Privacy Impact Assessment for the VA IT System called:

Patient Engagement Tracking and Longterm Support (PETALS)

Health Services Research & Development

Veterans Health Administration

Date PIA submitted for review:

01/06/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Kim Murphy, Michelle Christiano	Kimberly.Murphy@va.gov; Michelle.Christiano@va.gov	781-331-3206
Information System Security Officer (ISSO)	Scott Miller, Stuart Chase	Scott.Miller@va.gov, Stuart.Chase@va.gov	215-600-9491, 410-340-2018
Information System Owner	Nicolle Marinec	Nicolle.Marinec@va.gov	708-471-2334

Abstract

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

The purpose of the Patient Engagement Tracking and Longterm Support (PETALS) system is to provide a resource for developing and implementing automated communication with veterans between face-to-face encounters with their clinical team. The system allows research investigators and clinicians to provide veterans with more frequent health monitoring and behavior change support.

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 IT system name is PETALS (Patient Engagement Tracking and Longterm Support). The name of the program office that owns the IT system is HSR&D (Health Services Research & Development).

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

The purpose of the system is to provide a resource for developing and implementing automated communication with veterans between face-to-face encounters with their clinical team. The system allows research investigators and clinicians to provide veterans with more frequent health monitoring and behavior change support.

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

HSR&D is the program office that owns the IT system.

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.

The expected number of individuals whose information is stored in the system is up to 5000 participant records. Only information from individuals that are participating in a health monitoring and behavior change support program on the system will be stored in the system.

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

Information in the IT system includes names, phone numbers, email address, year of birth, gender, audio or text messages, and health information (described in section 1.1). This information will be collected as part of an individual's participation in a health monitoring and behavior change support program.

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

Information sharing is conducted with only the necessary data in order for the health monitoring and behavior change support programs to function.

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 system may be used by users in more than one site. Validations and trainings will be used to ensure consistency across user sites.

3. Legal Authority and SORN

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

SORN 34VA10/86 FR 33015 Authority for Maintenance of the System: Title 38, United States Code, Section 7301. Routine use: 19.

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 SORN will not require an amendment or revision and approval as a result of this system. The SORN does cover cloud storage systems.

D. System Changes

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

The completion of this PIA would not result in circumstances that require changes to business processes.

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

The completion of this PIA would not result in 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)

SPI includes: audio or text messages (from Veterans and/or from research therapists/clinicians), and health information that is self-reported by Veterans. Health information that is self-reported by Veterans may include information related to their general health, chronic/acute diseases, treatments, medications, side effects, weight, blood sugar, blood pressure, pain and interference, step count, physical activity, sleep, mood, affect, depression, patient health questionnaire-9, stress, supports/relationships, headache, memory, confusion, concentration, balance, dizziness, appetite, fluid/food/salt/caffeine intake, alcohol/substance/tobacco use, cravings, shortness of breath, cough, sputum, inhaler use, fever, temperature, chest pain, nausea, vomiting, diarrhea, constipation, bowel movements/urine, swelling, neuropathy, skin rash/sensitivity/appearance/sweat, fatigue/energy/weakness, infections, allergies, senses, dry mouth, speech, libido, menses, lab readings, use of health services and resources, health behaviors, health care providers and self-management activities and confidence.

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

PII Mapping of Components (Servers/Database)

PETALS consists of 7 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 PETALS 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

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
Microsoft Azure SQL database	Yes	Yes	Names, phone numbers, email address, birth year, gender, audio or text messages, health information (described in section 1.1)	PII is stored and used when programs on the system contact participants.	PIV authentication for access. Authorized individuals who have completed/ approved user provisioning will have access. Encryption of data.

TRA	Yes	Yes	Names, phone numbers, email address, birth year, gender, audio or text messages, health information (described in section 1.1)	PII is needed for the programs on the system to contact participants.	PIV authentication for access. Authorized individuals who have completed/ approved user provisioning will have access. Encryption of data.
TCA	Yes	Yes	Names, phone numbers, email address, birth year, gender, audio or text messages, health information (described in section 1.1)	PII is needed for the programs on the system to contact participants.	PIV authentication for access. Authorized individuals who have completed/ approved user provisioning will have access. Encryption of data.
Microsoft Power Platform – Dynamics 365	Yes	Yes	Names, phone numbers, email address, birth year, gender, audio or text messages, health information (described in section 1.1)	PII is needed for participants to be enrolled into health monitoring and behavior change support programs on the system.	PIV authentication for access. Authorized individuals who have completed/ approved user provisioning will have access. Encryption of data.
CXP	Yes	No	Names, phone	PII is needed for the	Only authorized individuals will have

