

**Do not alter the Template. Provide responses where prompted only.**

## Purpose and Scope

The Privacy Threshold Analysis (PTA) is privacy compliance and risk management assessment tool designed to document the collection, creation, maintenance, use and disclosure of personally identifiable information (PII) and personal health information (PHI) within an information technology (IT) system, program, rulemaking, or project.

A PTA is used to determine if an IT system or project contains PII/PHI, whether a Privacy Impact Assessment (PIA) is required, whether a System of Records Notice (SORN) is required or needs to be updated, and if any other privacy requirements apply. Additionally, a PTA must be completed for an IT system or project to receive an ATO.

A PTA is reviewed and approved by VA Privacy Service before the development or acquisition of a new IT system and annually, thereafter, unless there is a major change to an existing IT system or project. When a major change<sup>1</sup> occurs to an existing IT system or project, the PTA must be updated and approved *prior* to the implementation of the change.

**Note:** Major changes to information system may require updates to other privacy compliance documentation such as the PIA and SORN *prior* to the implementation of the change. VA Privacy Service will inform the system contacts of any additional privacy requirements.

The completion of the PTA is a collaborative effort between the VA Privacy Service, Information System Owner (ISO) or Program Manager (PM), Information System Security Officer (ISSO), System Privacy Officer (PO), and other stakeholders. The PTA review must be reviewed and concurred with by the PO, ISSO, and ISO prior to submission to PIA Support. Please see the **PTA and PIA Guide** for more details. Upon completion of an initial review, the PO, ISSO, or the System Steward will forward a copy to the VA Privacy Service's PIA Support Mail Group for final review and approval.

**Note: You must obtain PO concurrence prior to submitting to the VA PIA Support Team. Additionally, PTAs must receive approval and be signed by the VA PIA Support Analyst prior to uploading the document into the Enterprise Mission Assurance Support Service (eMASS). PTAs without VA Privacy Service approval are invalid. Please review the PTA/PIA Submittal Checklist and Process Overview prior to submission.**

---

<sup>1</sup> VA DIRECTIVE 6508 - 5. DEFINITIONS **d.** Major Change. A change to the information collected or maintained that could result in greater disclosure of information or a change in the way personal data is used.

**\*Spell out all acronyms first time used\***

## 1 - Information System and Project Information

1.1 Date PTA submitted to PIA Support for review: 3/27/2025

1.2a Name of the IT System or Project (Add system name as it appears in eMASS):

Data Synchronization

1.2b Former System Name (from last PTA): *Click or tap here to enter text.*

1.3 eMASS ID #: 2050

1.3b ☐ Artificial Intelligence (AI) (checkbox if system uses Artificial Intelligence)

1.4 Name of VA Administration/Offices processing the PTA:

- ☐ VHA
- ☒ VBA
- ☐ NCA
- ☐ VACO (Includes Enterprise, OI&T, FSC, etc.)

1.4a Identify data owners in this system (check all that apply)

- ☐ VHA ([List of VHA Offices](#))
- ☒ VBA ([List of VBA Offices](#))
- ☐ NCA
- ☐ VACO (i.e., Enterprise, OI&T, VEO, FSC, etc.) ([List of VACO Offices](#))
- ☐ If other, please specify: \_\_\_\_\_

1.5 Name of the Program Office within the Administration that the system is sponsored by:

Office of Information and Technology

1.5.1 Indicate system ownership/control for the IT system or project. If the system has an [eMASS](#) entry, ensure this information matches with the eMASS entry:

- ☐ VA Partnership
- ☒ VA Owned and VA Operated
- ☐ VA Owned and non-VA Operated
- ☐ VA Controlled / non-VA Owned and Operated

