Privacy Impact Assessment for the VA IT System called:

Direct Secure Messaging (DSM)

VA Office of Information and Technology (OIT) Enterprise Program Management Office (EPMO)

Date PIA submitted for review:

September 23, 2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Peggy Pugh	Margaret.Pugh@va.gov	202-731-6843
Information System Security Officer (ISSO)	Carl J. Lindsey	Carl.Lindsey@va.gov	786-299-1300
Information System Owner	Christopher Brown	Christopher.Brown1@va.gov	202-270-1432

Abstract

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

DSM allows for the sharing of medical information between the Department of Veterans Affairs (VA) and non-VA care providers. DSM permits the electronic exchange of information over the Internet using the Direct Project standards published by Health and Human Services, the Office of the National Coordinator for Health IT. Supports the Veterans Health Information Exchange (VHIE) program.

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?*

Direct Secure Messaging (DSM) allows secure communication of health data among healthcare participants who already know and trust each other. DSM is to replace current manual (mail, hand-carried information, and fax) exchange processes between VA and non-VA local clinical practices with secure electronic exchange over the Internet. The system is a secure email application that enables participants to send encrypted health information directly to known, trusted recipients over the Internet. The system provides a foundation for the exchange of information in support of future user stories as previously identified by the Nationwide Health Information Network Direct Workgroup. The Direct specification calls for a Simple Mail Transfer Protocol (SMTP),

Secure/Multipurpose Internet Mail Extensions (S/MIME), and X.509 certificates to securely transport health information over the Internet. Participants in a Direct exchange are identified using standard e-mail addresses associated with X.509 certificates. Anyone whose information is contained within the MPI system is processed through DSM. These participants include Electronic Health Record (EHR) and Personal Health Record (PHR) vendors, medical organizations, systems integrators, integrated delivery networks, federal organizations, state and regional health information organizations, that provide health information exchange capabilities, and health information technology consultants. The integration with Master Person Index (MPI) will provide DSM users the ability to identify and authenticate patients, which will be maintained in the MPI and kept up to the current identity management standards. DSM consists of a user interface for a custom webmail application between Cerner Health Information Service Provider (HISP) and other VA third parties that have a signed Direct Trust Agreement. Information will be encrypted with digital signatures.

DSM is only used by VA providers throughout the VA direct trust network. A citation of the legal authority to operate the IT system as listed in the SORN 24VA10A7, Patient Medical Record-VA, and in SORN 168VA005, Health Information Exchange-VA, is Title 38, United States Code, Sections 501(b) and 304. This PIA will not result in changes to business processes and will not result in technology changes. The SORN will not require amendment or revision and approval and does cover cloud usage and storage.

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)

Other information maintained in the system: Health/Medical Information (Diagnosis, Treatment, Medication and X-Ray), Electronic Data Interchange Personal Identifier (EDIPI) and Biometrics.

PII Mapping of Components

DSM consists of 2 key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by DSM and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

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
VAC10APPDIR300	Yes	Yes	• Patient ID (EDIPI or ICN)	Used to verify identity/ Correspond with Veterans	Centralized access control with two factor authentication
Prod-database	Yes	Yes	• Patient ID (EDIPI or ICN)	Used to verify identity/ Correspond with Veterans	Centralized access control with two factor authentication

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

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

Describe why information from sources other than the individual is required. For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question 1.3 indicate why the system is using this source of data.

If the system creates information (for example, a score, analysis, or report), list the system as a source of information.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

The source of DSM information is from the MPI system and Cerner HISP where the Veteran inputs their own information. Veterans' health information is being stored/encrypted to the DSM application database servers.

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 technologies 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.

DSM information is sent and received electronically as encrypted email messages from VA users who are part of the Direct Trust Network. The information collected by the system is maintained by the system users, in this case Veterans and VA clinician staff. Data is saved and archived to the local DSM database servers.

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.

DSM does not analyze any patient data. The system is designed to provide security, privacy, data integrity, authentication of senders and receivers, and confirmation of delivery consistent with the data transport needs for health information exchange. The system is a secure email application that enables participants to send encrypted health information directly to known, trusted recipients over the Internet.