			numbers, email address, birth year, gender, audio or text messages, health information (described in section 1.1)	programs on the system to contact participants.	access. Authorized individuals who have completed/approved VA form 9957 (or equivalent) will have access. System administrators will grant access to approved individuals.
Prophecy	Yes	No	Names, phone numbers, email address, birth year, gender, audio or text messages, health information (described in section 1.1)	PII is needed for the programs on the system to contact participants.	Only authorized individuals will have access. Authorized individuals who have completed/approved VA form 9957 (or equivalent) will have access. System administrators will grant access to approved individuals.
Microsoft Azure SQL database	No	Yes	Names, phone numbers, email address, birth year, gender, audio or text messages, health information (described in section 1.1)	PII is stored and used when programs on the system contact participants.	Only authorized individuals will have access. Authorized individuals who have completed/approved VA form 9957 (or equivalent) will have access. System administrators will grant access to approved individuals.

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?

Authorized staff will enter the participants' information into the Microsoft Power Platform (Microsoft Dynamics 365) to enroll them into health monitoring/behavior change support programs on the system. Participants enrolled in a program will provide numeric/audio/text data collected through the participant's phone. Research therapists/clinician may provide audio/text feedback to participants.

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

The participants' enrollment information will be entered by authorized staff following approved research protocols.

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

The system may be a source of information as it may create scores based on participant responses.

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?

Information may be collected directly from an individual by authorized staff, or from VA investigators. Participants enrolled in a program may provide numeric/audio/text data collected via the participant's phone. Research therapists/clinician may provide audio/text feedback to participants.

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.

N/A

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.

The SPI is collected, maintained, and used in the system in order to provide health monitoring and behavior change support to participants, and to conduct research and data gathering for VA investigators. Authorized program staff will enter the participants' enrollment information into the system. Some, but not all, data fields used by staff to enter participant information will be restricted to certain values or formats to improve accuracy. The numeric telephone data may also be limited to accept certain values as valid to improve accuracy.

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.

N/A

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

SORN 34VA10/86 FR 33015 Authority for Maintenance of the System: Title 38, United States Code, Section 7301. Routine use: 19. The system allows research investigators and clinicians to provide veterans with more frequent health monitoring and behavior change support. Participants enrolled in a program may provide numeric/audio/text data collected via the participant's phone. Research therapists/clinician may provide audio/text feedback to participants.

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

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: Individuals enrolled in the system will be participating in health monitoring and behavior change support programs, and participating in research and data gathering conducted by VA investigators. Participant information is needed in order to be enrolled in the programs and conduct research. Risks include unauthorized access, misuse, and inaccurate data.

Mitigation: Only authorized individuals will have access to the system. Participant enrollment information will be entered into the system by authorized users. Some, but not all, data fields used by staff to enter participant information will be restricted to certain values or formats to improve accuracy. Participants enrolled in a program may provide numeric/audio/text data collected via the participant's phone. The numeric telephone data may also be limited to accept certain values as valid to improve accuracy. Research therapists/clinician may provide audio/text feedback to participants.

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.

Enter Major Application name here.

Name: Used to identify the individual
Date of birth (specifically and only birth year): Used as a pin to validate user during program engagement
Email address: Used to contact patient for program engagement
Personal Phone Number: Used to contact patient for program engagement
Gender: Used to tailor survey content for patient, when relevant
Other data elements : [general health, chronic/acute diseases, treatments, medications, side effects, weight, blood sugar, blood pressure, pain and interference, step count, physical activity, sleep, mood, affect, depression, patient health questionnaire-9, stress, supports/relationships, headache, memory, confusion, concentration, balance, dizziness, appetite, fluid/food/salt/caffeine intake, alcohol/substance/tobacco use, cravings, shortness of breath, cough, sputum, inhaler use, fever, temperature, chest pain, nausea, vomiting, diarrhea, constipation, bowel movements/urine, swelling, neuropathy, skin rash/sensitivity/appearance/sweat, fatigue/energy/weakness, infections, allergies, senses, dry mouth, speech, libido, menses, lab readings, use of health services and resources, health behaviors, health care providers and self-management activities and confidence]. Additionally, audio or text messages (from Veterans and/or from research therapists/clinicians): All elements are self-reported health information in the system will be used to support the participant as part of the health monitoring and behavior change support program in which they are enrolled. Information in the system will be used to support research and data gathering for VA investigators.

