Purpose and Scope

The Privacy Threshold Analysis (PTA) is a tool created by the VA Privacy Service and used by Privacy Officers, IT system owners, ISOs, and other stakeholders to determine the following:

1) Whether a Privacy Impact Assessment (PIA) is required under the E-Government Act of 2002.
2) There are no major changes to existing IT systems or projects with PIAs.

Please complete the PTA and forward to your assigned Privacy Officer for review. Upon completion of an initial review, the Privacy Officer will forward a copy to the VA Privacy Service for determination and documentation purposes.

1) If a PIA is necessary Privacy Officers, IT system owners, and ISOs will be added to the Annual PIA schedule and will be required to complete a PIA every 3 years until the IT system or project is decommissioned or the system undergoes major/new changes. You can download the most recent version of the PIA template at (http://vaww.oprm.va.gov/privacy/pia.aspx)

Date submitted for review: 7/24/2018

Name of the IT System: VistA Adaptive Maintenance (VAM)

Nam e of the Program Office: Enterprise Program Management Office (EPMO).

	Name	E-mail	Phone Number
Privacy Officer	Rita Grewal	Rita.grewal@va.gov	202-632-7861
Information Security Officer	Bobbi Begay	Bobbi.begay@va.gov	303-331-7837
System Owner	Dick Rickard	Dick.Rickard@va.gov	503-884-6178

SPECIFIC QUESTIONS

1. Status of project

   ☑ This is a new IT system

   ☐ This is a VIP (Veteran-focused Integration Process) system.
   Click here to enter the date the VIP system will be phased out.

   ☐ This IT system or project has an existing approved PIA

Click here to enter name of PIA   Click here to enter date approved.

☐ As part of the annual PTA validation process, there are major changes[1].

☐ As part of the annual PTA validation process there are no major changes.

☐ This project is a Patch to an IT system titled: Click here to enter text.
☐ This IT system or project is no longer operational as of: Click here to enter a date.

2. Please describe the purpose of the IT system, project or program in layman's terms so that a non-technical person can understand.

The VA VistA Adaptive Maintenance (VAM) is a Veteran-focused Integration Program (VIP) that provides a cloud-based roadmap and software for maintaining VistA and the VA workflows it supports in an efficient, cost-effective manner during the multi-year transition to VA's new commercial EHR. VAM enables VA to transition from 130 separate, complex, unmaintainable VistA systems to a single, secure, commercially-managed set of centralized cloud-based services - Veteran Integrated Care Services (VICS) - while maintaining full backwards-compatibility and continuity of care and workflows of the Computerized Patient Record System (CPRS). VAM will be hosted in production within the VA's Enterprise Cloud (VAEC) using Amazon Web Services (AWS).

3. Do you collect, process, or retain information on: (Check all that apply)
    ☑ Veterans or dependants

    ☑ VA Employees

    ☑ VA Contractors

    ☑ Members of the public

    ☑ Volunteers

    ☑ Clinical Trainees

    ☐ None of the above

4. Do you use or collect Social Security Numbers (SSNs)? If yes, please provide the function of the SSN within the project and the legal authority to use or collect it.

---

[1] 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.

☐No
☒Yes

Enter function of SSN and legal authority here;

The SSN may be used for patient medical care to include patient treatment services and procedures; volunteer, contractor and employee vehicle registration, job assignments, administrative support and personnel management. Executive Order 9397 allows Federal agencies to collect and use the SSN.

5. Does the IT system or project collect, maintain, or store PII information from any other IT systems in an identifiable form?
   ☐No
   ☒Yes
   If yes, please provide a specific description of information that might be collected, processed, or retained such as name, address, email, health information, financial information, biometrics, etc.