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 authority for the collection of information in the System of Records Notices 24VA10A7 Patient Medical Records – VA and 168VA005 Health Information Exchange- VA: 2020-21426.pdf (govinfo.gov) and 2021-01516.pdf (govinfo.gov) is the Privacy Act of 1974, as amended, 5 U.S.C. § 552a, which establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. The authority of maintenance of the system listed in question 1.1 falls under Title 38, United States Code, Sections 501(a), 1705, 1710, 1722, and 5317.

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?

This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

Privacy Risk: There is a risk of collecting too much information as well as the risk of collecting inaccurate information.

Mitigation: The VA's risk assessment validates the security control set and determines if any additional controls are needed to protect agency operations. Many of the security controls such as contingency planning controls, incident response controls, security training and awareness controls, personnel security controls, physical and environmental protection controls, and intrusion detection controls are common security controls used throughout the VA. Our overall security controls follow VA 6500 Handbook, and NIST SP800-53 high impact defined set of controls. The system owner is responsible for any system-specific issues associated with the implementation of this facility' common security controls. These issues are identified and described in the system security plans for the individual information systems. Prior to sending the messages using DSM, the participants must review the notice and consent information and authorize to send the information. Information is encrypted with digital signature.

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.

Name: Veteran's identification
Social Security Number: Used to lookup number in MPI
Date of Birth: Used to lookup number in MPI
Personal Phone Number(s): Passed within the medical record, not for use with DSM
Personal Address: Passed within the medical record, not for use with DSM
Personal Email Address: Passed within the medical record, not for use with DSM
Internet Protocol (IP) Address Numbers: Used for DSM users only
Medical Record Number: Used to identify user with JHIE
Gender: Used to lookup number in MPI
Integration Control Number (ICN): Used as medical record number
Health/Medical Information: Passed within the medical record, not for use with DSM
Electronic Data Interchange Personal Identifier (EDIPI): Used as medical record number
Biometrics: Passed within the medical record, not for use with DSM

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

DSM does not analyze any patient data. The system is designed to provide security, privacy, data integrity, authentication of senders and receivers, and confirmation of delivery consistent with the data transport needs for health information exchange. The system is a secure email application that enables participants to send encrypted health information directly to known, trusted recipients over the Internet.

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?

The minimum-security requirements for DSM's HIGH impact system will cover 17 security-related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. 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; and system and information integrity. DSM has encryption that is compliant and meets the VA6500 requirements for data at rest encryption as well as data in transit. SSNs are encrypted and are not searchable.

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

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

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

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

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

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

Add answer here:

DSM follows the standard documented need-to-know principle of only granting access to VA employees to the data they need to perform their jobs. As part of standard VA Privacy and Information Security training, users are taught not to arbitrarily share data with co-workers unless the co-worker has a need for that data.

Anyone needing access to data goes through the formal VA access request process, submitting a SNOW ticket and receiving their supervisor's approval before access can be granted. As with all access to PII and PHI, data access is monitored, tracked, and reported to identify possible misuse. The Information System Security Officer (ISSO) and Cybersecurity Operations Center (CSOC) are responsible for assuring safeguards for the PII. Access to all messages will be made available to a search by authorized users even if they were not originally a member of the message recipient group or distribution list. DSM includes a check box for secure electronic transmission of information to and from non-VA providers.

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

Name
SSN
Date of Birth
Personal Phone Number
Personal Address
Personal Email Address
Internet Protocol (IP) Address Numbers
Medical Record Number
Gender
Integration Control Number (ICN)
Health/Medical Information
Electronic Data Interchange Personal Identifier (EDIPI)
Biometrics

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.

National Archives and Records Administration (NARA) guidelines as stated in RCS 10-1 records retention schedule requires retention for 75 years. However, any documents that the veteran requests removal from the system will be manually purged from the system upon request.

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.

The records retention for VHA is RCS 10-1, https://vaww.va.gov/vhapublications/rcs10/rcs10-1.pdf

3.4 What are the procedures for the elimination of Sensitive Personal Information (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

Recall records per Records Control Schedule (RCS) 10-1 6000.1 will remain in VA health care facility until 3 years after last episode of care, and then convert to an inactive medical record.

