Privacy Impact Assessment for the VA IT System called:

CirrusMD Assessing

VHA

Date PIA submitted for review:

21 May 2021

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)	Terrell Bowden	Terrell.Bowden@va.gov	(216) 314-2597
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?" and will be published online to accompany the PIA link.

CirrusMD Chat increases Veteran Access to VA Care. CirrusMD provides VA with a Veteran clinical chat capability to increase the efficiency, capacity and response time for clinical care for our Veterans.

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 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 platform using their VA credential and the Single Sign- On Internal (SSOi) service. Staff will directly access the CirrusMD interface using the platform that is provided by the vendor or a VA 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 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 platform using their VA credential and the Single Sign- On Internal (SSOi) service. Staff will directly access the CirrusMD interface using the platform that is provided by the vendor CirrusMD. Chat increases Veteran Access to VA Care. CirrusMD provides VA with a Veteran clinical chat capability to increase the efficiency, capacity, and response time for clinical care for our Veterans.

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?*

Cirrus MD 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.

CirrusMD is a software as a service (SaaS) that is hosted and maintained by a third-party vendor. CirrusMD 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 ownership of the data belongs to the Veteran, per the user agreement with CirrusMD. The OIT Project Special Forces office will assist with implementing and securing the SaaS.

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 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. The system was categorized as Moderate and the required controls established. Eligibility for VA healthcare will be confirmed using the VA Enrollment Application Programming Interface (API).

VA staff will access the CirrusMD platform using their VA credential and the Single Sign- On Internal (SSOi) service. Staff will directly access the CirrusMD interface using the platform that is provided by the vendor.

CirrusMD is provided under –Public Law 114-31; Veteran Information: Title 38, United States Code, Section 5107, Title 38, United States Code, Section 5106, and Title 38 United States Code 5701. Title 38, United States Code, section 81 11 (38 U.S.C. 5811 I), titled "Sharing of Department of Veterans Affairs and Department of Defense Health Care Resources. "Title 10, United States Code, section 1104 (10 U.S.C.5 1104), titled "Sharing of Resources with the Department of Veterans Affairs," which incorporates Title 31, United States Code, section 1535 (31 U.S.C. 51 535), titled

"Agency Agreements," also known as the "Economy Act." E-government Act of 2002 (44 U.S.C. §208(b)). 38 United States Code 5706.

CirrusMD is covered under VA SORN (System of Records Notice) #173VA005OP2 VA Mobile Application Environment (MAE)-VA

Section 1. Characterization of the Information

The following questions are intended to define the scope of the information requested and collected as well as the reasons for its collection as part of the program, IT system, or technology being developed.

1.1 What information is collected, used, disseminated, created, or maintained in the system?

Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy- Protected Information. For additional information on these information types and definitions, please see VA Directives and Handbooks in the 6500 series (https://vaww.va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.
This question is related to privacy control AP-1, Authority To Collect, and AP-2, Purpose Specification.

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1.

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional SPI is collected, used, disseminated, created, or maintained, please list those in the text box below:

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

CirrusMD will receive possible data listed above provided by the Veteran for use with identity management and authentication to access the online chat session.

PII Mapping of Components

CirrusMD consists of 2 key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by CirrusMD and the functions that collect it are mapped 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
va-production1-app1	Yes	No	Full Name, Social Security Number, email address, phone number, DOB, zip code, SSN, VA ID, audio/video/photographic recording(s) of encounter.	To record patient / provider encounter information	Hosted in AWS Cloud, controlled physical and logical access, only approved and authorized users granted access to application. Data encrypted and physical/logical access restricted based upon least privilege
Elastic Search Repository	No	Yes	Full Name, email address, phone number, DOB, zip code, patient text-based chat.	Used for system logging and alerting functionality	Hosted in AWS Cloud, controlled physical and logical access, only approved and authorized users granted

					access to application. Data encrypted and physical/logical access restricted based upon least privilege

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.

Users will enter information in CirrusMD. Veterans name, email address, date of birth, and zip code. CirrusMD will provide all information to the VA Single Sign-on application verifying identity and allowing access to CirrusMD.

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.

Users will access SaaS web application and enter information directly into CirrusMD.

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 will be collected from the Veteran and is considered accurate. CirrusMD will validate identity using ID.me, MyHealtheVet, or DS Logon. ID.me, MyHealtheVet and DS Logon integrate with the Master Person Index (MPI) as part of the identity management and user authorization process. Information received and displayed from other VA systems is considered accurate.

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

CirrusMD is provided under –Public Law 114-31; Veteran Information: Title 38, United States Code, Section 5107, Title 38, United States Code, Section 5106, and Title 38 United States Code 5701. Title 38, United States Code, section 81 11 (38 U.S.C. 5811 I), titled "Sharing of Department of Veterans Affairs and Department of Defense Health Care Resources. "Title 10, United States Code, section 1104 (10 U.S.C.5 1104), titled "Sharing of Resources with the Department of Veterans Affairs," which incorporates Title 31, United States Code, section 1535 (31 U.S.C. 51 535), titled "Agency Agreements," also known as the "Economy Act." E-government Act of 2002 (44 U.S.C. §208(b)). 38 United States Code 5706.

CirrusMD is covered under VA SORN (System of Records Notice) #173VA005OP2 VA Mobile Application Environment (MAE)-VA

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

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks.

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 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 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 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 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.

CirrusMD will be used to gather information in order to verify identity for use with authentication and accessing authorized VA applications/systems.

