Privacy Impact Assessment for the VA IT System called:

MedEx

Veterans Health Administration

Health Services- VISN 7 Healthcare Technology Management

eMASS ID # TBD

Date PIA submitted for review:

11/15/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	John Potter	John.potter@va.gov	(843) 614-1859
Information System Security Officer (ISSO)	Shionell Williams	Shionell.williams@va.gov	(205) 957-3882
Information System Owner	David Croall	David.Croall@va.gov	(681) 242-4094

Abstract

The abstract provides the simplest explanation for "what does the system do for VA?".

MedEx will serve as the face of VISN 7 to patients and guests. The system will be one of the primary forms of communication and engagement with our customers. The application can sync with the patient's appointment, remind, and notify them when they should leave for their appointment and navigate them to their site of care. The application has the ability to display targeted content, maintain an event calendar and send out notifications. The application can also link patients and guests to existing VA resources through APIs. Once onsite, the application has active wayfinding capabilities, giving turn by turn directions with blue dot map technology to its users. The VA facilities program in clinical care locations and other points of interest which are then routable through the application. The application also has the capability to send out surveys and questionnaires for immediate feedback from customers.

Overview

The overview is the most important section of the Privacy Impact Assessment (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. What is the business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?

VISN 7 Healthcare Technology Management will use MedEx system as the primary form of communication and engagement with their customers to navigate VISN 7.

B. Who is the owner or has control of the IT system or project? If the system has an eMASS entry, ensure this information matches with the eMASS entry.

MedEx is a SaaS that will be a VA Controlled.

2. Information Collection and Sharing

Indicate the expected number of individuals whose information is stored in the system and include a brief description of the typical client or affected individual?

250 VA Employee users to start with growth to the whole VISN 7 with 8 total medical centers. 250,000 of patient/veteran users.

Check if Applicable	Demographic of individuals
☒	Veterans or Dependents
☒	VA Employees
☐	Clinical Trainees
☐	VA Contractors
☐	Members of the Public/Individuals
☐	Volunteers

C. *What is a general description of the information in the IT system and the purpose for collecting this information?*

MedEx provides an improved patient experience for Veterans. MedEx allows Veterans to easily search and navigate to clinics and hospital amenities, using their mobile phones.
MedEx also provides appointment functionalities and other functionalities connected with EHR at the VA Authorization Boundary. MedEx collects information to provide the following functionalities to patients:

- Wayfinding
- View hospitals wait and access times
- Access to medical reports, records and results
- Appointment scheduling
- Smart reminders for appointments

MedEx collects the following general patient information for user information purposes:

- Name, surname
- Date of birth
- Gender
- Race

MedEx collects the following patient health information for providing improved patient experience:

- Appointments
- Medical Records
- Medications

MedEx collects the following organization information for providing general information about hospitals and departments:

- Hospital General Information
- Hospital Department Information

D. What information sharing is conducted by the IT system? A general description of the modules and components, where relevant, and their functions.

MedEx will improve communication between Veterans and hospitals. MedEx offers Veterans a simple way to locate healthcare providers, schedule appointments, access medical reports, and meet with physicians remotely. With MedEx, Veterans will be able to easily navigate to and through registered hospitals, stay informed with announcements/updates, receive reminders, and overall enjoy a seamless patient experience.

Appointments:
This module allows Veterans to view their appointment history and schedule appointments with registered hospitals and providers.

Medical Reports:
This module allows Veterans to access their medical reports/records.

Hospitals:
This module allows Veterans to view registered hospitals and providers.

Pill Reminder:
This module allows Veterans to set medication reminders to have the application remind them to take their medicine.

Emergency:
This module allows Veterans to select a hospital and view the fastest route, wait and access time. In addition, the Veteran can schedule an appointment and get directions both to and through the hospital.

Telehealth:
This module allows Veterans virtual healthcare. Veterans will be able to attend appointments with their physician via online video calls.

Doctors:
This module allows Veterans to choose a provider by reviewing a list of registered doctors. The list will include the doctors name, background and hospital in which they are located. Patients will be able to schedule appointments with doctors by simply selecting their name.

Lab Results:
This module allows Veterans to access their lab reports/results.