### IT SYSTEM AND PROJECT CONTACTS

Title	Name	E-mail	Phone Number	Signature Required
Privacy Officer	Marvis Harvey	Marvis.harvey@va.gov	314-964-5469	Yes
Information System Security Officer	Tamer Ahmed	Tamer.Ahmed@va.gov	202-461-9306	Yes
Information System Owner	Christina Lawyer	Christina.lawyer@va.gov	518-210-0581	Yes
Data/Business/Information Owner <sup>2</sup>	Christina Lawyer	Christina.lawyer@va.gov	518-210-0581	No

### STATUS OF IT SYSTEM AND PROJECT

1.6 Select the box which reflects the status of IT system or project:

- ☐ This is a new IT system or project.
- ☐ This is an existing IT system or project that has never had a PIA.
- ☒ This is an existing IT system or project that has a **current** approved PIA. Provide the approval date for the PIA. **Approval date will be the date of the last signature.**  
5/31/2022
- ☐ This IT system or project is being decommissioned. Please refer to the [PTA and PIA Guide](#) for instructions on how to complete a Decommission PTA.
- a. Indicate date of decommission: *Click here to enter a date.*
- b. Describe what will happen to the system data upon decommission, if data is being migrated, indicate where:  
*Enter Major Application name here.*
- ☐ This IT system or project is no longer operational but not decommissioned.  
*Click here to enter the planned/expected decommission date*

1.7 Select the box that applies to the IT system or project:

(Select one of the below checkboxes, if applicable):

---

<sup>2</sup> VA DIRECTIVE 6508: System Steward/Data Owners - Work with the POs, Program Managers, Project Managers, ISOs, System Managers, and System Developers to ensure that appropriate privacy protections related to data sensitivity are in place and indicated in their PIA submissions; Serve as point of contact for questions related to system data; Respond to questions from POs, Program Managers, Project Managers, ISOs, System Managers, and System Developers that are related to the PA submission.

- ☒ This IT System or project is categorized as minor system and augments a major system<sup>3</sup>

Benefits Integration Platform (BIP) eMASS ID # 136

- ☐ This IT System or project is categorized as a major system with no minor systems.
- ☐ This IT System or project is categorized as a major system with minor systems under it.

1.8 Select the box that reflects the type of model used by the IT system or project:

- ☒ Software as a Service (SaaS)
- ☐ Platform as a Service (PaaS)
- ☐ Infrastructure as a Service (IaaS)
- ☐ Desktop as a Service (DaaS)
- ☐ Mobile Backend as a Service (MBaaS)
- ☐ Information Technology Management as a Service (ITMaaS))
- ☐ Not Applicable

1.9 Check the box below that reflects the type of information contained in the IT system or project:

- ☒ The product/Service **WILL** contain and/or process VA data.
- ☐ The product **WILL NOT** contain and/or process VA data. If selected, please use the below checkboxes to indicate the applicable criteria:
- ☐ User owns a device (even if VA paid for the purchase of the device).
  - ☐ product/Service has no direct connections or interfaces to VA systems or network.
  - ☐ Users consent to share their data (which may include PII and PHI) directly with the provider.
  - ☐ Provider must have published terms and conditions for user consent.
  - ☐ VA providers access data in a view-only mode, or with limited functionality per the user's consent.

1.10 If the system is registered in eMASS, please identify the PII confidentiality impact level within the Privacy Overlay (under Categorization) as marked in eMASS (**Skip this question if the system does not have an entry in eMASS or is not privacy sensitive.**)

---

<sup>3</sup> OMB Circular A-130, Major information system means a system that is part of an investment that requires special management attention as defined in OMB guidance and agency policies, a "major automated information system" as defined in 10 U.S.C. § 2445, or a system that is part of a major acquisition as defined in the OMB Circular A-11, Capital Programming Guide, consisting of information resources.

- ☐ Low  
☒ Moderate  
☐ High

## 2 - Annual PTA Validation Process

[Skip this section if this is a new PTA submission or if system is being decommissioned]

The IT System and Project contacts must resubmit the PTA annually to attest or indicate if any major changes have occurred to the IT system or project which creates new privacy risks.