For the inactive medical record, VHA RCS 10-1 6000.2 Electronic Health Record (EHR) states to Destroy/delete record 75 years after the last episode of care.

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

Test Patients with mock data such as names, social security numbers and medical records are used for testing, demonstration, and training purposes. DSM product development teams do not use or store real patient data in DSM lower-level environments.

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:

<u>Principle of Minimization:</u> Does the project retain only the information necessary for its purpose? Is the PII retained only for as long as necessary and relevant to fulfill the specified purposes?

<u>Principle of Data Quality and Integrity:</u> Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?

This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:

Privacy Risk: The risk to maintaining data within the DSM system is the longer time frame information is kept, the greater the risk that information possibly will be compromised, unintentionally released, or breached.

Mitigation: To mitigate the risk posed by information retention, DSM adheres to the VA Records Control Schedule (RCS) schedules for each category or data it maintains. When the retention data is reached for a record, DSM will manually dispose of the data by the determined method as described in question 3.4.

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***
Data Access Service (DAS)	To provide summary of care document for treatment purposes.	• Name • SSN • Date of Birth • Personal Phone Number • Personal Address • Personal Email Address • Internet Protocol (IP) Address Numbers • Medical Record Number • Gender • Integration Control Number (ICN) • Health/Medical Information • Electronic Data Interchange Personal Identifier (EDIPI) • Biometrics	Pull data HTTPS/443 thru AWS to DSM Database via SQL Server/1433
JHIE	To provide summary of care document for treatment purposes.	• Name • SSN • Date of Birth • Personal Phone Number • Personal Address • Personal Email Address • Internet Protocol (IP) Address Numbers • Medical Record Number • Gender • Integration Control Number (ICN) • Health/Medical Information	Pull data HTTPS/443 thru AWS to DSM Database via SQL Server/1433

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*
		• Electronic Data Interchange Personal Identifier (EDIPI) • Biometrics	
On prem VA User Workstation	To provide summary of care document for treatment purposes.	• Name • SSN • Date of Birth • Personal Phone Number • Personal Address • Personal Email Address • Internet Protocol (IP) Address Numbers • Medical Record Number • Gender • Integration Control Number (ICN) • Health/Medical Information • Electronic Data Interchange Personal Identifier (EDIPI) • Biometrics	Pull data HTTPS/443 thru AITC Network Proxy to DIR Database via SQL Server/1433
Master Person Index (MPI)	To provide summary of care document for treatment purposes.	• Name • SSN • Date of Birth • Personal Phone Number • Personal Address • Personal Email Address • Internet Protocol (IP) Address Numbers • Medical Record Number • Gender • Integration Control Number (ICN)	Pull data HTTPS/443 thru AWS Network Proxy to DIR Application Mail Server via SMTP/(25, 465, 587)

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*
		• Health/Medical Information • Electronic Data Interchange Personal Identifier (EDIPI) • Biometrics	
VA Internal Email Service	To provide summary of care document for treatment purposes.	• Message Delivery Notification (MDN) • Name	SMTP

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks.
This question is related to privacy control UL-1, Internal Use.

Follow the format below:

Privacy Risk: There is a risk that information may be shared with an unauthorized VA program, system, or individual. The privacy risk associated with maintaining PII is that sharing data within the Department of Veteran's Affairs could happen and that data may be disclosed to individuals who do not require access and heightens the threat of the information being misused.

Mitigation: Safeguards implemented to ensure data is not sent to the wrong VA organization are employee security and privacy training and awareness and required reporting of suspicious activity. Use of secure passwords, access for need-to-know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization using Network Identification (NTID) are all measures that are utilized within the facilities. The principle of need-to-know is strictly adhered to by the Veteran's Crisis Line personnel. Only personnel with a clear business purpose are allowed access to the system and the information contained within the system.

