Privacy Impact Assessment for the VA IT System called:

CirrusMD Virtual Health Chat for Government -E

Veteran Health Administration

Patient Care Services and Connected Care

2212

Date PIA submitted for review:

10/7/2024.

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Kimberly Murphy	Kimberly.Murphy@va.gov	781-331-3206
Information System Security Officer (ISSO)	Karen McQuaid	Karen.McQuaid@va.gov	708-724-2761
Information System Owner	Scottie Ross	Scottie.Ross@va.gov	(478) 595-1349

Abstract

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

CirrusMD Virtual Health Chat for Government -E provides VA with a Veteran clinical chat capability to increase the efficiency, capacity, and response time for clinical care for our Veterans.

CirrusMD Virtual Health Chat for Government -E Chat will enable Veterans access to a VA physician (or other VA staff member) who can provide immediate care or help to guide the Veteran to the right point of care. The solution will allow Veterans to connect via secure chat messaging using their mobile device or computer.

Veterans will access the online chat capabilities using a VAMC-approved mobile application. Veterans will use their own personal devices to access this system via a web application. Veterans will be required to sign on to the CirrusMD Virtual Health Chat for Government -E Chat platform using an approved VA credential as part of the Single Sign On External (SSOe) service. The existing VA credentials approved for use are DS Logon, MyHealtheVet and ID.me. Eligibility for VA healthcare will be confirmed using the VA Enrollment Application Programming Interface (API).

VA staff will access the CirrusMD Virtual Health Chat for Government -E platform using their VA credential and the Single Sign-On Internal (SSOi) service. Staff will directly access the CirrusMD Virtual Health Chat for Government -E interface using the platform provided by the vendor.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

1 General Description

A. What is the IT system name and the name of the program office that owns the IT system?

System Name (as per eMASS):
CirrusMD Virtual Health Chat for Government -E

Program Office that owns the IT System:
Patient Care Services and Connected Care

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

The **CirrusMD Virtual Health Chat for Government -E** platform is designed to offer accessible, real-time healthcare services for veterans by enabling secure communication between veterans and VA healthcare providers or staff. This service ensures that veterans can receive immediate care or appropriate guidance toward the right point of care, enhancing the efficiency and timeliness of healthcare delivery.

Veterans can access the system using **VAMC-approved mobile applications** or web-based platforms on personal devices. Authentication is managed through the **Single Sign-On External (SSOe)** service, utilizing approved VA credentials like **DS Logon, MyHealtheVet,** and **ID.me**. The system verifies healthcare eligibility via the **VA Enrollment API** and ensures secure data management through compliance with FedRAMP controls.

The **business purpose** aligns with the **VHA Office of Connected Care's mission** by promoting **veteran-centric care** through innovative and accessible technologies. The system directly supports the VA's mission of enhancing public welfare by improving healthcare outcomes, streamlining services, and safeguarding personal data through secure digital interactions.

C. *Who is the owner or control of the IT system or project?*

The CirrusMD Virtual Health Chat for Government -E Chat platform is a software-as-a-service (SaaS) hosted and maintained by a third-party vendor. The CirrusMD Virtual Health Chat for Government -E Chat product is sponsored by VHA Office of Connected Care and hosted in Amazon cloud service. All information sent to/from is via a VA Network and Security Operations Center (NSOC) approved, encrypted site-2-site Virtual Private Network (VPN) tunnel, Trusted Internet Connections (TIC) across which approved connections to VA-internal systems are established. The data ownership belongs to the Veteran, per the user agreement with the CirrusMD Virtual Health Chat for Government -E Chat. The OIT Project, Special Forces office, will assist with implementing and securing the SaaS.

2. Information Collection and Sharing

D. *What is the expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual?*

The CirrusMD Virtual Health Chat for Government -E Chat Platform pilot will be primarily fielded at two VA Medical Centers (VAMCs) with a total population of approximately 150,000 Veterans, and will provide VA with an initial proof of concept to demonstrate efficacy of the solution. The targeted initial Veteran population will allow the VA to monitor success based on defined metrics, including Veteran engagement and satisfaction with the platform.

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

The CirrusMD Virtual Health Chat for Government -E Chat for Government system manages sensitive information, including **Personally Identifiable Information (PII)** and **Protected Health Information (PHI)**, collected to support healthcare services and communication. This information includes patient identifiers, medical history, health-related data, and administrative records, ensuring efficient care delivery and communication between healthcare providers and patients.

The primary purpose of collecting this information is to facilitate secure and seamless virtual healthcare interactions, enabling the delivery of government-affiliated healthcare services. It allows real-time communication for consultations, health monitoring, and patient support. Additionally, the system ensures the proper management of user data through compliance with privacy standards like FedRAMP and HIPAA, safeguarding the confidentiality, integrity, and availability of critical healthcare data.