Radiology:
This module allows Veterans to access their radiology reports/results.

Water Reminder:
This module allows Veterans to set water drinking reminders to have the application remind them to drink water.

Announcements:
This module allows VA to push announcements out to patients.

MedEx provides the modules and functionalities using its components / submodules. MedEx has the following components below:

- VAAPP app database: holds the application configuration data, content management system and user data
- CDR database: holds the patient healthcare data
- API server: provides APIs to the applications
- Admin API server: provides administration APIs to admin portal
- Admin Portal: provides a management interface
- Integration Engine: provides integration channels to send and receive HL7, REST, SOAP data.

E. Are the modules/subsystems only applicable if information is shared?

The features require information share are as follows;

- Appointments
- Medical Reports
- Pill Reminder
- Lab Results
- Radiology

F. Is the system operated in more than one site to include primary and secondary 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?

MedEx will be used only in VISN 7.

3. Legal Authority and System of Record Notices (SORN)

G. What is the citation of the legal authority and SORN to operate the IT system?

The Privacy Act of 1974, as amended, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. The authority of maintenance of the system listed in question 1.1 falls under Title 28, United States Code, title 38, U.S.C., sections 501(a), 1705, 1710, 1722, and 5317.

VA Enterprise Cloud—Mobile Application Platform (Cloud) Assessing (VAEC–MAP) (173VA005OP2)
SORN -173VA005OP2

H. What is the SORN?

VA Enterprise Cloud—Mobile Application Platform (Cloud) Assessing (VAEC–MAP) (173VA005OP2)

I. SORN revisions/modification

There are not any SORN revisions/modifications.

H. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval.

SORN does not require amendments or revisions.

4. System Changes

I. Will the business processes change due to the information collection and sharing?

X Yes
☐ No
If yes, the features/modules would be disabled if the information collection and sharing is not allowed.

J. *Will the technology changes impact information collection and sharing?*

☐ Yes
X No
if yes, <<ADD ANSWER HERE>>

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 Information 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. It must also match the information provided in question 3.4 of the PTA.

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
☐ **Full** Social Security Number
☐ **Partial** 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[1]
☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☒ Medications
☐ Medical Records
☒ Race/Ethnicity
☐ Tax Identification Number

☒ Medical Record Number
☒ Gender/Sex
☐ Integrated Control Number (ICN)
☐ Military History/Service Connection
☐ Next of Kin
☐ Date of Death
☒ Business Email Address

☐ Electronic Data Interchange Personal Identifier (EDIPI)
☒ Other Data Elements (list below)

Other PII/PHI data elements: Doctor ID, Patient ID, Work Phone, Hospital Department, Title of Staff (Doctor Title), Appointment

1.2 List 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?

MedEx uses information received from the VA Electronic Medical Records.

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.

MedEx uses the information received from the VA EMR to provide patients with necessary information from the modules listed under MedEx platform, this data will be accessed by the patient only.

1.2c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?

MedEx does not create information.

1.3 Methods of information collection
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

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

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?

All data will be collected via MedEx integration engine. MedEx does not use any external data source rather than the VA systems via the agreed channels. The data will be transmitted using the standard HL7 messages and the predefined APIs if exists.

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

MedEx is not subjected to this section.

1.4 Information checks for accuracy, and 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.

MedEx will not perform any data changes from the user side. MedEx's source of the data will be the VA applications. The data will reflect what VA has for the patients in its own data sources.

1.4b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?

MedEx is not subjected to this section.

1.5 Identify the specific legal authorities, arrangements, and agreements that defined the collection of information.

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

The Privacy Act of 1974, as amended, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. The authority of maintenance of the system listed in question 1.1 falls under Title 28, United States Code, title 38, U.S.C., sections 501(a), 1705, 1710, 1722, and 5317.

VA Enterprise Cloud—Mobile Application Platform (Cloud) Assessing (VAEC–MAP) (173VA005OP2)

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

Principle of Minimization: The information is directly relevant and necessary to accomplish the specific purposes of the program.

Principle of Individual Participation: The program, to the extent possible and practical, collects information directly from the individual.

Principle of Data Quality and Integrity: VA policies and procedures must ensure that personally identifiable information is accurate, complete, and current.
This 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:

1. **Identity Theft:** Key identifiers like Social Security Number, Medical Record Number, and Personal Email Address can enable unauthorized individuals to impersonate the person, potentially accessing financial or healthcare services fraudulently.
2. **Medical Identity Theft:** Medications, Medical Records, and Medical Record Number allow impersonation in healthcare settings, potentially leading to incorrect medical treatment or billing fraud.
3. **Privacy Invasion**: Disclosure of sensitive information like Race/Ethnicity, Gender, Date of Birth, and Mother's Maiden Name can infringe on personal privacy and may lead to discrimination or profiling.

Mitigation:

1. **Data Encryption:** All sensitive data, both at rest and in transit encrypted to prevent unauthorized access even if data is intercepted or breached. Data collected, processed, and retained will be protected in accordance with VA Handbook 6500 and FIPS 140-2 encryption and data in-transit protection standards.
2. **Access Control:** Strict access control policies that only allow authorized personnel to access specific data elements based on necessity are implemented. All systems and individuals with access to the system will be approved, authorized, and authenticated before access is granted.
3. **Data Minimization and Masking:** Only necessary data stored and sensitive information is masked wherever full data visibility is not required.
4. **Training and Awareness**: Education of the employees on handling sensitive information, recognizing phishing attempts, and adhering to data security best practices.

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 that 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.

PII/PHI Data Element	Internal Use	External Use
Name	Used to display patient name on the application	Not used
Phone	Used to send appointment reminders to the patient phone number via SMS	Not used
Email	Used to send appointment reminders and announcements to the patients	Not used
Medical Record Number	Used in data exchange operations between MedEx and VA EHR systems such as booking appointment, etc.	Not used
Date of Birth	Used in data exchange operations between MedEx and VA EHR systems such as booking appointment, etc.	Not used
Hospital Department	Used in booking appointment	Not used
Title of Staff (Doctor Title)	Used to display patients for booking appointment	Not used
Appointment	Used to display patient appointments on the mobile application	Not used
Patient ID	This is usually MRN, if there is no MRN available on the EHR patient ID is used in data exchange operations between MedEx and VA EHR systems such as booking appointment, etc.	Not used
Doctor ID	Used in data exchange operations between MedEx and VA EHR systems for booking appointment	Not used

Work Phone Number	Used to display patients for booking appointment if applicable	Not used
Work Address	Used to display patients for booking appointment if applicable	Not used

2.2 Describe the types of tools 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?
MedEx does not apply any data analytics on the data that it holds or transfers. The data will be used to be displayed to the patients and no data will be used for any type of analysis.

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.
MedEx is not subjected to this section.

2.3 How the information in the system is 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?
MedEx's environment and infrastructure are hosted within Amazon Gov Cloud, so it inherits all the security roles and policies. MedEx protects the confidentiality and integrity of the information being transmitted by ensuring that TLS version 1.2 is encrypting all traffic from end to end, and that encrypted traffic is terminated on FIPS 140-2 validated endpoints. AWS protects the confidentiality and integrity of information being transmitted within the AWS managed infrastructure, including transmissions to external telecommunications services, which is documented in SC-8 and SC-9 of the AWS SSP.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs? (refer to PTA question 3.8).
MedEx does not collect or save SSNs. MedEx uses MedEx IDs for the patients and it will not be holding any information that identifies the patient.

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

1. **Data Minimization Strategy:** Only the minimum PII/PHI necessary for operations are collected used and retained.
2. **Access Control and Encryption:** Data collected, processed, and retained will be protected in accordance with VA Handbook 6500 and FIPS 140-2 encryption and data in-transit protection standards. All systems and individuals with access to the system will be approved, authorized, and authenticated before access is granted.
3. **Privacy Impact Assessments:** PIAs are conducted annually and for any major system changes.
4. **Training and Awareness:** VA annual privacy and security training compliance will be enforced for all VA employees, contractors, and vendors.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

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

2.4a How is access to the PII determined?

Access to PII is determined by a request through the ticketing system of MedEx, each request must contain a clear justification for the needed access and for how long. After checking the request and getting needed approvals, access could be provided in case of the justification is enough and the access should be provided based on the submitted request.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented? How are the documented, i.e. Policy, SOP, other. And where is this documentation located?

The criteria, procedures, controls and responsibilities documented in the SSP controls, and SSP attachments for policy and procedures.

2.4c Does access require manager approval?

Each access to the system requires manager approval using the ticketing system for MedEx.

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

All the access to MedEx infrastructure that holds PII is being monitored, tracked and recorded with MedEx SecOps monitoring tools.

2.4e Who is responsible for assuring safeguards for the PII as identified in eMASS?
MedEx Information Security Officer is responsible for assuring safeguards for the PII.

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
First and Last Name, Date of Birth, Personal Phone Number, Personal Email Address, Medication, Race/Ethnicity, Medical Record Number, Gender/Sex, Business Email Address, Doctor ID, Patient ID, Work Phone Number, Hospital Department, Title of Staff (Doctor Title), Appointment

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 https://www.archives.gov/records-mgmt/grs? This question is related to privacy control DM-2, Data Retention and Disposal.*

Records from this system that are needed for audit purposes will be disposed of 6 years after a user's account becomes inactive. Routine records will be disposed of when the agency determines they are no longer needed for administrative, legal, audit, or other operational purposes. These retention and disposal statements are pursuant to NARA General Records Schedules GRS 20, item 1c and GRS 24, item 6a.

3.3 The retention schedule 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. Please work with the system VA Records Officer to answer these questions.
This question is related to privacy control DM-2, Data Retention and Disposal.

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

Yes

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

Records from this system that are needed for audit purposes will be disposed of 6 years after a user's account becomes inactive. Routine records will be disposed of when the agency determines they are no longer needed for administrative, legal, audit, or other operational purposes. These retention and disposal statements are pursuant to NARA General Records Schedules GRS 20, item 1c and GRS 24, item 6a.

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.
There are no paper records in the MedEx system.

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.

MedEx does not use any PII for testing, training and research. There are pre-defined anonymous data in the system for testing and training. For further testing, training and research capabilities it is going to be required from the related integration endpoints to have data in the same concept.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System Privacy Officer (PO) 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:

Principle of Minimization: *The project retains only the information necessary for its purpose, additionally, the PII is retained only for as long as necessary and relevant to fulfill the specified purposes.*

Principle of Data Quality and Integrity: *The PIA should describe 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:

1. **Exposure to Unauthorized Access:** The longer data is retained, the more time there is for unauthorized parties to access it, either through accidental exposure or malicious attacks. Legacy data may not be as actively monitored or protected as newer data, leading to potential vulnerabilities.
2. **Data Breach Possibility:** Outdated or rarely accessed data may lack up-to-date security measures, increasing the chances of breaches, especially if it is stored in less secure or legacy systems.
3. **Compliance Risks:** Retaining data beyond required timeframes can lead to legal consequences, fines, and reputational damage in cases of non-compliance.
4. **Data Integrity and Quality Issues:** Retaining outdated data can lead to incorrect or suboptimal decision-making if the data is used operationally.

Mitigation:

1. **Data Retention Policies:** The system has data retention policies in order to retain related data.
2. **Automated Data Deletion:** The system automatically deletes the data on the databases subject to retention period.
3. Regular Data Audits: Annually audits are planned to identify data that is eligible for deletion or archiving. During audits, assess the accuracy and integrity of retained data, removing or updating information that is outdated or inaccurate.
4. **Access Control and Encryption for Retained Data:** Data collected, processed, and retained will be protected in accordance with VA Handbook 6500 and FIPS 140-2 encryption and data in-transit protection standards. All systems and individuals with access to the system will be approved, authorized, and authenticated before access is granted.
5. **Data Anonymization:** For data that must be retained for analytical or historical purposes, consider de-identifying or anonymizing it to reduce privacy risks.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

PII Mapping of Components

4.1a **MedEx** consists of **3** key components (servers/databases/instances/applications/software/application programming interfaces (API)). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **MedEx** 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 server names in the table. The first table of 3.9a in the PTA should be used to answer this question.

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	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
MXAPP	**Yes**	**Yes**	• Name • Phone • Personal/VA Email • Medical Records	**Providing user information**	**FIPS 140-2 cryptography applied to specific table and table row where such data is encrypted**
MXCDR	**Yes**	**Yes**	• Name • Phone • Personal/VA Email • Date of Birth • Medical Record Number	**Providing patient information**	**FIPS 140-2 cryptography applied to specific table and table row where such data is encrypted**
MedEx Application	**Yes**	**No**	• Name • Medical Record Number	**Exchanging related healthcare data /**	**FIPS 140-2 cryptography applied to specific table and table**

				medical records	**row where such data is encrypted**

4.1b List internal organizations information is shared/received/transmitted, the information shared/received/transmitted, and the purpose, and how the information is transmitted.

NOTE: Question 3.9b (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

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
EHR (Electronic Health Record) System	We use this as patient identification so it can get the necessary information through the integration with the VA EHR.	• First name • Last name • Email • Phone Number • Hospital Department • Title • Scheduling- Appointment • Patient ID • Doctor ID • Prescription/Medication	• HTTPS • TCP

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the VA network 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 in this section.).

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

Follow the format below:

Privacy Risk:

1. **Unauthorized Access or Misuse of Information:** As data is shared internally, it becomes accessible to more individuals, increasing the risk that someone without a legitimate need might view or misuse it.
2. **Inconsistent Data Security Practices Across Teams:** Different teams or systems may have varying levels of security and privacy protocols. When PII/PHI moves between them, it might be exposed to environments with weaker controls, leading to increased risk of unauthorized disclosure.
3. **Inadequate Tracking and Monitoring of Shared Data:** When data is shared internally, tracking who accessed it and for what purpose can be challenging, making it difficult to detect unauthorized use or disclosure.

Mitigation:

1. **Role-Based Access Controls (RBAC):** The system has RBAC for the data access.
2. **Data Access Monitoring and Audit Logs:** The access of the data is monitored and the logs are saved for audit.
3. **Security and Privacy Training:** VA annual privacy and security training compliance will be enforced for all VA employees, contractors, and vendors.
4. **Data Minimization and Purpose Limitation:** Data in transit and at rest are minimized to mitigate the risks. Also, the system is not sharing the data without its functional boundaries.

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 List the external organizations (outside VA) that information shared/received. and information shared/received, and the purpose, and how the information transmitted and what measures are taken to ensure it is secure.

The sharing of information outside the agency must be compatible with the original collection. The sharing must be covered by an appropriate routine use in a SORN. If not covered, 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 IT System or External Program Office information is shared/received with	***List the purpose of information being shared / received / transmitted***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)***	***List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
N/A	N/A	N/A	N/A	N/A

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

If no External Sharing listed on the table above, ***(State there is no external sharing in both the risk and mitigation fields).***

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.
Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.

This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

Privacy Risk: There is not any external sharing.

Mitigation: There is not any external sharing.

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 The notice provided to the individual before collection of the information. Please provide a copy and/or screen shot of a web notice of the notice as an Appendix-A 6.1 on the last page of the document. (A notice may include a posted privacy policy, a Privacy Act notice on forms, notice given to individuals by the sources system, or a system of records notice published in the Federal Register.) If notice was not provided, explain why.

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 Provide the Privacy Notice provided to the public by this system or any source systems. Include a copy of the notice in Appendix A of the PIA, the Federal Register citation, or Privacy Statement from collection of information such as forms or surveys.
System of Records Notice SORN is clear about the use of the information, specifically SORN - 173VA005OP2. This PIA also serves as public notice that VA data will be collected in this system.

6.1b If notice was not provided, explain why.
The mobile application has a dedicated Privacy Policy page to provide adequate notice to individuals whose information is being collected, promoting transparency and trust in the data collection and usage process.

6.1c Provide how the notice provided at the time of collection meets the purpose of use for this system.
The notice provided at the time of data collection clearly states the purpose of collecting personal information, aligning with the purpose outlined in SORN -173VA005OP2. Individuals are informed that their data will be used to support the operational functions and will only be disclosed as necessary to fulfill these functions. This notice also includes information on how their data will be protected and the rights they have concerning their data, ensuring full transparency and alignment with the stated purpose of the system.

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.
Only the information of the individuals who would like to use the system are provided to the system. The individuals who delete their account, their data is retained and destroyed regarding the related policies.

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.
MedEx system does not collect PII/PHI information directly from VA employees.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

Principle of Transparency: This is referring to sufficient notice provided to the individual.

Principle of Use Limitation: The information used only for the purpose for which notice was provided either directly to the individual or through a public notice. The procedures in place must 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:

1. **Lack of Informed Consent:** Without clear notice, individuals may not be fully informed about the purpose, scope, and intended uses of their data. This can result in a lack of informed consent, where individuals unknowingly provide sensitive information without understanding its implications.
2. **Increased Risk of Privacy Complaints and Legal Liability:** Failure to provide sufficient notice can result in privacy complaints or legal challenges. Individuals who feel their data was collected or used without their understanding or consent may file formal complaints or lawsuits.
3. **Non-Compliance with Privacy Regulations:** Insufficient notice may lead to non-compliance with privacy laws such as the Privacy Act, which mandates that individuals are informed about data collection practices.

Mitigation:

1. **Clear and Accessible Privacy Notices:** All privacy notices are reviewed and updated regularly to ensure they clearly articulate what information is being collected, why it's necessary, how it will be used, and any third parties it may be shared with.
2. **Standardized System of Records Notice (SORN):** SORNs are required to be reviewed regularly to confirm they are up-to-date and accurately reflect the VA data practices.
3. **Training and Awareness:** VA annual privacy and security training compliance will be enforced for all VA employees, contractors, and vendors.
4. **Feedback Mechanisms for Individuals:** Individuals are able to provide feedback using the support e-mail.

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 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 VA Public Access Link-Home (efoia-host.com) to obtain information about FOIA points of contact and information about agency FOIA processes.***

As described in SORN 173VA005OP2, individuals seeking information regarding access to and contesting of records in this system may write the Director of VA Connected Health, VHA Office of Informatics and Analytics, Department of Veterans Affairs, 810 Vermont Avenue NW, Washington, DC 20420. Inquiries should, at a minimum, include the person's full name, social security number, type of information requested or contested, their return address, and phone number.

7.1b If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR)?
The system is not exempt.

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?
The system is a Privacy Act system.

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.

As described in SORN 173VA005OP2, individuals seeking information regarding access to and contesting of records in this system may write the Director of VA Connected Health, VHA Office of Informatics and Analytics, Department of Veterans Affairs, 810 Vermont Avenue NW, Washington, DC 20420. Inquiries should, at a minimum, include the person's full name, social security number, type of information requested or contested, their return address, and phone number.

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.

As described in SORN 173VA005OP2, individuals seeking information regarding access to and contesting of records in this system may write the Director of VA Connected Health, VHA Office of Informatics and Analytics, Department of Veterans Affairs, 810 Vermont Avenue NW, Washington, DC 20420. Inquiries should, at a minimum, include the person's full name, social security number, type of information requested or contested, their return address, and phone number.

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.
Forma redress is provided.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

Principle of Individual Participation: The individual must be provided with the ability to find out whether a project maintains a record relating to them.

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

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

Follow the format below:

Privacy Risk: The Department's access, redress, and correction policies are essential for maintaining data accuracy and supporting individuals' privacy rights. Potential risks associated with these policies include data inaccuracy, lack of transparency, legal non-compliance, and challenges to program integrity for sensitive data (e.g., law enforcement records).

Mitigation: To mitigate these risks, MedEx has implemented role-based access controls. The individuals are able to provide feedback for correction requests. VA annual privacy and security training compliance will be enforced for all VA employees, contractors, and vendors.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures. (Work with your ISSO to complete this section).

8.1 The procedures in place to determine which users may access the system, must be 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?
The patients can access the system if using the SSO or ID systems of the VA. There is no additional grant access is required by design.

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?
Users from other agencies will not 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.

User Access (An access to create records such as appointments) – Users (Patients)
Edit Access – Admins (VA Staff)

Read Only Access – Technical Support
Limited Read Only Access (An access to read only limited data) – User Support

8.2a. Will VA contractors have access to the system and the PII?

VA contractors will not have access to the MedEx system.

8.2b. What involvement will contractors have with the design and maintenance of the system?

VA contractors will not have access to the MedEx system.

8.2c. Does the contractor have a signed confidentiality agreement?

VA contractors will not have access to the MedEx system.

8.2d. Does the contractor have an implemented Business Associate Agreement for applicable PHI?

VA contractors will not have access to the MedEx system.

8.2e. Does the contractor have a signed non-Disclosure Agreement in place?
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 contractors will not have access to the MedEx system.

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.
The MedEx team provides general training and guidelines to users on how to maintain their privacy. The team ensures role-based training is completed before information system users are permitted access to an information system or able to perform assigned duties which require access to PII. The Technical Lead of MedEx has developed, documented, and disseminated to the Problem Manager this Security Awareness and Training Procedure to facilitate the implementation of FedRAMP Security Awareness and Training control requirements. The Technical Lead of MedEx reviews and updates the Security Awareness and Training Procedures at least annually, when there is a change to Medrics Corp./MedEx operations that impact applicable security controls, and as needed when any other significant change occurs which may impact these procedures. This procedure covers all Medrics Corp. information and information systems used, managed, and/or operated by a contractor,

agency, or organization on behalf of the Medrics Corp. In addition, this procedure applies to all Medrics Corp. employees, contractors, and users of Medrics Corp. information and information systems that support the operation and assets of Medrics Corp.

8.4 The Authorization and Accreditation (A&A) completed for the system.

8.4a If Yes, provide:

1. *The Security Plan Status:* <<ADD ANSWER HERE>>
2. *The System Security Plan Status Date:* <<ADD ANSWER HERE>>
3. *The Authorization Status:* <<ADD ANSWER HERE>>
4. *The Authorization Date:* <<ADD ANSWER HERE>>
5. *The Authorization Termination Date:* <<ADD ANSWER HERE>>
6. *The Risk Review Completion Date:* <<ADD ANSWER HERE>>
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* <<ADD ANSWER HERE>>

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

8.4b If No or In Process, provide your ***Initial Operating Capability (IOC) date.***
MedEx request is currently in the SaaS intake Process and has not received an Authority to Operate (ATO)

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. ***(Refer to question 1.8 of the PTA)***

This system is a Software as a Service (SaaS) that uses cloud technology. There is no current agency authorization or FedRAMP Authorization for the solution, but it is currently in process of pursuing a VA-Sponsored FedRAMP Authorization. The system has a current data security categorization of **Moderate** from VA's Digital Transformation Center. Both a PIA and PTA have been completed and approved by the VA Privacy Office.

9.2 Does the contract with the Hosting 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 3.3.1*

of the PTA) *This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

The Cloud Service Provider is under contract with the VA and contract is awarded. Contract questions can be directed to Business Owner Lucas Marsh. Contract # NNG15SD26B 36C10B21F0352.

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.

MedEx system produces logs in its environment, but it doesn't include any PII metadata. The mentioned log, ancillary data belongs to MedEx.

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.

Medrics is under contract as the cloud provider and has provided documentation for implementing security controls including what they are responsible vs. what the VA is responsible for related to the security and privacy of data held by Medrics in the MedEx system.

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).

MedEx is not utilizing Robotics Process Automation (RPA)

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

ID	Privacy Controls
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.

JOHN POTTER

Digitally signed by JOHN POTTER
Date: 2024.12.17 09:53:36 -05'00'

Privacy Officer, John Potter

SHIONELL WILLIAMS

Digitally signed by SHIONELL WILLIAMS
Date: 2024.12.17 09:22:33 -06'00'

Information System Security Officer, Shionell Williams

DAVID CROALL

Digitally signed by DAVID CROALL
Date: 2024.12.19 09:33:56 -05'00'

Information System Owner, David Croall

APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy; a Privacy Act notice on forms; screen shot of a website collection privacy notice).

HELPFUL LINKS:

Records Control Schedule 10-1 (va.gov)

General Records Schedule
https://www.archives.gov/records-mgmt/grs.html

National Archives (Federal Records Management):
https://www.archives.gov/records-mgmt/grs

VA Publications:
https://www.va.gov/vapubs/

VA Privacy Service Privacy Hub:
https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):
VHA Directive 1605.04
IB 10-163p (va.gov)