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***
External Healthcare Organizations who have signed the Direct Trust	To provide summary of care document for	• Name • SSN • Date of Birth • Personal Phone Number • Personal Address • Personal Email Address	The Direct Trust Federated Services Agreement (FSA) and	Secure encrypted connection

Federated Services Agreement and been onboarded for sharing with VA.	treatment purposes.	• Internet Protocol (IP) Address Numbers • Medical Record Number • Gender • Integration Control Number (ICN) • Health/Medical Information • Electronic Data Interchange Personal Identifier (EDIPI) • Biometrics	Data Sharing Policy covers HISP to HISP Messaging (MOU)	
Cerner		• Name • SSN • Date of Birth • Personal Phone Number • Personal Address • Personal Email Address • Internet Protocol (IP) Address Numbers • Medical Record Number • Gender • Integration Control Number (ICN) • Health/Medical Information • Electronic Data Interchange Personal Identifier (EDIPI) • Biometrics	Cerner Corporation EHR VA National MOU ISA 2021.02.02	Secure encrypted connection

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 a risk that information may be shared with an unauthorized VA program, system, or individual. The privacy risk associated with sharing VA sensitive data outside of the Department of Veteran's Affairs could increase the risk that data may be disclosed to individuals who do not require access and heightens the threat of the information being misused. Additionally, there is a privacy threat of a breech during the transmission of the data.

Mitigation: Safeguards implemented to ensure data is not sent to the wrong VA organization are employee security and privacy training and awareness and required reporting of suspicious activity. Use of secure passwords, access for need-to-know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized within the facilities.

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.

Additional notice is provided by the system's System of Record Notice (SORN), "Patient Medical Records–VA" (24VA10A7), which can be viewed at the following link: 2020-21426.pdf (govinfo.gov)
and
"Health Information Exchange- VA", 168VA005, 2021-01516.pdf (govinfo.gov)

The VHA Notice of Privacy Practices, effective September 30, 2022, is found at the following link:

IB 10-163p (sharepoint.com)

A third form of notice is provided by this Privacy Impact Assessment, which is available online as required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii).

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

VHA Directive 1605.01 'Privacy and Release of Information', paragraph 5 lists the rights of the Veteran to request VHA to restrict the uses and/or disclosures of the individual's individually-identifiable health information to carry out treatment, payment, or health care operations. The Veterans have the right to refuse to disclose their SSN to VHA. The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VHA an SSN (see 38 CFR 1.575(a)).

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

VHA Directive 1605.01 'Privacy and Release Information', paragraph 5 (a) (6) lists the rights of the Veterans to request VHA to restrict the uses and/or disclosures of the individual's individually-identifiable health information to carry out treatment, payment, or health care operations.

(6) Individuals have the right to request that VHA restrict the uses or disclosures of the individual's individually-identifiable health information to carry out treatment, payment, or health care operations. Individuals also have the right to request VHA to restrict disclosures of the individual's individually-identifiable health information to next-of-kin, family, or significant others involved in the individual's care. VHA is not required to agree to such restrictions, but if it does, VHA must adhere to the restrictions to which it has agreed, unless information covered under the agreed to restriction is needed to provide emergency treatment to a patient. VHA will not agree to a restriction of a use or disclosure required by law.

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:

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

<u>Principle of Use Limitation:</u> 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: Only assigned role users for the system are allowed access to participant's data in the system. There is a risk that VA employees, employee veterans and other members of the public will not know that the DSM exists or that it collects, maintains, and/or disseminates PII and other SPI about them.

Mitigation: If an assigned user no longer requires access to the system, the user account can be de-activated by the program administrator.

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.

VHA Directive 1605.01 'Privacy and Release of Information', paragraph 7(b) states the rights of Veterans to request access to review their records. VA Form 10-5345a, Individual's Request for a Copy of Their Own Health Information, may be used as the written request requirement. 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.

Under the jurisdiction of VHA, VHA Directive 1605.01 'Privacy and Release Information', paragraph 8 states the rights of Veterans to amend their records via submitting VA Form 10-5345a, Individual's Request for a Copy of Their Own Health Information, may be used as the written request requirement, which includes designated record sets, as provided in 38 CFR 1.579 and 45 CFR 164.526. 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 health care facility 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 VHA system of records, and the facility Privacy Officer, or designee, to be date stamped; and be 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.