VA staff will access the **CirrusMD Virtual Health Chat for Government -E platform** using their **VA credentials** through the **Single Sign-On Internal (SSOi)** service. Staff will also directly engage with the CirrusMD Virtual Health Chat for Government -E interface through the **platform provided by the vendor**, ensuring seamless integration with existing VA systems and enhancing operational efficiency.

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

The **CirrusMD Virtual Health Chat for Government -E system** securely manages the sharing of **PII and PHI** through integration with several VA systems and services, using **predefined security controls** to maintain data confidentiality, integrity, and availability.

1. **Single Sign-On External (SSOe):**
   - ○ Purpose: Verify user identity and manage authentication for veterans accessing the platform.
   - ○ Data Shared: Name, Phone Number, Email Address, Date of Birth, Social Security Number (SSN).
   - ○ Method of Transmission: Encrypted electronic communication using FedRAMP-authorized services.
2. **Master Veteran Index (MVI):**
   - ○ Purpose: Validate and synchronize veteran identity across VA systems to ensure consistency in records.
   - ○ Data Shared: Name, Date of Birth, Integrated Control Number (ICN).
3. **VA Enrollment API:**
   - ○ Purpose: Confirm eligibility for healthcare services.

  - ○ Data Shared: Veteran’s enrollment status and eligibility indicators.
  - ○ Transmission: Secure API requests between systems over encrypted channels.

The system **does not directly share PII/PHI externally** with non-VA systems or third parties. However, it ensures that **all external system connections** such as through **AWS-hosted services** adhere to **FedRAMP compliance**, ensuring secure data handling.

- **AWS Services Used:**
  - **S3 for Data Storage**: Encrypted storage and categorized management of encounter records.
  - **Security Groups & TLS Certificates**: Secure transmission protocols for all communications between internal VA systems.
  - **SentinelOne**: Monitors system files to ensure they are free from malicious content.

In cases of **cross-domain data transfers**, metadata attributes and discrete security policies are employed to control the flow and prevent unauthorized access. Each transfer or sharing of data is validated against **organizational security policies**, and all access is logged for compliance monitoring and auditing purposes.

G. If 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?

Yes, the CirrusMD Virtual Health Chat for Government -E system is operated across multiple sites, including the AWS East and West regions. The system uses availability zones in these regions, allowing the system to switch to another region or availability zone if there is an issue at the primary site. The same controls are implemented across all sites to ensure consistency, including security measures and operational procedures. In case of a disaster, failover and recovery processes are implemented to minimize impact and ensure the continuity of services. The system also maintains backup data and configuration files at AWS, following standardized procedures across sites.

3. Legal Authority and SORN

H. What is the citation of the legal authority to operate the IT system?

The **CirrusMD Virtual Health Chat for Government -E** operates under the following legal authorities:

- **Public Law 114-31**
- **Title 38, U.S. Code**: Sections **5106, 5107, 5701, and 8111**
  - Section 8111: "Sharing of Department of Veterans Affairs and Department of Defense Health Care Resources"
- **Title 10, U.S. Code, Section 1104**: "Sharing of Resources with the Department of Veterans Affairs"

- **Title 31, U.S. Code, Section 1535**: Known as the **Economy Act**, covering "Agency Agreements"
- **E-Government Act of 2002** (44 U.S.C. §208(b))
- **38 U.S.C. §5706**

The system is covered under **VA SORN #168VA005**, titled **Health Information Exchange-VA**. This SORN outlines the conditions for collecting, maintaining, and sharing the personal data of veterans. It ensures compliance with federal regulations concerning the use of **PII** and **PHI**, supporting secure operations and safeguarding the privacy of the individuals whose data is managed by the system.

I. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?

The **CirrusMD Virtual Health Chat for Government -E** system is covered under **SORN #168VA005 Health Information Exchange-VA**. This SORN governs the collection, storage, and sharing of PII and PHI, ensuring compliance with federal guidelines and privacy policies, including cloud usage and storage.

- **Cloud Technology Usage**: Yes, the system utilizes **cloud technology** (hosted on AWS), and the existing SORN covers cloud usage and storage. This ensures all data stored and transmitted through the cloud is handled in accordance with VA's privacy and security policies.
- **SORN Amendment or Revision**: No amendments or revisions to the SORN are required at this time, as the system's current operations align with the provisions outlined under **SORN 168VA005 Health Information Exchange-VA**. If future modifications necessitate changes to how PII or PHI is managed, an amendment will be submitted for approval.

4. System Changes

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

No Changes in the business process will result from this PIA completion.

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

No Changes in the technology changes will result from this PIA completion.

