing (internal to VA) data that is currently utilized by one or more systems. The system does not create or make available any new information about individuals.

2.3 How is the information in the system secured?

These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

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

The Enterprise Event Bus leverages the encryption features provided by Amazon MSK to encrypt data at rest and in transit. We only allow encrypted data in and out of our cluster; any system that produces or consumes our data streams must connect via `SASL_SSL.` (For more information, please see the Amazon MSK documentation at https://docs.aws.amazon.com/msk/latest/developerguide/msk-encryption.html)

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

The Event Bus team is actively collaborating with the Health Middleware Data Management (HMDM) team to build integrations that will allow us to obtain and leverage ICNs instead of SSNs. If these integrations are unable to provide us with the data we need to reduce the proliferation of SSNs, in addition to the end-to-end encryption described above there is no long-term storage of this data on the Enterprise Event Bus system. Furthermore, access to this data is restricted to only those systems that require this data to function.

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

In accordance with OMB Memorandum M-06-15, the Enterprise Event Bus provides end-to-end encryption for all PHI/PII passing through the system. The event streams are flushed when the retention period for an event expires (after 7 days), preventing data from being stored long-term on the system. The system has implemented fine-grained authorization, allowing administrators to limit the data that other VA systems are allowed to access to only that which are determined to be necessary for their business process. Additionally, the system seeks to minimize the amount of PHI/PII it collects and is actively working to seek alternatives to SSNs. The Event Bus's internal

guidelines for handling PII and PHI and the implications of working with this data are available in our internal documentation at https://github.com/department-of-veterans-affairs/VES/blob/master/research/Event%20Bus/Phase%203%20Artifacts/PII%20and%20PHI%20Security%20Implications.md.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?
This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

2.4a How is access to the PII determined?

Access is not granted to individuals, but to other systems. Before a system is given access to a data stream, a meeting between the team supporting a prospective Event Bus producer or consumer system and the Enterprise Event Bus administrative team must occur. The onboarding team must outline the information that they require and provide a justification for access. The Enterprise Event Bus is only available to connect with VA internal systems. After this initial review of access, the Enterprise Event Bus Administrative team creates a request to create the IAM (Identity and Access Management) policy that will be approved and applied by a member of the Lighthouse Delivery Infrastructure team. In addition to the process described above, access to production data will require that the team obtain their own Authority to Operate (ATO). Enterprise Event Bus Team administrators do not have direct access to PII or PHI but can modify who has access to this data. These individuals must undergo mandatory annual online information security and HIPAA training via the VA Talent Management System (TMS). Regular audits of individuals with this role will be performed to ensure that only active team members have access to modify permissions on the enterprise event bus system.

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

The design criteria for creating new events can be located in our PII & PHI Guidelines document (https://github.com/department-of-veterans-affairs/VES/blob/master/research/Event%20Bus/Engineering/PII%20and%20PHI%20Security%20Implications.md). A technical overview of our procedure for implementing controls can be found in

our Authorization and Authentication ADR (https://github.com/department-of-veterans-affairs/VES/blob/master/research/Event%20Bus/Engineering/ADR/ADR%20MSK%20Authentication%20and%20Authorization.md). The onboarding process for systems interested in consuming events is located in our documentation portal, with versions available for both consuming systems (https://department-of-veterans-affairs.github.io/ves-event-bus-developer-portal/consume-events/) and producing systems (https://department-of-veterans-affairs.github.io/ves-event-bus-developer-portal/produce-events/).

2.4c Does access require manager approval?

Access requires approval from both the Event Bus Administrative team leadership and the Lighthouse Delivery Infrastructure team.

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

The Enterprise Event Bus Administrative team does not have direct access to modify access control policies and must make these changes through Terraform. In addition to the internal logs of changes kept by Amazon, all changes that are made to these access policies, including the individual who submitted and approved them, are recorded via GitHub. The Enterprise Event Bus system does not monitor what consuming systems do with the data once they have subscribed to the topic. These systems are subject to their own PIA reviews to ensure best practices are followed.

