



Privacy Impact Assessment for the VA IT System called:

# Medication Possession Information for Clinicians (MedPIC)

## Lighthouse Product Engineering Veterans Health Administration

Date PIA submitted for review:

9/14/2022

System Contacts:

*System Contacts*

	Name	E-mail	Phone Number
Privacy Officer	Phillip Cauthers	<i>Phillip.Cauthers@va.gov</i>	(503)-721-1037
Information System Security Officer (ISSO)	Andrew Vilailack	Andrew.Vilailack@va.gov	(813) 970-7568
Information System Owner	Andrew Fichter	Andrew.Fichter@va.gov	(240) 274-4459

## Abstract

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

Medication Possession Information for Clinicians (MedPIC) is a standards-based (utilizing Substitutable Medical Applications and Reusable Technologies (SMART) on Fast Healthcare Interoperability Resources (FHIR)) web application that will be accessible from within the electronic health record and will provide an overview of a patient’s medication possession information and adherence trends over time. This application utilizes an existing technical infrastructure to interact with electronic health record data, launch from within the electronic health record, authenticate users, maintain appropriate security, and other capabilities. This technical infrastructure constitutes a clinical decision support platform that is used to quickly launch applications within the electronic health record and assist physicians with rapidly responding to future healthcare emergencies.

## 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:*

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *Indicate the ownership or control of the IT system or project.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *A general description of the information in the IT system and the purpose for collecting this information.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *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.*
- *A citation of the legal authority to operate the IT system.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*
- *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?*

Medication Possession Information for Clinicians (MedPIC) is owned by VA OIT and is being developed in collaboration with the Lighthouse Product Engineering (PE) program.

Version Date: October 1, 2021

Page 1 of 26

MedPIC will help clinicians to administer a high standard of care by reducing cognitive load when reviewing patients' medications. It will also help clinicians to work more efficiently by assisting with managing and acting upon the high volumes of data clinicians must work with amidst the current shortcomings of the existing Electronic Health Record. MedPIC will also support the Lighthouse Continuous Risk Management Framework (cRMF) effort by being the first application to achieve Ongoing Authorization.

MedPIC is owned by the Lighthouse organization in the VA Office of Information Technology. Individuals' information will not be stored by MedPIC.

MedPIC will access patients' electronic health record data (patient name, date of birth, social security number, sex assigned at birth, and medications) in order to fetch and display medication possession information and adherence trends from the past year. No data will be stored in the system and no decisions or predictions will be made on behalf of the patient. It is purely a read only tool to aid clinicians during patient visits.

MedPIC does not share any data. All data is retrieved from VistA through the Lighthouse Clinical Health API.

This system will be used in multiple VA Medical Centers. The same controls will be used across all sites. MedPIC is a standards-based (utilizing Substitutable Medical Applications and Reusable Technologies (SMART) on Fast Healthcare Interoperability Resources (FHIR)) web application, and it is through use of these standards that consistency of the PII accessed by the system will be maintained.

Authority for the maintenance of the system: Title 38, United States Code, section 7301(a).

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

The completion of this PIA will not result in technology changes.

The SORNs do not require amendment. The system uses cloud technology and falls under the following SORN information: Patient Medical Record-VA, SORN 24VA10A7

<https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf>, and Veterans Health Information Systems and Technology Architecture (VistA) Records –VA, SORN 79VA10/85 FR 84114 (<https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf>)

## 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:

- |   |   |   |
|---|---|---|
| <input checked="" type="checkbox"/> Name            | <input type="checkbox"/> Health Insurance               | <input checked="" type="checkbox"/> Integration Control |
| <input checked="" type="checkbox"/> Social Security | <input type="checkbox"/> Beneficiary Numbers            | <input type="checkbox"/> Number (ICN)                   |
| Number  | <input type="checkbox"/> Account numbers                | <input type="checkbox"/> Military                       |
| <input checked="" type="checkbox"/> Date of Birth   | <input type="checkbox"/> Certificate/License            | <input type="checkbox"/> History/Service                |
| <input type="checkbox"/> Mother's Maiden Name       | numbers   | <input type="checkbox"/> Connection                     |
| <input type="checkbox"/> Personal Mailing           | <input type="checkbox"/> Vehicle License Plate          | <input type="checkbox"/> Next of Kin                    |
| Address   | Number  | <input type="checkbox"/> Other Unique                   |
| <input type="checkbox"/> Personal Phone             | <input type="checkbox"/> Internet Protocol (IP)         | <input type="checkbox"/> Identifying Information        |
| Number(s)   | <input type="checkbox"/> Address Numbers                | (list below)  |
| <input type="checkbox"/> Personal Fax Number        | <input checked="" type="checkbox"/> Current Medications |   |
| <input type="checkbox"/> Personal Email             | <input checked="" type="checkbox"/> Previous Medical    |   |
| Address   | Records   |   |
| <input type="checkbox"/> Emergency Contact          | <input type="checkbox"/> Race/Ethnicity                 |   |
| Information (Name, Phone                            | <input type="checkbox"/> Tax Identification             |   |
| Number, etc. of a different                         | Number  |   |
| individual)   | <input type="checkbox"/> Medical Record                 |   |
| <input type="checkbox"/> Financial Account          | Number  |   |
| Information   | <input checked="" type="checkbox"/> Gender              |   |