2.1 Select the appropriate box(es) below.

- ☒ As part of the annual PTA validation process, there **ARE** major changes<sup>4</sup>. If there are major changes, provide a description of the changes.

The removal of Veteran Benefits Management System (VBMS) system and the addition of External Consumer/Consumer Utilization system in section 3.9b table.

- ☐ The major change involves a Patch to an IT system titled: *Click here to enter text*.

- ☐ As part of the annual PTA validation process there are **NO** major changes.

- ☐ As part of the annual PTA validation process there are **NO** major changes, but PIA needs to be updated to match the PTA.

## 3 - Privacy Threshold Analysis Questions

- 3.1 Please **start with the eMASS system name** and describe how information is collected, used, and transmitted in layman's terms so that a non-technical person can understand. The description should be at least a paragraph. (**Spell out all acronyms first time use**)

The Data Synchronization application, or "Data Sync" is a replacement for a legacy capability originally built inside of Veteran Benefits Management System (VBMS) Core that supported synchronizing changes that occur to Person or Claim data in VBA Corporate Database (CorpDB) through an interface with Benefits Gateway Services (BGS). This Data Sync extracts the logical elements of the legacy application within

---

<sup>4</sup> For guidance on "major changes", please refer to the "PTA and PIA Guide" available at <https://dvagov.sharepoint.com/sites/OITPrivacyHub/SitePages/PTA-Training-Resources.aspx>, and OMB M-3-22 "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002" available at [https://department.va.gov/privacy/wp-content/uploads/sites/5/2023/02/OMB\\_Memorandum\\_03-22.pdf](https://department.va.gov/privacy/wp-content/uploads/sites/5/2023/02/OMB_Memorandum_03-22.pdf)

VBMS and restructures them as a standalone application for use both in updated VBMS capabilities as well as new capabilities requiring access to Person or Claim change “events”.

3.2 Does the IT system or project employ any of the following technologies? *(Check all that apply.)*

- ☒ Cloud Computing<sup>5</sup>
- ☐ Web Portal
  - ☐ Internal
  - ☐ External ☐ SharePoint
- ☐ Closed Circuit TV
- ☐ Social Media
- ☐ Mobile Devices/Applications
- ☐ Applications
- ☐ Robotic Process Automation (RPA)<sup>6</sup>
- ☐ Other: *Click here to enter information.*
- ☐ Not Applicable

3.3 Is data stored in the cloud?

- ☒ Yes.
- ☐ No.

---

<sup>5</sup> Cloud Computing includes the following products/services: Software as a Service (SaaS), Managed Software as a Service (MSaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), and Information Technology Management as a Service (ITMaaS).

<sup>6</sup> Robotic Process Automation (RPA): 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).

3.3.1 Please list each Cloud Service Provider (CSP) hosting the information, describe the agreement in in place, and specify FedRAMP Status.

[Enter Hosting CSP Name]	Agreement in Place {Yes or No}	Description of Agreement {SLA, MOU, Contract Number, etc}	FedRAMP Approve {Yes or No}
VAEC AWS Government	Yes	Contract # NNG15SD22B VA118-17-F-2284	Yes

3.4 Does the IT system or project collect, process, retain or share any information about individuals?

- ☐ No. If no, briefly describe the type of information collected, processed, retained, or shared by the IT system or project.

*Click here to enter response.*

**NOTE:** If you checked “No”, STOP hereafter entering the types of information. Please do not make any checkbox selections after 3.4 as no further responses are required. This also applies to decommissioned systems as they should no longer collect, process, or retain PII/PHI. Proceed with submitting the PTA to VA Privacy Service’s PIA Support team ([piasupport@va.gov](mailto:piasupport@va.gov)) for review and determination.

- ☒ Yes. Please complete the table below.