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. 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
☒ 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
☐ Integrated Control Number (ICN)
☐Military History/Service Connection
☐ Next of Kin
☒ Other Data Elements (list below)

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

Veterans or Dependents

- Full Name
- Email Address
- SSN
- Gender
- Phone number
- VA ID
- DOB
- Primary site of care
- Audio recording
- Video recording
- Photographic recording
- Encounter video/transcript – this is a longitudinal record of the Veterans' conversation on the app
- Health information notes (summary of the encounter) in CPRS

VA Employees

- Full Name
- Email Address
- VA ID
- Site ID

PII Mapping of Components (Servers/Database)

CirrusMD Virtual Health Chat for Government -E consists of 1 (one) key component (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 CirrusMD Virtual Health Chat for Government -E 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 3.9 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
va-production1-app1.c5vwoxeb4xlr.us-east1.rds.amazonaws.com	**Yes**	**Yes**	Full Name, Social Security Number, email address, phone number, DOB, zip code, SSN, audio/video/photographic recording(s) of encounter.	Required to connect users with healthcare providers	Hosted in AWS Cloud, with controlled physical and logical access, only approved and authorized users are granted access to the application.

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

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.2a List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

In addition to information directly entered by users, the CirrusMD Virtual Health Chat for Government -E system collects data from the following **external sources**:

1. **Master Veteran Index (MVI)**: Provides identity verification by matching user input (e.g., name, DOB) with VA records to ensure consistency and accuracy across VA systems.
2. **Authentication Providers**:
    - **ID.me, MyHealtheVet,** and **DS Logon** supply authentication data through the **Single Sign-On External (SSOe)** service, facilitating secure access.
3. **VA Enrollment API**: Confirms healthcare eligibility for veterans, preventing unauthorized access.
4. **Other VA Systems**: Data from existing medical records and service records may be referenced to provide necessary medical history or continuity of care during interactions on the platform.

These sources ensure the platform delivers seamless service by validating user information, managing identity, and confirming eligibility without requiring duplicate data entry from veterans. This approach minimizes errors, ensures data integrity, and enhances operational efficiency.

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.

> Information from sources other than the individual is required for several reasons. The CirrusMD Virtual Health Chat for Government -E system may use data from third-party sources such as commercial aggregators or external systems. These data sources are necessary to enhance system functionality, provide authentication services, or verify the integrity and accuracy of the information being used or shared. For example, identity verification services might be used to ensure that individuals accessing the system meet certain security criteria or to provide multifactor authentication. These sources allow VA CirrusMD Virtual Health Chat for Government -E to validate user identities, particularly when sensitive information like PII or PHI is involved, ensuring compliance with privacy and security regulations. Data from commercial providers can supplement internal data to enhance the system's security posture, reducing risks associated with fraud, data manipulation, or unauthorized access.

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

> Yes, the CirrusMD Virtual Health Chat for Government -E system creates information such as audit reports and analysis. These reports are generated through its integration with tools like Splunk Cloud, which provides log aggregation, audit review, and analysis capabilities. These processes help detect suspicious activities, support investigations, and ensure compliance. Additionally, summary reports for audit review are generated on a regular basis to maintain situational awareness across different system components, particularly in the AWS environment. This information is used by security teams and system administrators to respond promptly to security events.

1.3 How is the information collected?

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.3a This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technologies used in the storage or transmission of information in identifiable form?

In addition to **user-entered information**, the CirrusMD Virtual Health Chat for Government -E system also collects data from the following **external sources**:

1. **Master Veteran Index (MVI)**: Used to validate veteran identity and synchronize records across VA systems.
2. **Authentication Providers**:
   - **ID.me**, **MyHealtheVet**, and **DS Logon** provide authentication data for Single Sign-On External (SSOe), ensuring that only authorized individuals access the system.
3. **VA Enrollment API**: Confirms eligibility for VA healthcare services, ensuring that only eligible veterans can utilize the platform.

This information is transmitted securely using encrypted channels, and it integrates seamlessly with the platform to authenticate users, verify eligibility, and maintain continuity of care within the VA healthcare ecosystem. This ensures compliance with data integrity and privacy requirements while minimizing user input redundancy.

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?

No information is being collected on a form.

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

These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

The purpose of CirrusMD Virtual Health Chat for Government -E receiving the information is to verify Veteran identity and provide data to VA Single Sign-on system for authenticating user to access the CirrusMD Virtual Health Chat for Government -E.

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?

This system does not use a commercial aggerate to check for accuracy.

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

The **legal authorities** that permit the collection and use of information for CirrusMD Virtual Health Chat for Government -E include the following:

- **Public Law 114-31**
- **Title 38, U.S. Code, Sections 5106, 5107, and 5701**: These sections govern the use and sharing of veteran information between agencies to support care coordination.
- **Title 38, U.S. Code, Section 8111**: Authorizes the sharing of healthcare resources between the VA and the Department of Defense.
- **Title 10, U.S. Code, Section 1104**: Governs resource-sharing agreements with the VA, aligning with Title 31, U.S. Code, Section 1535 (Economy Act) on agency agreements.
- **E-Government Act of 2002 (44 U.S.C. §208(b))**

Additionally, the system aligns with **VA SORN #168VA005 Health Information Exchange-VA** System of Records Notice, which covers the use, collection, and disclosure of personal information stored and managed by the platform. This ensures compliance with privacy regulations and proper data handling across all integrated systems.