### PII Mapping of Components

MedPIC consists of 0 key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by MedPIC and the reasons for the collection of the PII are in the table below.

### PII Mapped to Components

**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.**

#### PII Mapped to Components

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

### 1.2 What are the sources of the information in the system?

*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?*

*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 1.3 indicate why the system is using this source of data.*

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

*This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.*

The information is collected from the electronic health record stored in VistA. Some of this information has been provided by the individual in the past while other information is gathered from the individual's medical history within the VA. The system uses this information to help clinicians identify a patient and provide them with medication information to aid with treatment plans and patient visits.

### 1.3 How is the information collected?

*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 technology used in the storage or transmission of information in identifiable form?*

*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.*

*This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.*

Information is collected through an Clinical Health API over encrypted HTTPS connection.

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

*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.*

*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.*

*This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.*

All information in the system is checked for accuracy within VistA and is never modified. Clinical practitioners review the information as part of routine patient visits. Additionally, clinicians will not use MedPIC as their sole source of information for making medication-related decisions.

#### **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*

Patient Medical Records-VA, SORN 24VA10A7 / 85 FR 62406

<https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf>

Authority for maintenance of the system: Title 38, United States Code, Sections 501(b) and 304.

Version Date: October 1, 2021

Page 5 of 26

Veterans Health Information Systems and Technology Architecture (VistA) Records –VA, SORN 79VA10 / 85 FR 84114 (<https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf>) Authority for maintenance of the system: Title 38, United States Code, section 7301(a).

### **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.*

*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:** MedPIC accesses and displays PII and PHI. As a result, privacy concerns could arise if this information were breached or exposed to an unauthorized user including personal and/or emotional harm to the impacted individuals.

**Mitigation:** MedPIC only displays information necessary to assist clinicians with developing a better understanding of a patient’s medication possession information and adherence trends. The application can only be accessed by authorized clinicians and launched via the existing Electronic Health Record (CPRS). MedPIC does not display any PII or PHI not already shown within CPRS, nor does it publish information to any external sources. If a link to the application were to fall into the wrong hands, the unauthorized user would get a 404 error page and not be able to view any data including PII or PHI. As a result, the primary risk would be an unauthorized user getting access to a clinician’s VA workstation which is a concern with or without MedPIC being open on the screen.

## 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.*

MedPIC displays patient information and medication history with the goal of reducing cognitive load for clinicians when reviewing medications during patient visits. The existing User Interface within the Electronic Health Record (CPRS) requires clinicians to do mental math and read from a challenging list in order to get an accurate mental picture of a patient's medication possession information and adherence trends. MedPIC uses the same information but displays it in a more easily understood way to help clinicians. The application does not make any decisions on behalf of the clinician or patient nor does it write any changes back to CPRS or VistA. It purely acts as an informational tool to assist clinicians. The PII and PHI included are solely for ensuring the clinician can properly identify the patient and also view the necessary medication information.

### **2.2 What types of tools are used to analyze data and what type of data may be produced?**

*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.*

*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.*

*This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information*

MedPIC is a data visualization application, so it collects medication information and displays it to a clinician in a graphical format. The application does not make any complex calculations in the backend, it simply displays data that clinicians could find elsewhere in different formats. The application is read-only so no changes can be made in the UI and nothing gets written back to the electronic health record.



## 2.3 How is the information in the system secured?

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

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

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

*This question is related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest*

Access is restricted to authorized VA personnel who already have access to the underlying VistA/CPRS data. If a user tries to access the application via direct URL or bookmarked link they will get a 404 error, even if they are authorized to launch the application via CPRS. This prevents any unauthorized users from ever stumbling upon the application. SSNs are encrypted in the header of the API calls we make which adds an additional layer of protection for sensitive information.

## **2.4 PRIVACY IMPACT ASSESSMENT: Use of the information. How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?**

*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.*

Add answer here:

MedPIC utilizes SSOi for authentication. Only clinicians with access to the patients' records within the electronic health record (CPRS) are authorized to launch our application. If a new user wanted to view MedPIC they would need to follow the same steps a VA healthcare professional would follow to get access to CPRS.

## 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*

No data is retained in MedPIC.

### 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. If the system is using cloud technology, will it be following the NARA approved retention length and schedule?*

*The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented. This question is related to privacy control DM-2, Data Retention and Disposal.*

MedPIC does not retain any data.

### 3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so please indicate the name of the records retention schedule.

*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.*

MedPIC does not retain any data.

### 3.4 What are the procedures for the elimination of SPI?

*Explain how records are destroyed or eliminated at the end of the 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*

MedPIC does not retain any data.

### **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. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?*

*This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research*

MedPIC uses synthetic data in all lower environments that does not contain any PII. MedPIC does not use PII for research, testing, or training.

### **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.*

*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: 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?*

*Principle of Data Quality and Integrity: 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:** N/A – MedPIC does not retain any data – it displays view only data received from Clinical Health API to authorized users.

**Mitigation:** N/A – MedPIC does not retain any data - it displays view only data received from Clinical Health API to authorized users.

## 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.*

<i>List the Program Office or IT System information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</i>	<i>Describe the method of transmittal</i>
Veterans Health Administration (VHA) - Lighthouse Clinical Health API	Clinical Health API acts as source of data for MedPIC to provide VA clinicians with information about a patient's medication possession information and adherence trends	Patient Names, DOB, Prescriptions and refills, Provider name, MRN, Address	REST API

**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.*

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

Follow the format below:

**Privacy Risk:** The only privacy risk of sharing data within the VA is the chance for an unauthorized user to view sensitive data.

**Mitigation:** As of now the only way an unauthorized user could view MedPIC would be via direct access to a clinician's VA workstation that has been left unattended with PII on the screen. Workstations are designed to maximize physical security and access to logs is limited to personnel with proper permissions.

**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*

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

## **5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure**

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

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

*Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.*

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

Follow the format below:

**Privacy Risk:** MedPIC does not share/receive data with external systems

**Mitigation:** MedPIC does not share/receive data with external systems

## **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 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?**

*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. If notice was provided in the Federal Register, provide the citation.*

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

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

MedPIC does not retain data. All data displayed is in a read-only format and is information that previously exists in the patient's electronic health record. Nothing gets written back to the electronic health record.

The VA Notice of Privacy Practice (NOPP) IB 10-163, [https://www.va.gov/files/2022-02/Notice\\_of\\_Privacy\\_Practices\\_IB\\_10-163.pdf](https://www.va.gov/files/2022-02/Notice_of_Privacy_Practices_IB_10-163.pdf) is a document which explains the collection and use of protected information to individuals applying for VHA benefits. Major changes are mailed out every three years to all VHA beneficiaries. Employees and contractors are required to review, sign and abide by the National Rules of Behavior on an annual basis.

The Department of Veterans Affairs provides additional notice of this system by publishing two System of Record Notices (SORNs):

1)The VA System of Record Notice (SORN) Patient Medical Records-VA, SORN 24VA10A7, in the Federal Register and online. An online copy of the SORN can be found at: <https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf>.

2)The VA System of Record Notice (SORN) Veterans Health Information System and Technology Architecture (VISTA) -VA, SORN 79VA10, in the Federal Register and online. An online copy of the SORN can be found at: <https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf>

This Privacy Impact Assessment (PIA) also serves as notice of the Enterprise VistA System. As required by the eGovernment Act of 2002, Pub.L. 107-347 §208(b)(1)(B)(iii), the Department of Veterans Affairs “after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means.”

**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*

MedPIC does not collect or retain any data hence this question does not apply.

**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*

MedPIC does not collect or retain any data hence this question does not apply.

#### **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.*

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

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

*Principle of Use Limitation:* *Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?*

*This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use*

Follow the format below:

**Privacy Risk:** There is a risk that an individual may not receive notice that their information is being collected, maintained, processed, or disseminated by the Veterans' Health Administration and the local facilities prior to providing the information to the VHA.

**Mitigation:** This risk is mitigated by the common practice of providing the VA Notice of Privacy Practices (NOPP) when Veterans apply for benefits. Employees and contractors are required to review, sign and abide by the National Rules of Behavior on a yearly basis as required by VA Handbook 6500 as well as complete annual mandatory Information Security and Privacy Awareness training. Additional mitigation is provided by making the System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) available for review online, as discussed in question 6.1.

## **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?**

*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.*

*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).*

*If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information. This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.*

MedPIC does not retain data. There are several ways a veteran or other beneficiary may access information about them. The Department of Veterans' Affairs has created the MyHealthEVet program to allow online access to their medical records. More information on this program and how to sign up to participate can be found online at <https://www.myhealth.va.gov/index.html>. Veterans and other individuals may also request copies of their medical records and other records containing personal data from the Release of Information (ROI) office at the facility where they are treated. VHA Directive 1605.01, Privacy and Release of Information, Paragraph 7 outlines policy and procedures for VHA and its staff to provide individuals with access to and copies of their PII in compliance with the Privacy Act and HIPAA Privacy Rule requirements. VHA also created VA form 10-5345a for use by individuals in requesting copies of their health information under right of access. VA Form 10-5345a is voluntary but does provide an easy way for individual to request their records.

## **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.*

MedPIC does not collect or retain any data hence this question does not apply.

## **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.*

MedPIC does not collect or retain any data hence this question does not apply.

#### **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.*

*This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.*

*Example: Some projects allow users to directly access and correct/update their information online. This helps ensure data accuracy.*

MedPIC does not collect or retain any data hence this question does not apply.

#### **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.*

*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:** There is a risk that a Veteran does not know how to obtain access to their records or how to request corrections to their records and that the health record could contain inaccurate information and subsequently effect the care the Veteran(s) receive.

**Mitigation:** As discussed in question 7.3, the Notice of Privacy Practice (NOPP), is provided to all enrolled Veterans which discusses the process for requesting an amendment to ones' records. The VHA staffs Release of Information (ROI) offices at facilities to assist Veterans with obtaining access to their medical records and other records containing personal information. The Veterans' Health Administration (VHA) established MyHealthVet program to provide Veterans remote access to their medical records. The Veteran must enroll to obtain access to all the available features. In addition, Directive 1605.01 Privacy and Release of Information establishes procedures for Veterans to have their records amended where appropriate.

## 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?**

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

*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?*

*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.*

*This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.*

The VA has established policies and procedures for the identification and authorization of VistA/CPRS users. MedPIC follows these previously established mechanisms. No user can be authorized to view MedPIC without having permission to view the patient's electronic health record in CPRS.

### **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 contractors that have access to MedPIC are only able to view non-production data. Development environments contain no PII/PHI. Contractors with access to application logs have all undergone HIPAA and Privacy training and can only access logs on approved government platforms.

### **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.*

Personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA National ROB or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training which all personnel must complete via the VA's Talent Management System (TMS). After the user's initial acceptance of the ROB, the user must re-affirm their acceptance annually as part of the security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system. System administrators are required to complete additional role-based training. Users with access to PHI are required to complete HIPAA privacy training annually.

- PRIVACY AND HIPPA TRAINING
- VA PRIVACY & VA INFORMATION SECURITY

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

*If Yes, provide:*

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

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

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

Conditional ATO was granted on 4/25/22 for a period of 180 days. We expect to achieve ongoing authorization by 6/30/22. The system is classified as Moderate.

## 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).*

*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.*

The system uses VA Enterprise Cloud (VAEC)

### 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)

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

N/A - The system uses VA Enterprise Cloud (VAEC)

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

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

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

N/A - The system uses VA Enterprise Cloud (VAEC)

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

*What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met?*

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

N/A - The system uses VA Enterprise Cloud (VAEC)

**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).*

MedPIC does not utilize Robotics Process Automation (RPA) hence this question does not apply.

## Section 10. References

### Summary of Privacy Controls by Family

*Summary of Privacy Controls by Family*

<b>ID</b>	<b>Privacy Controls</b>
<b>AP</b>	<b>Authority and Purpose</b>
AP-1	Authority to Collect
AP-2	Purpose Specification
<b>AR</b>	<b>Accountability, Audit, and Risk Management</b>
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
<b>DI</b>	<b>Data Quality and Integrity</b>
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
<b>DM</b>	<b>Data Minimization and Retention</b>
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
<b>IP</b>	<b>Individual Participation and Redress</b>
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
<b>SE</b>	<b>Security</b>
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
<b>TR</b>	<b>Transparency</b>
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
<b>UL</b>	<b>Use Limitation</b>



<b>ID</b>	<b>Privacy Controls</b>
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

**Signature of Responsible Officials**

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

---

**Privacy Officer, Phillip Cauthers**

---

**Information System Security Officer, Andrew Vilailack**

---

**Information System Owner, Andrew Fichter**

## APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy, a Privacy Act notice on forms).

The VA System of Record Notice (SORN) Patient Medical Records-VA,  
<https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf>

The VA System of Record Notice (SORN) Veterans Health Information System and Technology Architecture (VISTA), <https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf>

VA Notice of Privacy Practices IB 10-163, [https://www.va.gov/files/2022-02/Notice\\_of\\_Privacy\\_Practices\\_IB\\_10-163.pdf](https://www.va.gov/files/2022-02/Notice_of_Privacy_Practices_IB_10-163.pdf)