*PII / PHI Data Collected*

Check if Applicable	Categories of Individuals	List PII/PHI data elements
<input checked="" type="checkbox"/>	Veterans or Dependents	<ul style="list-style-type: none"> <li>• Name</li> <li>• Social Security Number</li> <li>• Date of Birth</li> <li>• Military History/Service Connection</li> <li>• Flashes</li> <li>• Stations of jurisdiction</li> <li>• File Numbers</li> <li>• Benefit Information</li> <li>• Claims Decisions</li> <li>• DD-212</li> </ul>
<input type="checkbox"/>	VA Employees	•
<input type="checkbox"/>	VA Contractors	•
<input type="checkbox"/>	Members of the Public/Individuals	•
<input type="checkbox"/>	Volunteers	•
<input type="checkbox"/>	Clinical Trainees	•

### PRIVACY ACT SYSTEM OF RECORDS

3.5 Is information about individuals **retrieved** from the IT system or project by a unique identifier such as Name, Social Security Number, or other number (ex. Internal/Integrated Control Number (ICN))?

- ☐ No.  
☒ Yes.

3.5.1 If **yes**, is there an existing Privacy Act system of records notice (SORN) that has been published in the Federal Register to cover this IT system or project and the information within it?

- ☐ No. If no, please consult with your system Privacy Officer or VA Privacy Service for guidance.  
☒ Yes. If yes, provide the SORN number, SORN Title and a link to the SORN from the OPRM site<sup>7</sup>([https://www.oprm.va.gov/privacy/systems\\_of\\_records.aspx](https://www.oprm.va.gov/privacy/systems_of_records.aspx)).

---

<sup>7</sup>SORNs can be used from the point of collection system (feeder system) as data elements apply and/or a SORN developed for system-specific systems.



58VA21/22/28 – Compensation, Pension, Education and Vocational Rehabilitation and  
Employment Records - VA

<https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf>.

**If yes**, does the SORN need to be updated? (SORNs need to be updated if older than 6 years from date of publication in the Federal Register)

- ☒ No  
☐ Yes, **if yes**, please contact SORN Point of Contact

NOTE: If the SORN needs to be updated, please do not give the System of Records the same name as the IT system. SORNs should be technology-neutral – they pertain to the information within the IT system, not the IT system itself.

3.6 Does the system involve information collected directly from individuals who are the subject of the information<sup>8</sup>?

- ☒ No  
☐ Yes

### SOCIAL SECURITY NUMBER REDUCTION

3.7 Are Social Security Numbers (SSNs) collected, processed, retained, or shared by the IT system or project?

- ☐ No  
☒ Yes (Can a different identifier be used in place of SSN)?

3.8 Does the IT system or project employ any of the following Privacy Enhancing Technologies to protect SSN?

- ☐ No  
☒ Yes. If yes, (Check all that apply)  
☒ Encrypted  
☐ Anonymized  
☐ Truncated  
☐ Partial form (Last four digits)

---

<sup>8</sup> Information collected directly from individuals requires a Privacy Act (e)(3) statement. Agencies must provide a Privacy Act Statement to all persons asked to provide personal information about themselves, which will go into a system of records (i.e., the information will be stored and retrieved using the individual's name or other personal identifier such as a Social Security Number). Per [VA Handbook 6300.5](#): "VA shall provide a Privacy Act statement in such circumstances regardless of whether the information will be collected on a paper or electronic form, on a website, on a mobile application, over the telephone, or through some other medium. This requirement ensures that the individual is provided with sufficient information about the request for information to make an informed decision on whether or not to respond."

- ☐ Hidden from all users
- ☐ Only available to certain users
- ☐ Not applicable.

INTERNAL AND EXTERNAL INFORMATION SHARING

3.9a Does the IT system or project connect, receive, or share PII<sup>9</sup> with another **internal** VA organization, IT system, website, or application?