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

Event Bus Team Administrators are responsible for submitting requests for access and performing audits to remove access for offboarded teams. The Lighthouse Delivery Infrastructure team is responsible for creating the policies that systems leverage to access sensitive data, as described in this authorization and authentication document: https://github.com/department-of-veterans-affairs/VES/blob/master/research/Event%20Bus/ADR/ADR%20MSK%20Authentication%20and%20Authorization.md Any changes to how data is handled internally on the Event Bus system is subjected to code review and must be technically vetted by the Event Bus engineering team prior to being incorporated into the project.

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*

All information listed in 1.1 is retained in the relevant events in the Kafka instance. See this Event Retention discussion for more details: https://github.com/department-of-veterans-affairs/VES/blob/master/research/Event%20Bus/Engineering/ADR/ADR%20event%20design.md#event-retention.

3.2 How long is information retained?

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

Events that include information listed in 1.1 are retained for a default period of seven days in the Kafka instance. This should provide adequate time for any consuming systems to pick up the event. See this Event Retention discussion for more details: https://github.com/department-of-veterans-affairs/VES/blob/master/research/Event%20Bus/ADR/ADR%20event%20design.md#event-retention.

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

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

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

This is not applicable to the Enterprise Event Bus. The Event Bus system does not create or store any records in a system of record. It is only passing a stream of messages from one system to another and does not retrieve any individual records based on a specific personal identifier.

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

This is not applicable to the Enterprise Event Bus. As noted in the previous question, the Event Bus system does not create or store any records in a system of record.

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

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

This is not applicable to the Enterprise Event Bus. As noted in the previous question, the Event Bus system does not create or store any records in a system of record.

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

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

The Enterprise Event Bus does not use PII for testing purposes. Data found in lower environments, such as development, is mocked out.

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

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

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

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

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

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

<u>Privacy Risk:</u> Data persists on the event stream for seven days. This period has been selected as an appropriate amount of time for systems to pick up an event, with an allowance for some buffer time

in case there is scheduled system downtime or an unplanned network connection interruption. While our system does not persist the data for longer than this seven-day period, the data stream records are stored in an underlying file system.

Mitigation: Systems can only access the data stream through Kafka. Data is encrypted throughout all stages of this process. Once the retention period has passed, AWS EBS automatically purges this data from the file record. AWS EBS acts as an internal file system and is only directly accessible by the internal Kafka brokers. Consuming and producing systems cannot directly access the underlying file system. This minimizes the amount of time that the sensitive data is persisted in our system, and ensures that once the retention period has passed, it is purged from the system.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA.

4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

NOTE: Question 3.9 (second table) on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system within VA with which information is shared.

State the purpose for the internal sharing. If you have specific authority to share the information, provide a citation to the authority.

For each interface with a system outside your program office, state what specific data elements (PII/PHI) are shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?
This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Veterans Health Administration Veterans Health Information Systems and Technology Architecture (VistA)	Provides updated appointment data as it happens so that clinician facing applications show current appointment status and any other relevant applications can take appropriate follow-up actions.	• Appointment Date and Time • Patient Data File Number (DFN) • Patient Name • Patient SSN	TCP
Benefits Integration Platform (VASI #2259) – • Claim Lifecycle StatusUpdated Event	This will be the source event that will create an action for VANotify to generate an email that will be sent to a Veteran when a claim decision letter is available to view in the Claim Status Tool.	• VeteranParticipantId	TCP
VA.gov - Veteran-facing Services Platform (VASI #2103) • VANotify (System Architect/Publisher (va.gov)) • Claim Status Tool	VANotify will generate an email, based on a notification sent by the Event Bus, to be sent to a Veteran when a claim decision letter is available to view in the Claim Status Tool.	• VeteranParticipantId	TCP

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

This question is related to privacy control UL-1, Internal Use.

Privacy Risk: As a conduit between VA systems, the Enterprise Event Bus does not have control of the data once it leaves our system. It will ultimately fall upon the consuming systems to ensure that any PII or PHI data is appropriately handled.

Mitigation: The Enterprise Event Bus is implementing an onboarding process for systems that are interested in consuming events, which will help walk them through expectations regarding how sensitive data should be handled. All data found in lower environments, such as development, staging, and other test environments, must be mocked out. Consuming systems must undergo their own PIA reviews before accessing production data.