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: 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: Data collected by the CirrusMD Virtual Health Chat for Government -E application contains PII, and other sensitive information. Due to the sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious harm or even identity theft may result in a significant financial burden to address impact of stolen identity.

Mitigation: CirrusMD Virtual Health Chat for Government -E ensures strict access to information by enforcing thorough access control and requirements for end users. All roles in CirrusMD Virtual

Health Chat for Government -E will be managed by system administrators and undergo a documented approval process. Access to VA, CirrusMD Virtual Health Chat for Government -E will be limited to authorized users of the system and will have appropriate credentials for authentication. As part of the access management activities, the highest level of assurance for providing identity along with multi-factor authentication will be used. Additionally, the system will log access and activity.

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 as an identifier	Not used
Social Security Number (SSN)	Used as an identifier	Not used
Date of Birth (DOB)	Used as an identifier	Not used
Phone Number	Used for identity verification and communication	Not used
Personal Email Address	Used to contact individuals	Not used
Medical Record Number	Used as an identifier for healthcare purposes	Not used
Medications	Used to reference medical history during consultations	Not used
Integrated Control Number (ICN)	Used to manage interactions across VA systems	Not used
Mailing Address	Used to contact the individual	Not used

2.2 What types of tools are used to analyze data and what type of data may be produced?
These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis?

This system does not process or analyze the data submitted. The data provided is used to produce the identity management information needed to verify identity and authenticate users for accessing CirrusMD Virtual Health Chat for Government -E.

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.

> When CirrusMD Virtual Health Chat for Government -E creates or derives new information about an individual, such as system activity or behavioral patterns, it is typically used to enhance the system's functionality or ensure compliance with security protocols. If new information is generated (such as audit logs or security alerts), it may be added to the individual's existing record or associated with their account profile within the system. This derived data is used primarily for security monitoring, risk assessment, and ensuring compliance with organizational policies. In some cases, such as a change in security status or observed suspicious behavior, a new record may be created (such as a security incident report), and actions may be taken to either limit or expand access based on the findings. This derived information is accessible only to authorized personnel, such as system administrators, security officers, or managers, who use this information to make determinations about system access, security controls, or corrective actions. In cases where actions are necessary (e.g., disabling an account), the decision is made following the organization's incident response and access control policies, ensuring that derived information is used only under appropriate circumstances and by authorized personnel.

2.3 How is the information in the system secured?

These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

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

CirrusMD Virtual Health Chat for Government -E adheres to National Institutes of Standards and Technology (NIST) Special Publication 800-83, and VA 6500 directives in order to protect the confidentiality, integrity, and availability of the information processed, stored and transmitted. The security-related areas include: access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; system and information integrity; and privacy.

Access to the system is governed by a need to know. All those with access have been trained in Privacy and Information Security and have signed Rules of Behavior.

All data in transit and at rest is encrypted using FIP 140-2 validated encryption.

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

Yes, all SSNs are encrypted in transit and at rest.

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

PII/PHI is safeguarded by least privileged access. Access to PII/PHI is protected by Role Based Access Controls integrated with multi-factor authentication in accordance with NIST SP 800-63A AAL2.

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?

User profiles are currently private; Practice Partners profiles are visible on the respective practice page along with name, work email address, job title, and profile picture (optional). CirrusMD Virtual Health Chat for Government -E adheres to National Institutes of Standards and Technology (NIST) Special Publication 800- 83, and VA 6500 directives in order to protect confidentiality, integrity and availability of the information processed, stored and transmitted. The security-related areas include access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; system and information integrity; and privacy. Access to the system is governed by a need to know. All those with access have been trained in Privacy and Information Security and have signed Rules of Behavior.

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

Yes, In the CirrusMD Virtual Health Chat for Government -E System Security Plan, Policies and Procedures

2.4c Does access require manager approval?

All access the CirrusMD Virtual Health Chat for Government -E System requires VA-specific onboarding process, as necessary for the specific roles and responsibilities: prerequisite skills and knowledge, background investigations, professional/technical certifications, security and privacy awareness training, and occasionally security clearances.

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

The CirrusMD Virtual Health Chat for Government -E system logs all system activity and creates audit reports for analysis, tracking, and after-the-fact investigation. This is implemented using log integration with tools like Splunk Cloud, which provides log aggregation, audit review, and analysis capabilities. These processes help detect suspicious activities, support investigations, and ensure compliance. Additionally, summary reports for audit review are generated on a regular basis to maintain situational awareness across different system components, particularly in the AWS environment. This information is used by security teams and system administrators to respond promptly to security events.