- ☐ No *[If “No,” place “N/A” in the Table below]*
- ☒ Yes *[If “Yes,” please explain in Table below]*

PII Mapping of Components

**Components are the technology that make up the system. Components gather the data, process the data, and communicate information to the user of the system.** *[All PII/PHI data elements listed in this table must be listed in question 3.4 above. If PIA is required, this information in this table should match the information in the Components table of question 1.1 in the PIA.] Please list all components that make up the system. Databases can be found on the [Database Inventory Portal](#).*

Internal Components Table

Component Name (Database, Instances, Applications, Software, Modules, Application Program Interface (API) etc.) that contains PII/PHI	Specifically list the PII/PHI Data Elements Sharing (Internally)
Corporate Database (CorpDB)	<div><ul style="list-style-type: none"><li>• Name</li><li>• Social Security Number</li><li>• Date of Birth</li><li>• Military History/Service Connection</li><li>• Flashes</li><li>• Stations of jurisdiction</li><li>• File Numbers</li><li>• Benefit Information</li><li>• Claims Decisions</li><li>• DD-212</li></ul></div>

<sup>9</sup> VA Directive 6508. Personally Identifiable Information (PII). A subcategory of VA Sensitive Data, PII means any information about the individual maintained by an agency, including but not limited to the following: (i) education, financial transactions, medical history, and criminal or employment history; (ii) Information that can be used to distinguish or trace the individual's identity, including name, social security number, date and place of birth, mother's maiden name, biometric records or any other personal information which is linked or linkable to an individual. This term can be interchanged with Sensitive Personal Information (SPI).

<b>Component Name (Database, Instances, Applications, Software, Modules, Application Program Interface (API) etc.) that contains PII/PHI</b>	<b>Specifically list the PII/PHI Data Elements Sharing (Internally)</b>

3.9b Internal VA Sharing: Examples include persons/administrations, system connections, or other sharing. Please refer to pages 13 and 14 of the [PTA Training Resources \(sharepoint.com\)](#) for guidance on completing the below table. [All PII/PHI data elements listed in this table must be listed in question 3.4 above. If PIA is required, the information in this table should match the information in question 4.1 of PIA]:

*Data Shared/Received Internally*

<b>Identify the internal system name, groups of persons, and/or VA program office (parties which data is shared sent or received)</b>	<b>List the specific PII/PHI data shared/received Internally</b>	<b>Method of Transmission<sup>10</sup></b>
Corporate Database (CorpDB)	<ul style="list-style-type: none"> <li>• Name</li> <li>• Social Security Number</li> <li>• Date of Birth</li> <li>• Military History/Service Connection</li> <li>• Flashes</li> <li>• Stations of jurisdiction</li> <li>• File Numbers</li> <li>• Benefit Information</li> <li>• Claims Decisions</li> <li>• DD-212</li> </ul>	Representational State Transfer (REST) over HTTPS using SSL encryption and certificate exchange
BGS (Benefit Gateway Services) SyncIdService/ SyncPersonService/ SyncClaimService	<ul style="list-style-type: none"> <li>• Social Security Number</li> <li>• File Number</li> <li>• Benefits Information</li> <li>• Claims Decisions</li> </ul>	Representational State Transfer (REST) over HTTPS using SSL Encryption and Certificate Exchange
External Consumer/ Consumer Utilization	<ul style="list-style-type: none"> <li>• Benefits Information</li> <li>• Claims Decisions</li> </ul>	Representational State Transfer (REST) over

<sup>10</sup> Method of Transmission - Site to Site (S2S), Internet Protocol Security (IPSEC) Tunnel, Secure Web- Portal, Secure Socket Layer (SSL)/Transport Layer Security (TLS), Bi-directional Health Information Exchange, Electronic Data Interchange (EDI), Secure fax, and verbal disclosure via telephone, etc.