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.

Data scoring, comparisons, and other basic analytical tasks may be conducted.

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.

The new information will be stored in the system. The comparisons and tasks may result in various actions within the health monitoring and behavior change support program(s). Only authorized individuals will have access to the system.

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?

Data is stored within VA approved MAG / VAEC MAG / VA tenancy (Microsoft Power Platform – Dynamics 365). Information sharing between the components is conducted with only the necessary data in order for the health monitoring and behavior change support programs to function.

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

The system is not collecting, processing, or retaining SSNs.

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

Authorized users will be provided training as to the appropriate use of the system. Authorized users will only have access to areas of the system that are needed to conduct their duties. User access will be removed when their duties no longer require access.

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?

Authorized users will only have access to areas of the system that are needed to conduct their duties. User access will be removed when their duties no longer require access

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

User access criteria, procedures, controls, and responsibilities have been documented as part of the ATO process.

2.4c Does access require manager approval?

Access requires manager approval.

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

Access to PII is monitored, tracked, and recorded as part of user access protocols.

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

All authorized users are responsible for assuring safeguards for the PII. Authorized users will be provided training as to the appropriate use of the system.

Section 3. Retention of Information

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

*Identify and list all information collected from question 1.1 that is **retained** by the system. This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal*

The SPI gathered can include: name, personal phone number(s), personal email, year of birth, gender, audio or text messages (from Veterans and/or from research therapists/clinicians), and health information that is self-reported by Veterans. Health information that is self-reported by Veterans may include information related to their general health, chronic/acute diseases, treatments, medications, side effects, weight, blood sugar, blood pressure, pain and interference, step count, physical activity, sleep, mood, affect, depression, patient health questionnaire-9, stress, supports/relationships, headache, memory, confusion, concentration, balance, dizziness, appetite, fluid/food/salt/caffeine intake, alcohol/substance/tobacco use, cravings, shortness of breath, cough, sputum, inhaler use, fever, temperature, chest pain, nausea, vomiting, diarrhea, constipation, bowel movements/urine, swelling, neuropathy, skin rash/sensitivity/appearance/sweat, fatigue/energy/weakness, infections, allergies, senses, dry mouth, speech, libido, menses, lab readings, use of health services and resources, health behaviors, health care providers and self-management activities and confidence.

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.*

Data collected for each program in the system will be retained for the duration of the individual program, and retained as part of research records for the required period of 6 years, 3 months.

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.

Yes. See link to approved retention schedule: https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

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

Yes

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

Research records will be retained for the required period of at least 6 years, as defined by the Department of Veterans Affairs Records Control Schedule 10-1 (Item Number: 8300.6; Disposition Authority: DAA-0015-2015-0004, item 0032).

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.

Paper documents are destroyed to an unreadable state in accordance with the Department of Veterans' Affairs VA Directive 6371, (April 8, 2014), https://www.va.gov/vapubs. Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are sanitized in accordance with the Department of Veterans' Affairs Directive 6500. Electronic data files will be sanitized at the end of the required retention period in accordance with VA Policy in Directive 6500.

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 system is supporting research, so individuals enrolled in research programs on the system will have PII used for research. PII will not be used for system testing or training. Only authorized individuals will be accessing the system.

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.

Follow the format below:

Privacy Risk: The records will be retained for the duration required. The longer the length of data retention the greater the risk of unauthorized access or misuse.

Mitigation: The system retains only the information necessary for the duration of the individual programs and the required retention period for research records. Electronic data files will be deleted at the end of the required retention period in accordance with Directive 6500.

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***
VA Health Services Research and Development (HSR&D) / VA Investigators PETALS	To achieve the research protocol for research data analysis.	The data elements can include name, personal phone number(s), personal email, year of birth, gender, audio or text messages (from Veterans and/or from research therapists/clinicians), and health information that is self-reported by Veterans. Health information that is self-reported by Veterans may include information related to their general health, chronic/acute diseases, treatments, medications, side effects, weight, blood sugar, blood pressure, pain and interference, step count, physical activity, sleep, mood, affect, depression, patient health questionnaire-9, stress, supports/relationships, headache, memory, confusion, concentration, balance, dizziness, appetite, fluid/food/salt/caffeine intake, alcohol/substance/tobacco use, cravings, shortness of breath, cough, sputum, inhaler use, fever, temperature, chest pain, nausea, vomiting, diarrhea, constipation, bowel movements/urine, swelling, neuropathy, skin rash/sensitivity/appearance/sweat, fatigue/energy/weakness, infections, allergies, senses, dry mouth, speech, libido, menses, lab readings, use of health services and resources, health behaviors, health care providers and self-management activities and confidence.	Electronic, manual entry input and export

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*

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: The privacy risk includes the risk that the SPI is release to unauthorized individuals.