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

CirrusMD Virtual Health Chat for Government -E will be using multi-factor authentication mechanism through MyhealthVet DSLogon and ID.me to allow users internal to the VA to access the system (e.g., using Personal Identity Verification (PIV). Server-level access will be managed and granted to developers on an as-needed basis by the CirrusMD Virtual Health Chat for Government -E Information Security Officer (ISO). We will be limiting access to only a small set of trusted developers approved to work with and diagnose production issues. Secure Shell (SSH) access will be logged and monitored.

Access to the system is governed by a need to know. All those with access have been trained in Privacy and Information Security, and have signed Rules of Behavior

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*

- **Personal Identifiers:**
  - Name
  - Social Security Number (SSN)
  - Date of Birth (DOB)
  - Integrated Control Number (ICN)
  - Medical Record Number
  - Gender
- **Contact Information:**
  - Phone Number
  - Email Address
  - Mailing Address (if collected)
- **Health Information:**
  - Medications
  - Medical Records
  - Encounter Records (including transcripts or video recordings of communication)
- **Service Information:**
  - Military History/Service Connection (if applicable)

The system retains this information temporarily as part of the **user session** to support **identity verification and authentication**. The data submitted during chat sessions is retained for **up to 60 days** to allow for follow-ups, audit trails, and communication continuity. After this period, the information is securely deleted, adhering to **VA's data retention policies** and ensuring **compliance** with relevant privacy controls.

3.2 How long is information retained?

In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. ***The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.*** *If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

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.

This question is related to privacy control DM-2, Data Retention and Disposal.

> VA Directive 6000.2. Electronic Health Record (EHR) communicates that CirrusMD Virtual Health Chat for Government -E shall retain the Veterans information for 75 years (beyond the death of Veteran), in accordance with VA retention policy of medical records.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)?

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner. Please work with the system Privacy Officer and 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, **CirrusMD Virtual Health Chat for Government -E** is classified as a system of record and adheres to the approved **System of Records Notice (SORN) #168VA005 Health Information Exchange-VA**. All records stored in this system align with the **VA's approved disposition authorities** for medical and health-related records.

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

Per **VA Directive 6000.2 (Electronic Health Record Retention Policy)**, the system retains veterans' information for **75 years beyond the death of the veteran**. This retention schedule complies with the VA’s **medical record retention policy**, ensuring that all health records and associated data are properly maintained and disposed of according to federal regulations.

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.

All data cached/stored by CirrusMD Virtual Health Chat for Government -E is deleted upon reaching the deletion timeframes as specified in 3.2.
CirrusMD Virtual Health Chat for Government -E operates on time-based deletion rules that programmatically triggers a clean-up script. This is in accordance with VA Handbook 6500, Data Minimization and Retention, which states VA has requested CirrusMD Virtual Health Chat for Government -E retain the Veterans information for 75 years (beyond the death of Veteran), in accordance with VA retention policy of medical records.

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.

CirrusMD Virtual Health Chat for Government -E provides security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users, when required by system changes, and at least annually thereafter via the VA OIT Talent Management System (TMS). CirrusMD Virtual Health Chat for Government -E does NOT use PII/PHI for testing information systems or pre-production prior to deploying to production.

CirrusMD Virtual Health Chat for Government -E awareness training program commences with the VA OIT TMS training, VA Privacy and Information Security Awareness and Rules of Behavior (ROB), number 10176. Following the training, all information system users will be able to identify the types of information that must be carefully handled to protect privacy; recognize the required information security practices, legal requirements, and consequences and penalties for non-compliance; and explain how to report incidents. The awareness program is consistent, updated and deployed for all employees regularly.

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 ISSO to complete all Privacy Risk questions inside the document this section).

While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

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

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: Records must be maintained to be accurate, relevant, timely and complete. The risk to maintaining data within CirrusMD Virtual Health Chat for Government -E for a longer time period than what is needed or required is that the longer information is kept, the greater the risk that information will be compromised, unintentionally released or breached.

Mitigation: Access to the system is governed by a need to know. All those with access have been trained in Privacy and Information Security. The system only retains information long enough to process request to print identification card. The information is stored temporarily just in case there is a need to resubmit a request for printing because the originally request was not received, or the Veteran did not receive the identification card. CirrusMD Virtual Health Chat for Government -E is housed in a secure Amazon AWS Cloud. CirrusMD Virtual Health Chat for Government -E users are granted access to the system based on supervisor approved request. CirrusMD Virtual Health Chat for Government -E users access the system via Identity Access Management Single Sign-on or multi-factor credentials.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

NOTE: Question 3.9 (second table) on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system within VA with which information is shared.

State the purpose for the internal sharing. If you have specific authority to share the information, provide a citation to the authority.

For each interface with a system outside your program office, state what specific data elements (PII/PHI) are shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?
This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Veterans' Health Administration-Vista A	Verify identity and manage authentication	System Log files, Progress notes the VA health care provider made about the encounter.	Electronically pushed through VistA to CPRS via HTTPS on port 443.
Veterans' Health Administration-MyHealtheVet (MHV) / Mobile Authentication Services (SSOe)	Verify identity and manage authentication	PII, Veteran name, DOB, zip code, email address, SSN.	Encrypted JavaScript Object Notation (JSON) Web Token via HTTPS on port 443.

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: Data collected by the CirrusMD application contains PII, and other sensitive information. Due to the sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious harm or even identity theft may result in a significant financial burden to address the impact of stolen identity.

Mitigation: CirrusMD ensures strict access to information by enforcing thorough access control and requirements for end users. All roles in CirrusMD will be managed by system administrators and undergo a documented approval process. Access to CirrusMD will be limited to authorized users of the system, who will have appropriate credentials for authentication. As part of the access management activities, the highest level of assurance for providing identity along with multi-factor authentication will be used. Additionally, the system will log access and activity.

Section 5. External Sharing/Receiving and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to VA, which includes Federal, State, and local governments, and the private sector.

5.1 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

Is the sharing of information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.

NOTE: Question 3.10 on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any Federal, State, or local government agency or private sector organization with which information is shared.

For each interface with a system outside VA, state what specific data elements (PII/PHI) are shared with each specific partner.

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.
This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
VA Health Chat	To facilitate secure and seamless virtual healthcare interactions	Veteran Name, DOB, SSN, VA Health Facility Locations	System of Records Notice (SORN) #168VA005 Health	Web, VPN Traffic

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

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

*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:

<u>Privacy Risk:</u> Sharing information externally increases the chance that unauthorized individuals will gain access, potentially leading to data breaches in which sensitive information is exposed. Once information is shared outside an organization, control over who accesses, uses, or further shares it is often lost. This can lead to misuse or further sharing without consent.

Mitigation: CMD shares only the minimum necessary data to fulfill the purpose of sharing the data. To access authorized data, role-based access controls with multi-authentication are in place. All users are provided with the minimum permissions needed for their tasks or roles to minimize data exposure.

Section 6. Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an Appendix-A 6.1 on the last page of the document. Also provide notice given to individuals by the source system (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

These questions are related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

6.1a This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

> Yes. Notice is provided to Veteran upon entering any information into CirrusMD Virtual Health Chat for Government -E . It reinforces to the user that any information they enter into form-fields on the application will be collected. Please see Appendix A for an example. Also, notice is provided within this PIA and the governing SORN (System of Records Notice) #168VA005 Health Information Exchange-VA.

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

The CirrusMD Virtual Health Chat for Government -E Privacy Policy is publicly viewable at the following link; https://www.CirrusMD Virtual Health Chat for Government -E .com/privacy-policy

6.1c Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

The notice provided for the collection of information is considered adequate because it is presented to individuals at key points where their data is collected, ensuring they are informed about the collection and use of their information. Specifically, CirrusMD Virtual Health Chat for Government -E provides notice to users through:

1. Privacy Policies on Forms and Web Sites: These notices are made available on the application's interfaces, such as form fields or during registration processes, clearly informing individuals that their information will be collected and used. This notice is consistent with privacy control TR-1 (Privacy Notice) and TR-3 (Dissemination of Privacy Program Information).
2. System of Records Notices (SORNs): The relevant SORN, such as VA SORN (System of Record Notice) #168VA005 Health Information Exchange-VA, is published in the Federal Register, providing the legal authority, purpose, and uses of the collected information, as required by TR-2. This makes it clear how the information will be managed and under what conditions it may be shared.

The notices explain the purpose of data collection, with whom the data may be shared, and outline the rights of individuals regarding access to their information, ensuring that individuals are fully aware of how their information is being handled.

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.

Yes, the Veteran has the right to decline. To verify identity and authentication for access authorized VA applications/systems, the Veteran must use CirrusMD Virtual Health Chat for Government -E or another approved VA system. There is no penalty for a Veterans refusal; however, we will be unable to verify identity without the information. Information is required to verify identity. Providing information is a basic assumption and requirement of for accessing CirrusMD Virtual Health Chat for Government -E .

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.

The individual has the right to consent as outlined within the System of Records Notice #168VA005 Health Information Exchange-VA. All requests must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA address outlined.

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 System ISSO to complete all Privacy Risk questions inside the document this section).

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

Principle of 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 the Veterans' who provide information to CirrusMD Virtual Health Chat for Government -E will not know how their information is being stored in CirrusMD Virtual Health Chat for Government -E .

Mitigation: A disclaimer will be placed on the CirrusMD Virtual Health Chat for Government -E landing page outlining the scope of information usage and retention. Notice is published within the Privacy Act, PIA would be covered under VA SORN (System of Records Notice) #168VA005 Health Information Exchange-VA.