In case the information in the DSM system is inaccurate, the Veterans have the right to request amendment of erroneous information in accordance with SORN 24VA10A7. Individuals have the right to request an amendment (correction) to their health information in VA records if they believe it is incomplete, inaccurate, untimely, or irrelevant. They must submit their request in writing, specify the information that they want corrected, and provide a reason to support the request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the last VA health care facility where care was rendered. Inquiries should include the patient's full name, Social Security number, and return address.

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.

If the individual discovers that incorrect information was provided during intake, they simply follow the same contact procedures as before, and state that the documentation they are now providing supersedes those previously provided.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that the individual accidentally provides incorrect information when entering the information. There is a risk that individual may seek to access or redress records about them held by the VA Office, but they are unaware that the DSM systems exists.

Mitigation: This PIA provides notice to the public that their information is being collected, processed, and stored. The SORN and the VHA Notice of Privacy Practices provides guidance regarding how to request a correction or amendment to the record.

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.

Office of Information and Technology (OIT) documents and monitors individual information system security training activities including basic security awareness training and specific information system security training. This documentation and monitoring is performed through the use of Talent Management System (TMS).

Access to the system is granted to VA employees and contractors by the local authority within each administrative area staff office, (YourIT) following the described account creation process within the Access Control Standard Operating Procedure for DSM (DSM_AC_SOP_FINAL.doc) located on the DSM SharePoint site.

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 of DSM are authorized VA and contract employees are reviewed annually by the OIT contracting offices. AWS Relational Database Service (RDS) will maintain the virtual hardware and software but are not privileged users of the DSM system itself.

VA contract employee access is verified through VA personnel before access is granted to any contractor. Contracts and contractor access are reviewed annually at a minimum. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of Behavior training (TMS#10176) documented in TMS. All contractors are cleared using the VA background investigation process and must obtain the appropriate background investigation for their role. Contractors with systems administrative access are required to complete additional role-based training prior to gaining system administrator access. Contractors with access to PHI are required to complete HIPAA (TMS# 10203) privacy training annually.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately. This question is related to privacy control AR-5, Privacy Awareness and Training.

Personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB (for AITC technicians) prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training which all personnel must complete via the VA's Talent Management System (TMS). After the DSM user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system. All VA employees must complete annual VA Privacy and Information Security and Rules of Behavior training. All employees with access to Protected Health Information (PHI) or access to VA information systems such as VA DSM users, must also complete Privacy and HIPAA Focused Web-Based Training.

8.4 Has Authorization and Accreditation (A&A) been completed for the system? No

If yes, provide:

1. *The Security Plan Status,* ***in progress***
2. *The Security Plan Status Date,* ***in progress***
3. *The Authorization Status,* ***not yet authorized***
4. *The Authorization Date,* ***not yet authorized***
5. *The Authorization Termination Date,* ***not yet authorized***
6. *The Risk Review Completion Date,* ***not yet authorized***
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH).* ***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.***

Deployment Target Completion Date for the DSM VAEC AWS Cloud HIGH is **11/04/2022.**

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.

Yes, DSM utilizes VAEC AWS Gov Cloud as a IaaS.

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.

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.

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.

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).

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.

Margaret L. Pugh 104985

Digitally signed by Margaret L. Pugh 104985
Date: 2022.10.20 14:53:39 -04'00'

Privacy Officer, Peggy Pugh

CARL LINDSEY

Digitally signed by CARL LINDSEY
Date: 2022.10.20 19:20:39 -05'00'

Information Systems Security Officer, Carl J. Lindsey

Christopher Brown 101386

Digitally signed by Christopher Brown 101386
Date: 2022.10.24 11:03:56 -05'00'

System Owner, Christopher Brown

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).

System of Record Notice (SORN), "Patient Medical Records–VA" (24VA10A7), which can be viewed at the following link: 2020-21426.pdf (govinfo.gov)
and
SORN "Health Information Exchange- VA", 168VA005, 2021-01516.pdf (govinfo.gov)

The VHA Notice of Privacy Practices, effective September 30, 2022, is found at the following link:

IB 10-163p (sharepoint.com)