Privacy Risk: While we have policies that all data found in lower environments must be mocked, it is possible that a system may inadvertently push PII/PHI into these lower environments.

Mitigation: All individuals accessing the Enterprise Event Bus as administrators must undergo annual training regarding online information security and HIPAA policies via the VA Talent Management System (TMS), and thus are familiar with the protocol that must be followed regarding handling incidents where private data is exposed. We also have a protocol for purging sensitive records (https://github.com/department-of-veterans-affairs/VES/blob/master/research/Event%20Bus/Phase%203%20Artifacts/PII%20and%20PHI%20Security%20Implications.mds) to minimize exposure if private data is exposed.

Privacy Risk: Event-based architecture creates streams of data; because data is actively pushed to consuming systems, this potentially increases the impact of any security incident. In the event of misconfigured permissions, data will actively stream to systems configured to receive it.

Mitigation: The process of allocating new Identity and Access Management (IAM) policies requires two approvals to minimize the chances of policy misconfiguration that could give systems access to data that they should not have. Whenever possible, events are designed to minimize the amount of sensitive data they contain (see this Event Guidance document: https://github.com/department-of-veterans-affairs/VES/blob/master/research/Event%20Bus/Phase%202%20Artifacts/Engineering%20Notes%20-%20Event%20Guidance.md) to minimize the impact of such a misconfiguration.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

Data Shared with External Organizations

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

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

Discuss the privacy risks associated with the sharing of information outside the Department and what steps, if any, are currently being taken to mitigate those identified risks.

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a

Memorandum of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.
Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.
This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Privacy Risk: There is no privacy risk, as the Enterprise Event Bus system does not share any information with systems external to VA.

Mitigation: N/A

Section 6. Notice

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

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

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

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

This is not applicable; the Enterprise Event Bus does not do any direct data collection from individuals.

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

This is not applicable; the Enterprise Event Bus does not do any direct data collection from individuals.

6.1c Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

This is not applicable; the Enterprise Event Bus does not do any direct data collection from individuals.

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress.

This is not applicable; the Enterprise Event Bus does not do any direct data collection from individuals.

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

This question is directed at whether an individual may provide consent for specific uses, or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent.

This is not applicable; the Enterprise Event Bus does not do any direct data collection from individuals.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

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

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

Privacy Risk: Notice is provided to individuals by the systems that do the initial collection of data, not the Event Bus system. Although the information is collected from other source systems, there is still a risk of no notice.

Mitigation: The SORN documents referenced in Overview Section 3H and Characterization of Information Section 1.5 in this document should serve as a mitigation.

Section 7. Access, Redress, and Correction

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

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

These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. ***For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.***

Procedures put into place to access information are handled by the systems that initially collect the information, not the Event Bus system.

7.1b If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR).

The Enterprise Event Bus system is exempt from these provisions as it does not collect or write any information about individuals; the system only transfers information from one system to another.

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

This is not applicable, as the Enterprise Event Bus system does not directly collect information from individuals, and no individuals have access to the system; it only provides system to system information transport.

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.

This is not applicable, as the Enterprise Event Bus system does not directly collect information from individuals and thus does not have any means to correct information that originates in other

systems. If an individual wishes to correct information about themselves, they will need to contact the system(s) that initially collected the information.

7.3 How are individuals notified of the procedures for correcting their information?

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

This is not applicable, as the Enterprise Event Bus system does not directly collect information from individuals and thus does not have any means to correct information that originates in other systems. When applicable, individuals will be notified by the system(s) that initially collected the information.

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

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

This would be handled by the systems that originally collect the information that is shared with the Enterprise Event Bus.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

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

Privacy Risk: The Enterprise Event Bus system does not directly collect any information from individuals and thus does not have any provision for providing access, redress, and correction. Although this system does not collect information from individuals, there is still a privacy risk associated to individuals not having access, redress and correction.

Mitigation: Access, redress, and correction activities take place through the systems that originally collect the information that is shared with the Enterprise Event Bus.

Section 8. Technical Access and Security

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

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

These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.

8.1a Describe the process by which an individual receives access to the system.