Section 7. Access, Redress, and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

7.1 What are the procedures that allow individuals to gain access to their information?

These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

7.1a Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. ***For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.***

Veterans may request access to Privacy Act records maintained by requesting a copy in writing. All requests to review must be received by direct mail, fax, in person, or by mail referral from another agency or VA office. All requests for access must be delivered to and reviewed by the System Manager for the concerned VHA system of records, the facility Privacy Officer, or their designee. Each request must be date stamped and reviewed to determine whether the request for access should be granted.

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 CirrusMD Virtual Health Chat for Government -E Health Chat system is not exempt from the privacy act.

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?

Veterans may request access to Privacy Act records maintained by requesting a copy in writing. All requests to review must be received by direct mail, fax, in person, or by mail referral from another agency or VA office. All requests for access must be delivered to and reviewed by the System Manager for the concerned VHA system of records, the facility Privacy Officer, or their designee. Each request must be date stamped and reviewed to determine whether the request for access should be granted.

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.

Veterans have the right to amend their records by submitting their request in writing. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA organization that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VA system of records, and the facility Privacy Officer, or designee, and needs to be date stamped; and filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579.

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.

If a Veteran has questions pertaining to data submitted to the VA to obtain services, they will follow standard Amendment processes listed within the SORN and this PIA.

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.

The system will allow user to enter correct information and request access to CirrusMD Virtual Health Chat for Government -E .

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

Privacy Risk: There is some risk of inaccurate information being sent to authorized VA credential providers as a result of a Veteran entering incorrect data into CirrusMD Virtual Health Chat for Government -E

Mitigation: Individuals are provided notice of how to access, redress and correct information maintained in a VA system of record within the applicable SORN and the PIA. We will monitor user feedback, as well as analyze system data for error rates. Any inaccuracies will be addressed immediately by Veteran either making changes to the information that was entered or by contacting the Veteran via letter sent using the United States Postal Service informing that the request could not be completed because erroneous information was submitted.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system, and are they documented?

These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.

8.1a Describe the process by which an individual receives access to the system?

CirrusMD Virtual Health Chat for Government -E will be using multi-factor authentication mechanism through MyhealthVet DSLogon and ID.me to allow users internal to the VA to access the system (e.g., using Personal Identity Verification (PIV).
Server-level access will be managed and granted to developers on an as-needed basis by the CirrusMD Virtual Health Chat for Government -E Information Security Officer (ISO). We will be limiting access to only a small set of trusted developers approved to work with and diagnose production issues. Secure Shell (SSH) access will be logged and monitored.

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?

The CirrusMD Virtual Health Chat for Government -E Health Chat system is only available to authorized and authenticated users internal to the VA, and a limited set of trusted developers have been approved to work with and diagnose production issues.

CirrusMD Virtual Health Chat for Government -E requires using multi-factor authentication mechanism through MyhealthVet DSLogon, and ID.me to allow users internal to the VA to access the system (e.g., using Personal Identity Verification (PIV). Server-level access will be managed and granted to developers on an as-needed basis by the CirrusMD Virtual Health Chat for Government -E Information Security Officer (ISO). We will be limiting access to only a small set of trusted developers approved to work with and diagnose production issues. Secure Shell (SSH) access will be logged and monitored

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.

The different roles created to provide access to the CirrusMD Virtual Health Chat for Government -E system are based on the principle of least privilege and are structured as follows:

- System Administrators and Application Operators: These roles are responsible for maintaining and operating the CirrusMD Virtual Health Chat for Government -E system. System Administrators manage AWS resources and have broader access to systems and services, allowing them to make changes, updates, and configurations as needed. They are part of groups with higher privileges that permit modification of system settings.
- Developers: They have access to the development environment and can make changes within that environment. Developers typically have "write" access to systems related to their work but are restricted from making changes to production environments.

- Read-only Users: Certain users, such as auditors or monitoring personnel, may only have read-only access, allowing them to view system information without making any changes.
- Privileged Users: These users have administrative-level access and can modify critical system settings, install software, and manage user accounts. Their activities are closely monitored and logged for security purposes.

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.

Contractors will be given access to hosting environment and complete their contractual obligations for ensuring the architecture, and hardware are available; and complies with VA OI&T policy. Contractors will have access to PII or data contained in the 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.

No additional privacy or security training would be offered specific to the Cirrus application. Existing VA privacy and PII trainings are deemed to be sufficient.
VA awareness training program commences with the VA OIT TMS training, *VA Privacy and Information Security Awareness and Rules of Behavior (ROB), number 10176.* Following the training, all information system users will be able to identify the types of information that must be carefully handled to protect privacy; recognize the required information security practices, legal requirements, and consequences and penalties for non-compliance; and explain how to report incidents. The awareness program is consistent, updated and deployed for all employees regularly.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Current
2. *The System Security Plan Status Date:* 8/7/2024

3. *The Authorization Status:* 180 Day ATO granted on
4. *The Authorization Date:* 4/21/2024
5. *The Authorization Termination Date:* 10/18/2024
6. *The Risk Review Completion Date:* 11/07/24
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

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

Section 9 – Technology Usage

The following questions are used to identify the technologies being used by the IT system or project.