Identify the internal system name, groups of persons, and/or VA program office (parties which data is shared sent or received)	List the specific PII/PHI data shared/received Internally	Method of Transmission <sup>10</sup>
		HTTPS using SSL Encryption and Certificate Exchange

3.10 Does the IT system or project connect, receive, or share PII/PHI with any other **external (outside of VA)** organization, IT system, third-party website, or application?

- ☒ No [If “No,” place “N/A” in the Table below]
- ☐ Yes [If yes, please explain in Table below]
- ☐ Yes, if yes, is this sharing covered by an existing information sharing agreement? *This could be a Memorandum of Understanding (MOU), Memorandum of Agreement (MOA), Business Associate Agreement (BAA) Letter of Intent (LOI), Information Exchange Agreement (IEA), etc.*

Please refer to page 14 of the [PTA Training Resources \(sharepoint.com\)](#) for guidance on completing the below table. [All PII/PHI data elements listed in this table must be listed in question 3.4 above. If PIA is required, the information in this table should match the information in question 5.1 of PIA]:

*Data Shared/Received Externally*

Identify the external system name, groups of persons, and/or organization program office (parties which data is shared sent or received)"	List the specific PII/PHI data shared/received Externally	Type of Connection	Agreement Type (Can be more than one)
N/A			

## Privacy Threshold Analysis Review

Must be completed by PIA Support (to Validate Finalization)

Date reviewed by VA PIA Support Analyst: 4/1/2025

Name of VA PIA Support Analyst: Bertha Okere-Ford

VA PIA Support Analyst Signature: \_\_\_\_\_

### DETERMINATION

#### Privacy Sensitive IT System or Project

- ☐ The IT system or project does not collect, process, retain or share PII/PHI information and is NOT privacy sensitive.
- ☒ The IT system or project IS privacy sensitive based on the responses provided above. Please see the comments below for additional privacy requirements for your IT system or project.

#### PIA SUPPORT ANALYST COMMENTS FOR PRIVACY SENSITIVE IT SYSTEMS/PROJECTS

##### Privacy Impact Assessment:

- ☐ a. This is a new IT system or project which collects, processes, retains or shares PII/PHI information and requires a new PIA within **90** days from last dated signature.
- ☒ b. Major changes have been made to an existing IT system or project and an updated PIA is required within **60** days of last dated signature.
- ☐ c. No major changes have been made to the existing IT system or project, and an updated PIA is required within 3 years of last dated signature on approved PIA: Click here to enter a date.
- ☐ d. No major changes but PIA needs to be updated to match the PTA.
- ☐ e. This IT system or project falls under the Rolodex Exception<sup>11</sup> and does not require a PIA.
- ☐ f. Other: *Click or tap here to enter text.*

##### Privacy Act System of Records Notice:

- ☒ a. A SORN is required for this IT system or project.
- ☐ b. A SORN needs to be created for this IT system or project.
- ☐ c. A SORN update is required for this IT system or project.
- ☐ d. A SORN is not required for this IT system or project.

##### Privacy Act (e)(3) statement:

- ☐ a. Is required for this IT system or project.
- ☒ b. Is not required for this IT system or project.

---

<sup>11</sup> [M-07-16 \(archives.gov\)](#)

**VA PIA SUPPORT ANALYST COMMENTS (continued)**

Additional Analyst Comments:

*The Data Synchronization is a privacy sensitive system that collects, maintains, and/or processes Personally Identifiable Information on Veterans and/or dependents. The system has undergone major changes since the last approved PIA from 5/31/2022. Therefore, a PIA update is required. This Privacy Threshold Analysis is approved upon arrival of the signed document.*

## Privacy Threshold Analysis Approval Signatures

Once the PO, ISSO, and ISO have signed the PTA, please return the PDF to the assigned VA PIA Analyst for their signature. Once the analyst has signed, they will return the final signed PTA back for uploading to eMASS. Please do not upload the PTA PDF copy to eMASS without the VA PIA Support Analyst's signature.

---

Privacy Officer Signature

---

Information System Security Officer Signature

---

Information System Owner Signature