Individuals outside of system administrators are not given direct access to the system. New system administrators must go through the process of obtaining a valid va.gov email address. Once this has been obtained, an existing system administrator must request access for that individual by contacting the Lighthouse Delivery Infrastructure support team per their support channels (https://animated-carnival-57b3e7f5.pages.github.io/SUPPORT/#product-owner-contact-info). Note that this does not grant that individual access to any of the data within the system, and system administrators cannot directly modify data access permissions. They must first open a pull request against the Lighthouse-DI managed customer resources repository (https://github.com/department-of-veterans-affairs/lighthouse-di-managed-customer-resources) to allocate the new permissions, and then reach out to an administrator on the Lighthouse Delivery Infrastructure team to approve the change and create the new resource.

8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

No users from other agencies will have access to the Enterprise Event Bus, only systems within VA have access.

8.1c Describe the different roles in general terms that have been created to provide access to the system. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

Note that these terms apply to systems that are accessing the system. The Enterprise Event Bus is intended for system-to-system communication, and individual users are not permitted to directly access the event streams. The Event Bus leverages AWS IAM (Identity and Access Management) for its authentication and authorization. “Topic Consumers” are systems which have read access to a

specific topic, and "Topic Producers" are systems that have read and write access to a specific topic. See MSK Service Authorization Reference (https://docs.aws.amazon.com/service-authorization/latest/reference/list_amazonmanagedstreamingforapachekafka.html) for a full listing of available actions and resource types.

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

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII. This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

The Enterprise Event Bus is designed and developed by a team with 100% contractor staff. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of behavior training via the VA's TMS. All contractors are cleared using the VA background investigation process and must obtain a Moderate Background Investigation (MBI) clearance before access is granted.

All user access to the Event Bus system is provisioned and processed in accordance with Lighthouse Delivery Infrastructure (LHDI) policies and procedures. See the following documentation for more information:

- LHDI Getting Started Guide
- Access Validation Guide
- Lighthouse Delivery Infrastructure (LHDI) Onboarding Process Overview (as of 5/22/23)

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.

VA Privacy and Information Security Awareness and Rules of Behavior (WBT); Privacy and HIPAA Training via the VA's TMS.

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

No. The system is currently in development and will not be deployed to production until sometime in the Q2 2024 time frame. The Event Bus team is actively working toward fulfilling the requirements

to be included in the LHDI Continuous ATO (cATO): https://jubilant-succotash-m55rqe7.pages.github.io/.

8.4a If Yes, provide:

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

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

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

As noted above, the system is currently in development and will not be deployed to production until sometime in the Q2 2024 time frame. Although we do not have a specific IOC date at this time, our current intention is to have a feature complete MVP system finished in the March – April, 2024 time frame, which will then start moving through the processed required to get to a production deployment.

Section 9 – Technology Usage

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

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

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

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

Yes, we are on the AWS (Amazon Web Services) VAEC, in the Lighthouse Delivery Infrastructure (LHDI).

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

N/A

9.3 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.

This question is related to privacy control DI-1, Data Quality.

N/A

9.4 NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

N/A

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

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

N/A

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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

Signature of Responsible Officials

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

Lynn A Olkowski

Digitally signed by Lynn A Olkowski
Date: 2023.10.19 10:20:55 -05'00'

Privacy Officer, Lynn Olkowski

ANDREW VILAILACK

Digitally signed by ANDREW VILAILACK
Date: 2023.10.20 13:32:22 -04'00'

Information System Security Officer, Andrew Vilailack

ANDREW FICHTER

Digitally signed by ANDREW FICHTER
Date: 2023.10.23 09:29:05 -04'00'

Information System Owner, Andrew Fichter

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).

This is not applicable; the Enterprise Event Bus does not do any direct data collection from individuals.

HELPFUL LINKS:

Record Control Schedules:

https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

General Records Schedule 1.1: Financial Management and Reporting Records (FSC):

https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

National Archives (Federal Records Management):

https://www.archives.gov/records-mgmt/grs

VHA Publications:

https://www.va.gov/vhapublications/publications.cfm?Pub=2

VA Privacy Service Privacy Hub:

https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices