



Privacy Impact Assessment for the VA IT System called:

Content Manager

Veterans' Health Administration (VHA)

Office of the Medical Inspector

Date PIA submitted for review:

10/11/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Phillip Cauthers	Phillip.Cauthers@va.gov	503-721-1037
Information System Security Officer (ISSO)	Kehinde A. Talabi	Kehinde.Talabi@va.gov	202-577-5414
Information System Owner	Elmer Clark	Elmer.Clark2@va.gov	202-815-9508

Abstract

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

Content Manager is a document and records management repository solution to capture, manage, and secure information discovered during an OMI investigation. All documents in CONTENT MANAGER are maintained in accordance with VA Records Management guidance and accessible only by OMI staff. In some cases, PII/PHI is included in discovery findings.

Overview

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

1 General Description

A. *The IT system name and the name of the program office that owns the IT system.*
Content Manager / VHA Office of the Medical Inspector

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

Content Manager is a document and records management repository solution to capture, manage, and secure information discovered during an OMI investigation. All documents in Content Manager are maintained in accordance with VA Records Management guidance and accessible only by OMI staff. In some cases, PII/PHI is included in discovery findings.

C. *Indicate the ownership or control of the IT system or project.*
VA Controlled / non-VA Owned and Operated.

2. Information Collection and Sharing

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

The expected number of individuals whose information will be stored is impossible to quantify because it is based upon the complainants listed in the referrals for investigation, which can't be quantified because it is based on unknown variables. It is impossible to predict. The Veterans Health Administration (VHA) is the largest integrated health care system in the United States, providing care at 1,255 health care facilities, including 170 VA Medical Centers and 1,074 outpatient sites of care of varying complexity (VHA outpatient clinics) to over 9 million Veterans enrolled in the VA.

E. *A general description of the information in the IT system and the purpose for collecting this information.*

Content Manager is a document and records management repository solution to capture, manage, and secure information discovered during an OMI investigation. All documents in Content Manager are

maintained in accordance with VA Records Management guidance and accessible only by OMI staff. In some cases, PII/PHI is included in discovery findings.

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

There is no sharing of information. An application of Content Manager is loaded on all Office of the Medical Inspector staff GFE issued laptops. The completion of this PIA will not result in circumstances that require changes to business processes. The completion of this PIA will not result in technology changes. The SORN ‘‘Investigative Database—OMI—VA’’ (162VA10E1B) will not require action. The system does not use cloud technology. If data is disclosed, intentionally or unintentionally the magnitude of harm cannot be quantified because it is dependent on variables that can’t be measured. The magnitude is person driven not system driven.

G. 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.

The system is not operated in more than one site.

3. Legal Authority and SORN

H. A citation of the legal authority to operate the IT system.

Legal authority to operate this system is Title 38 U.S.C. 501. ‘‘Investigative Database—OMI—VA’’ (162VA10E1B) <https://www.govinfo.gov/content/pkg/FR-2020-02-07/pdf/2020-02482.pdf>.

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

The SORN ‘‘Investigative Database—OMI—VA’’ (162VA10E1B) will not require action. The system does not use cloud technology. If data is disclosed, intentionally or unintentionally the magnitude of harm cannot be quantified because it is dependent on variables that can’t be measured. The magnitude is person driven not system driven.

D. System Changes

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

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

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

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

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://vawww.va.gov/vapubs/>). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

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

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

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

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

PII Mapping of Components (Servers/Database)

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

Note: Due to the PIA being a public facing document, please do not include the server names in the table. **The first table of 3.9 in the PTA should be used to answer this question.**

Internal Database Connections

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

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

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

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

The entities providing the information above are the witnesses, whistleblowers, etc. associated with the investigations performed by the Office of the Medical Inspector. Information sent to this system is sent manually from VHA medical facilities via email and the information contains data from other VHA SOR’s or agency records.

1.2b Describe why information from sources other than the individual is required. For example, if a program’s system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question indicate why the system is using this source of data.

The entities providing the information above are the witnesses, whistleblowers, etc. associated with the investigations performed by the Office of the Medical Inspector. Information sent to this system is sent manually from VHA medical facilities via email and the information contains data from other VHA SOR’s or agency records.

1.2c If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

The system does not produce a report.

1.3 How is the information collected?

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

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

The information collected from witnesses, whistleblowers, etc. is collected during the course of an investigation is received manually via email and uploaded to Content Manager. There is no external connections or automated uploading or transferring in this system.

1.3b 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.

If information is collected in paper form, it is not subject to Paper Reduction Act. The information collected from witnesses, whistleblowers, etc. is collected during the course of an investigation is received manually via email and uploaded to Content Manager. There is no external connections or automated uploading or transferring in this system.

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

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

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

OMI cannot account for the accuracy of the information they are provided from external sources.

1.4b 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.

The system does not check for accuracy by accessing a commercial aggregator of information.

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 to operate this system is Title 38 U.S.C. 501. The SOR for this system is “Investigative Database—OMI—VA”(162VA10E1B). <https://www.govinfo.gov/content/pkg/FR-2020-02-07/pdf/2020-02482.pdf>.

1.6 **PRIVACY IMPACT ASSESSMENT: Characterization of the information**

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

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: Content Manager will contain both PII, PHI and a variety of other Sensitive Personal Information (SPI). Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious personal, professional, or financial harm may result.

Mitigation: In mitigation of moderate risk, the project shall adhere to all applicable security controls and ongoing patching recommendations. These controls include, but are not limited to: National Institute of Standards and Technology, Federal Information Processing Standard,

Version Date: October 1, 2022

Security Technical Implementation Guide and administrative oversight, as assessed and directed by appointed VA Security Officers. All additional mitigation requirements shall be governed by on-site, VA Network Security Operations Center and VA security professionals.