Mitigation: Only authorized users will have access to the system. Authorized users will only have access to the research projects that they are assigned to. User access will be reviewed by the system approval staff and will be removed when access is no longer needed.

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***
Tech4Research PETALS	The system has components in non-VAEC MAG and	The data elements can include name, personal phone number(s), personal email, year of birth, gender, audio or text messages (from Veterans and/or from research therapists/clinicians), and	SORN 34VA10/86 FR 33015 Authority for Maintenance	HTTPS Post, using SSL protocol

	VAEC MAG / VA tenancies. Limited dataset is sent between entities to facilitate research protocols.	health information that is self-reported by Veterans. Health information that is self-reported by Veterans may include information related to their general health, chronic/acute diseases, treatments, medications, side effects, weight, blood sugar, blood pressure, pain and interference, step count, physical activity, sleep, mood, affect, depression, patient health questionnaire-9, stress, supports/relationships, headache, memory, confusion, concentration, balance, dizziness, appetite, fluid/food/salt/caffeine intake, alcohol/substance/tobacco use, cravings, shortness of breath, cough, sputum, inhaler use, fever, temperature, chest pain, nausea, vomiting, diarrhea, constipation, bowel movements/urine, swelling, neuropathy, skin rash/sensitivity/appearance/sweat, fatigue/energy/weakness, infections, allergies, senses, dry mouth, speech, libido, menses, lab readings, use of health services and resources, health behaviors, health care providers and self-management activities and confidence.	of the System: Title 38, United States Code, Section 7301. Routine use: 19.	

5.2 <u>PRIVACY IMPACT ASSESSMENT: External sharing and disclosure</u>

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

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum Of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.
Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.
This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

Privacy Risk: Electronic data is shared in the system between the components on VAEC MAG and the components on non-VAECMAG. Risks include unauthorized access and misuse.

Mitigation: Only the necessary information for individuals to participate in a program will be shared. Since there are components on VAEC MAG and on non-VAEC MAG, information must be shared for the programs to function. There is a contract and MOU/ISA for the system.

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.

https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946VHA Handbook 1605.04: Notice of Privacy Practices

The collection of information by the system will be explained as part of the research program enrollment process. System staff may train individual program staff and provide assistance in troubleshooting. Program staff may contact individuals and confirm their interest in enrolling in a health monitoring and behavior change support program. Program staff may distribute a letter explaining the program and allow for sufficient time for individuals to decline participation.

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

Staff from individual programs using the system will provide notice as part of research enrollment procedures as required and approved by their research office and/or institutional review board providing oversight. A copy of the notices from the programs are not currently available.

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.

Notice provided as part of research enrollment procedures will be reviewed and approved by each project's research office and/or institutional review board providing oversight.

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.

Individuals will have the opportunity and right to decline participation in the program without penalty.

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.

Individuals will not have the right to consent to particular uses of the information. Individuals can choose to participate in the program or they can choose to decline participation.

6.4 <u>PRIVACY IMPACT ASSESSMENT: Notice</u>

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:

<u>Principle of Transparency:</u> Has sufficient notice been provided to the individual?

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

Privacy Risk: Risks include inadvertent enrollments on the system.

Mitigation: Individuals will be given sufficient time to decline participation in the program(s) to prevent any inadvertent enrollments on the system. Program staff may send notice to individuals via letter, or may contact individuals directly regarding program enrollment.

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.***

During the enrollment process, individuals will be given information on how to contact research program staff regarding their participation in the program. This process is determined by each individual research project. Additional information about the system and how to contact system staff can be found on the system website (https://www.annarbor.hsrd.research.va.gov/ANNARBORHSRDRESEARCH/PETALS.asp).

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).

FOIA requests will be coordinated with the FOIA Officer at the VA location in which the program's principal investigator is located or the VA study site. Research program staff and system staff will work together to provide information to the FOIA Officer.

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.

FOIA requests will be coordinated with the FOIA Officer at the VA location in which the program's principal investigator is located or the VA study site. Research program staff and system staff will work together to provide information to the FOIA Officer.

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.

Authorized program staff and system staff may correct inaccurate or erroneous information. Program staff can contact the system staff if they discover any inaccurate or erroneous information that needs to be corrected. Additional information about the system and how to contact sy
stem staff can be found on the system website (https://www.annarbor.hsrd.research.va.gov/ANNARBORHSRDRESEARCH/PETALS.asp).

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.

Individuals will be notified during enrollment to contact program staff via phone if their information needs to be updated. This contact information will be provided by each individual research project.

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.

Individuals may contact program staff to discuss corrections/updates to their information. Individuals will be notified during enrollment how to contact program staff via phone if their information needs to be updated. This contact information will be provided by each individual research project.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?
This question is related to privacy control IP-3, Redress.

Follow the format below:

Privacy Risk: Risks include inaccurate data reported by the participant.

Mitigation: During the enrollment process, individuals will be given information about the program and contact information for the program staff in case they have questions. Individuals will be able to contact program staff if corrections to the information reported is needed.

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.

Only authorized users will have access to the system. Users will complete a user access form (VA 9957 form, snow ticket, or equivalent) to request access to components in the system. Only authorized users will be given access to the system, and only to the areas related to their program/duties.

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?

Only users who have completed the requirements to access VA systems will be authorized to have access to the system.

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

Authorized users will have access to enter/modify information only in the areas related to their program/duties.

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.

VA contract employee access is verified through the Contracting Officer's Representative (COR) and other VA supervisory/administrative personnel before access is granted to any VA system. Contractor access is reviewed annually at a minimum. All contactors and employees will complete and sign a non-disclosure agreement (NDA) as appropriate. 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 Talent Management System (TMS). All contractors are vetted using the VA background investigation process and must obtain the appropriate level background investigation for their role. Contractors with systems administrative access are required to complete additional role-based training prior to gaining system administrator access. Generally, contracts are reviewed at the start of the initiation phase of acquisitions and again during procurement of option years by the Contracting Officer, Information Security Officer, Privacy Officer, COR, Procurement Requestor/Program Manager and any other stakeholders required for approval of the acquisition. Contracts generally have an average duration of 1-3 years and may have option years stipulated in the original contract.

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.

Authorized users are required to complete annual VA HIPAA training, VA Privacy and Information Security and Rules of behavior training via the VA Talent Management System (TMS).

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 6/29/2022
3. *The Authorization Status:* Authorization to Operate (ATO)
4. *The Authorization Date:* 9/27/2022
5. *The Authorization Termination Date:* 3/26/2023
6. *The Risk Review Completion Date:* 8/23/2022
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

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

N/A

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)*

Government Cloud – Microsoft Azure Government / VAEC MAG / VA tenancies (Microsoft Power Platform – Dynamics 365). Cloud SaaS, FedRAMP Package ID F1603087869.

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.*

In accordance with Microsoft ELA Contract GS-35F-0884P, the VA retains ownership of all information, including PII/PHI, throughout the entire Microsoft Azure Government environment and Microsoft Power Platform applications.

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.

Microsoft does not collect any ancillary data. All data used in Power Platform applications and within the MAG environment is owned by VA.

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.

Microsoft Azure Government and Microsoft Power Platform maintains compliance with all FedRAMP and VA security control requirements, to include all Privacy Overlay controls.

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).

Microsoft Power Automate utilizes RPA to create automated workflows via no-code and low-code interfaces and API's. https://powerautomate.microsoft.com/en-us/

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

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

Signature of Responsible Officials

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

Digitally signed by Kimberly E. Murphy 183320
Date: 2023.02.02 14:17:29 -05'00'

Privacy Officer, Kim Murphy

SCOTT MILLER

Digitally signed by SCOTT MILLER
Date: 2023.01.30 07:42:34 -05'00'

Information System Security Officer, Scott Miller

Nicolle Marinec

Digitally signed by Nicolle Marinec
Date: 2023.01.27 11:48:41 -08'00'

Information System Owner, Nicolle Marinec

APPENDIX A-6.1

Notice for the collection of information will be provided as part of research enrollment procedures as required and approved by each research project's research office and/or institutional review board providing oversight. VHA patients also receive a copy of the VHA Notice of Privacy Practices (NOPP).

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