   The VAM system does not store any PII data in the current design that is the subject of the current ATO effort. However, VistA records will be accessed and processed by VAM users regarding Vitals, Allergy, and Problems and could be expected to potentially include the following data elements:

- Name
- Social Security Number
- Date of Birth
- Mother's Maiden Name
- Mailing Address
- Zip Code
- Phone Number(s)
- Fax Number
- Email Address
- Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- Financial Account Information
- Health Insurance Beneficiary Numbers/Account numbers
- Certificate/License numbers
- Vehicle License Plate Number
- Internet Protocol (IP) Address Numbers
- Current Medications
- Previous Medical Records
- Race/Ethnicity

- Gender
- Guardian name and contact information
- Next of kin name and contact information
- Military and service history
- Employment information
- Veteran dependent information
- Education information
- Research medical statistics
- Service connected rating and disabilities
- Criminal background information
- Date of death

6. Does the IT system or project collect, maintain, or store PII information from the Veterans /Individual? (i.e., information provided by the individual via web forms, surveys, VA forms, etc.)

   ☐No

   ☒Yes

   If yes, please provide a specific description of information that might be collected, processed, or retained such as name, address, email, health information, financial information, biometrics, etc.

   VAM users access and process veteran and individual PII data from VistA modules including Vitals, Allergy, and Problems. This processing may include entering PII data. However, no data is stored by VAM in the current design that is the subject of the current ATO.

7. Does the IT system or project connect, receive, or share information in identifiable form[2] or Personally Identifiable Information (PII)[3] with any other **internal** organization, IT system, website or application?

   ☐ No

   ☑ Yes

   If yes, please explain here: See Table below

---

[2] OMB Memorandum M-03-22 a. *Information in identifiable form*- is information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).

[3] 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).

Sample Database Table:

Server Name	Database Name that contain PII/PHI/SPI	Data Elements Sharing (Internally)
N/A	N/A	N/A

Sample Internal Organization, IT system, Third-Party website or Application:

Internal Organization Name	IT System Name	Data Elements	Method of Transmission
Veterans Health Administration	VistA (Regions 1-4)	System Log files, sample clinical data that may contain Protected Health Information (PHI) appropriate to the agreements. Veteran, veteran's primary contact and volunteer's service, medical, criminal record, guardian, education and benefit information may be collected as well as contractor and employee personnel and payroll records may be collected, processed and retained.	Electronically pulled from VistA thru Computerized Patient Record System (CPRS).

8. Does the IT system or project connect, receive, or share information in identifiable form[4] or Personally Identifiable Information (PII)[5] with any other **external (Outside of VA)** organization, IT system, third-party website or application?

    ☒No

---

[4] OMB Memorandum M-03-22 a. *Information in identifiable form-* is information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).

[5] 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).

☐Yes

If yes, please explain here: List external system name, data elements and ISA/MOUs/IEA/LOI as applicable for your System.

Sample Table

System Name	Data Elements
N/A	N/A

9. If information is shared with external (outside of VA) systems, is this sharing covered by an existing information sharing agreement? *This could be a Memorandum of Understanding (MOU), Memorandum of Agreement (MOA), Letter of Intent (LOI), Information Exchange Agreement (IEA), etc.*

☑ Not applicable

☐ Yes

Please describe applicable information sharing agreement, type of connection, and organization/Agency and system name in a table below.

Sample Table

System Name	External Organization or Agency Name	Type of Connection	Agreement Type (Can be more than one)
N/A	N/A	N/A	N/A

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

☐ Closed Circuit TV

☐ Sharepoint

☐ Social Media

6

☐ Mobile Applications

☐ Web Portal

☑ Cloud Computing

☐ None of the above

Privacy Threshold Analysis Review
(To be completed by the VA Privacy Service)

Date reviewed by Privacy Service Office: 8/24/2018

Name of Privacy Analyst:

Samuel Clark

DETERMINATION

☐ This is NOT a privacy sensitive IT system or project – The IT system/project contains no information in identifiable form or PII and does not require a Privacy Impact Assessment (PIA).

☐ PTA sufficient at this time

☑ This IS a privacy sensitive IT system or project

☑ A PIA is required

PRIVACY SERVICE COMMENTS

The Enterprise Program Management Office (EPMO) VistA Adaptive Maintenance (VAM) is a privacy sensitive system that collects PII/ PHI on individuals such as veterans and dependents, VA employees, VA contractors, members of the public, volunteers and clinical trainees. Due to the sensitive nature of this system a PIA is required at this time. This PTA is approved upon the signature of the Privacy Officer and System Owner below.

Privacy Officer Signature_____

Project Manager/
System Owner Signature_____