9.1 Does the system use cloud technology? If so, what cloud model is being utilized?
If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.
Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1*. (Refer to question 3.3.1 of the PTA)*

Yes, the CirrusMD Virtual Health Chat for Government -E system uses cloud technology and is a Software as a Service (SaaS), and it is hosted on Amazon Web Services (AWS). The system utilizes the AWS Platform as a Service (PaaS) model, as described in the documentation, which includes several AWS components such as S3, RDS, Lambda functions, and others.

The system has a FedRAMP authorization. Specifically, it inherits from AWS's existing FedRAMP authorization. Several interconnections, including AWS services like Route53, S3, and EC2, are listed as FedRAMP authorized, ensuring compliance with federal cloud security standards.

For systems that are not FedRAMP authorized, such as PagerDuty, the CirrusMD Virtual Health Chat for Government -E system ensures that no federal data or metadata is processed, stored, or transmitted, adhering to strict security requirements.

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.2 of* *the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

Yes, the contract with the Cloud Service Provider (CSP) and contractors establishes ownership rights over data, including Personally Identifiable Information (PII). The contract outlines specific requirements for protecting security-related components and ensuring compliance with applicable laws, regulations, and guidelines. CirrusMD Virtual Health Chat for Government -E ’s security requirements, as detailed in the contract addendum or rider, state that the CSP must adhere to federal laws and guidelines, including the ownership and protection of PII.

The contract number and supporting documentation related to PII/PHI can be referenced through acquisition agreements, including HIPAA Business Associate Agreements (BAAs), which are part of the CirrusMD Virtual Health Chat for Government -E System. These agreements ensure that data ownership and privacy requirements are established and maintained.

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.

Yes, the Cloud Service Provider (CSP) collects ancillary data. This includes data generated within the cloud environment, such as audit trails, logs, and information collected for resource usage metering.

Ownership of this ancillary data, as it relates to cloud service operations, typically remains with the Cloud Service Provider. However, this data is used exclusively for managing, securing, and maintaining the cloud infrastructure, and does not include direct customer data like PII or PHI unless explicitly stated in agreements or as required for compliance with applicable regulations.

According to the control DI-1 (Data Quality), CirrusMD Virtual Health Chat for Government -E ensures that any PII collected or generated adheres to strict accuracy, relevance, timeliness, and completeness checks, and that cloud providers hold this data securely and only use it as authorized. The specific ownership and handling of ancillary data such as audit logs and resource metering information would also be governed by agreements between CirrusMD Virtual Health Chat for Government -E , the CSP, and any third-party contractors.

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.

The CiurrsMD Health Chat implements the principle from NIST 800-144, which states that "organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf," is described in contracts with customers. Contracts clearly define the roles and responsibilities between the organization and the cloud provider, especially concerning the security and privacy of data.

The organization, in this case, remains accountable for ensuring that its data, including Personally Identifiable Information (PII), is secure, even when handled by a Cloud Service Provider (CSP). Contracts with CSPs and contractors include provisions for security measures and data protection requirements. This ensures that both the organization and CSP adhere to the necessary regulatory guidelines, like FedRAMP and VA Handbook 6517.

Roles and responsibilities are divided as follows:

1. The organization (CirrusMD Virtual Health Chat for Government -E): Responsible for ensuring compliance with privacy controls, defining privacy and security requirements, conducting risk assessments, and maintaining control over the data they manage.
2. The Cloud Service Provider (AWS in this case): Responsible for implementing the necessary security controls to protect the cloud infrastructure and adhering to privacy and security requirements specified in contracts. The CSP also provides data monitoring, audit logs, and compliance with FedRAMP.

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).

The CirrusMD Virtual Health Chat for Government -E Health Chat system does not use Robotics Process Automation.

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
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

Digitally signed by KIMBERLY MURPHY
Date: 2024.12.12 06:57:13 -05'00'

Privacy Officer, Kimberly Murphy

KAREN MCQUAID

Digitally signed by KAREN MCQUAID
Date: 2024.12.12 09:53:37 -06'00'

Information System Security Officer, Karen McQuaid

SCOTTIE ROSS

Digitally signed by SCOTTIE ROSS
Date: 2024.12.19 16:32:51 -05'00'

Information System Owner, Scottie Ross

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).

The CirrusMD Virtual Health Chat for Government -E Privacy Policy is publicly viewable at the following link; https://www.CirrusMD Virtual Health Chat for Government -E .com/privacy-policy

HELPFUL LINKS:

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 Notice of Privacy Practices
VHA Handbook 1605.04: Notice of Privacy Practices