Name: Used as an identifier
Phone Number: Used as an identifier
Email address: Used to contact individual
Social Security #: Used as an identifier
Medical record #: Used as an identifier
DOB: Used as an identifier
Medications: Used for medical history
Mailing Address: Used to contact individual

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

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.

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

CirrusMD uses kms encryption, TLS/SSL for communications, authentication mechanisms. CirrusMD uses a KMS key to encrypt data, along with roles to access the KMS key for encryption/decryption.

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.

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 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.

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

All data listed in section 1.1 is retained temporarily as part of the user session. The system retains information submitted by the Veteran that is required to support identity verification and authentication for accessing authorized VA applications/systems. The system retains, for up to 75 years after the last episode of patient care, information submitted by the Veteran as part of their online communication with the VA medical provider

- Name
- Phone Number
- Email address
- Social Security Number
- Medical record Number

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.

The records are retained and disposed of in accordance with General record Schedules (GRS) 5.1 & 5.2. GRS 5.1 Disposition Instruction provides for deletion of data files when the agency determines that the files are no longer needed for administrative, legal, audit or other operational purposes. https://www.archives.gov/records-mgmt/grs.html.

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.

As stated in SORN #173VA005OP2, records from this system that are needed for audit purposes will be disposed of 6 years after a user's account becomes inactive. Routine records will be disposed of when the agency determines they are no longer needed for administrative, legal, audit, or other operational purposes. These retention and disposal statements are pursuant to NARA General Records Schedules GRS 20, item 1c and GRS 24, item 6a.

3.4 What are the procedures for the elimination 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

All data cached/stored by CirrusMD is deleted upon reaching the deletion timeframes as specified in 3.2. CirrusMD 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 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. 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

CirrusMD 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 does NOT use PII/PHI for testing information systems or pre-production prior to deploying to production.

CirrusMD 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 <u>PRIVACY IMPACT ASSESSMENT: Retention of information</u>

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks.

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 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. CirrusMD is housed in a secure Amazon AWS Cloud. CirrusMD users are granted access to the system based on supervisor approved request. CirrusMD 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***
MAP/VistA	To record the session and details of it back to the patient record within the VA.	System Log files, Progress notes the VA health care provider made about the encounter	Electronically pushed through MAP/VistA to CPRS via HTTPS on port 443.
MyHealtheVet (MHV) / Mobile Authentication Services (SSOe)	To produce the identity management information needed to verify identity and authenticate users for accessing CirrusMD.	PII, Veteran name, DOB, zip code, email address, SSN.	Encrypted JavaScript Object Notation (JSON) Web Token via HTTPS on port 443

4.2 <u>PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure</u>

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: All parties with which we are sharing information already are able to access this information. Thus, it does not increase the risks from an internal sharing standpoint.

Mitigation: Existing mitigation techniques used to protect privacy from internal sharing and disclosure risks, such as trainings, will suffice as mitigation, since there is no increased risk. Risk increases with the number of people having access to protected information.

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***	***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.***	***List the method of transmission and the measures in place to secure data***

	specified program office or IT system		***that permit external sharing (can be more than one)***	
CirrusMD AWS East / West	To record patient and provider digital interaction over the internet.	Veteran Name, DOB, SSN, VA Health Facility Locations	MOU/ISA, BA	HTTPS on port 443

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: There is risk to the organization that a breach could occur leading to potential identity theft or unauthorized changes to the data.

Mitigation: Monitors and audits are conducted to ensure security of information. Policies and procedures are in place for guidance, along with ongoing education, in privacy and security. Use of secure passwords and access for need to know basis are utilized, and users are validated by the VA.

An MOU/ISA and BAA have been executed and are currently in place between CirrusMD and the VA.

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.

Yes. Notice is provided to Veteran upon entering any information into CirrusMD. 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) #173VA005OP2 VA Mobile Application Environment (MAE)-VA

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 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.

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 (173VA005OP2). 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.

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 will not know how their information is being stored in CirrusMD.

Mitigation: A disclaimer will be placed on the CirrusMD 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) #173VA005OP2 VA Mobile Application Environment (MAE)-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?

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.

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.
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 ensures data accuracy.

The system will allow user to enter correct information and request access to CirrusMD.

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 some risk of inaccurate information being sent to authorized VA credential providers as a result of a Veteran entering incorrect data into CirrusMD

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?

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.

CirrusMD 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 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.

8.2 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. These support contractors are required to sign Non-Disclosure Agreements (NDAs)/ Business Associate Agreements (BAAs) / Confidentiality Agreements.

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?

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.***

Yes. The Authorizing Official granted CirrusMD a 1-year ATO until August 12, 2022. The system categorization is rated at a 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.

Software as a Service (SaaS), and the hosting provider, AWS, has a FedRAMP ATO.

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.

VA customers has the rights over data including PII

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, Data is owned by the customer

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.

Yes, for the purposes of adhering to NIST 800-144 Guidelines

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 system is not utilizing RPA.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

ID	Privacy Controls
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.

Digitally signed by Kimberly E. Murphy 183320
Date: 2022.01.04 09:26:25 -05'00'

Privacy Officer, Kimberly Murphy

Terrell E Bowden 3595931

Digitally signed by Terrell E Bowden 3595931
Date: 2022.01.03 12:12:26 -05'00'

Information Systems Security Officer, Terrell Bowden

Scottie K. Ross 190132

Digitally signed by Scottie K. Ross 190132
Date: 2022.01.03 11:46:39 -05'00'

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).

173VA005OP2 VA Mobile Application Environment (MAE)-VA,
https://www.govinfo.gov/content/pkg/FR-2013-11-06/pdf/2013-26520.pdf