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.

Content Manager is used to aggregate the data involved in OMI investigations. All data collected within the system depends on each individual investigation. A 'name' collected within the system, could be a patient name in one investigation or it could be an employee name in another. It's all situationally dependent for "ALL the data types listed User level data may include:

SSN: Used as a patient identifier.

Phone Number: Used to contact the individual.

DoB: Used to identify patient age and confirm patient identity

Health Insurance Beneficiary Account Numbers: Used to communicate and bill third party health care plans

Other Unique Identifying Number - This system may have documents submitted to it from any agency record, which includes all VHA system of records. There could be another unique identifying number from those systems or in the future, for which we cannot account for. Please provide response here

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

These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

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

Content Manager does not perform any type of analysis. The system does not create or make new or unutilized information.

2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for

the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

The system does not create or make new or unutilized information.

2.3 How is the information in the system secured?

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

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

Permission to access the system is given by the Director of our service. The OMI office coordinates w/ OI&T to have a technician apply the application to the new staff GFE. OMI has an installation disc w/ Keys for HP TRIM. Access is removed when staff leave the OMI office by OI&T. Controls are in place to ensure data is used and protected in accordance with legal requirements, VA policies, and VA's stated purpose for using the data. Controls include mandatory training completion for all employees, volunteers, and contractors. Additionally, audits are performed to ensure information is accessed and retrieved appropriately. VA has implemented required security and privacy controls for Federal information systems and organizations according to NIST SP 800-53 and VA Handbook 6500, Risk Management Framework for VA Information Systems.

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

Micro Focus SecureData: Enables Structured Data Manager to protect sensitive data as it moves across the IT ecosystem, at rest, in motion and in use, without gaps in security.

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

Access is controlled by authentication and is restricted to authorized individuals. Tagence security policies address the required security controls that must be followed in order to protect PII.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?

This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

2.4a How is access to the PII determined?

Permission to access the system is given by the Director of our service. The OMI office coordinates w/ OI&T to have a technician apply the application to the new staff GFE. OMI has a installation disc w/ Keys for CONTENT MANAGER. Access is removed when staff leave the OMI office by OI&T.

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

Controls are in place to ensure data is used and protected in accordance with legal requirements, VA policies, and VA's stated purpose for using the data. Controls include mandatory training completion for all employees, volunteers, and contractors. Additionally, audits are performed to ensure information is accessed and retrieved appropriately. VA has implemented required security and privacy controls for Federal information systems and organizations according to NIST SP 800-53 and VA Handbook 6500, Risk Management Framework for VA Information Systems.

2.4c Does access require manager approval?

Permission to access the system is given by the Director of our service. The OMI office coordinates w/ OI&T to have a technician apply the application to the new staff GFE. OMI has a installation disc w/ Keys for CONTENT MANAGER. Access is removed when staff leave the OMI office by OI&T.

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

Yes, access to the PII being monitored, tracked, or recorded.

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

Each user is responsible for assuring safeguards for the PII.

Section 3. Retention of Information

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

*Identify and list all information collected from question 1.1 that is **retained** by the system. This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal*

- 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)
- Health Insurance Beneficiary Numbers
- Certificate/License numbers*
- Internet Protocol (IP) Address Numbers
- Medications
- Medical Records
- Race/Ethnicity
- Tax Identification Number
- Medical Record Number
- Gender
- Military History/Service Connection

3.2 How long is information retained?

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

Documents, memoranda, reports, and other records related to quality assurance investigations are destroyed 10 years after closure of the case or assessment. Site visit reports and other record documents related to site visits are destroyed 20 years after closure of case or assessment.

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

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner. Please work with the system Privacy Officer and VA Records Officer to answer these questions. This question is related to privacy control DM-2, Data Retention and Disposal.

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

Yes, complies with all VA retention and disposal procedures specified in VA Handbook 6300 and VA Directive 6300. The records are disposed of in accordance with Office of the Medical Inspector (10E1B) of the Veterans Health Administration Records Control Schedule (RCS) 10-1 (1160.1 Medical Inspector's Investigation Records and 1160.2 Medical Inspector Site Visit Record.) <https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf>.

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

RCS 10-1, 1160.1 Medical Inspector's Investigation Records, disposition authority N1-015-94-1 item 1a, and 1160.2 Medical Inspector Site Visit Record, disposition authority N1-015-94-1 item 1b.

3.4 What are the procedures for the elimination or transfer of SPI?

Explain how records are destroyed, eliminated or transferred to NARA at the end of their mandatory retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc.? This question is related to privacy control DM-2, Data Retention and Disposal.

We will not export data for retention. All data will be retained within CONTENT MANAGER until it is required to be deleted according to the Record Control Schedule 10-1. When required, this data is deleted from their file location. Digital media is shredded or sent out for destruction per VA Handbook 6500.1. The records are disposed of in accordance with Office of the Medical Inspector (10E1B) of the Veterans Health Administration Records Control Schedule 10-1 (1160.1 Medical Inspector's Investigation Records and 1160.2 Medical Inspector Site Visit Record.)

3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

No, system is not tested, and research is not conducted with the data.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk to maintaining data within CONTENT MANAGER as the information could be compromised or breached which is moderate.

Mitigation: OMI collects only the data necessary to meet the requirements of the investigations assigned. To further mitigate the risk posed by information retention, CONTENT MANAGER adheres to the VA RCS schedules for each category or data it maintains. When the retention data is reached for a record, OMI will carefully dispose of the data by the determined method as described in question 3.4. All electronic storage media used to store, process, or access OMI records will be disposed of in adherence with the latest version of VA Handbook 6500.1, Electronic Media Sanitization.

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

<i>List the Program Office or IT System information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</i>	<i>Describe the method of transmittal</i>
NA	NA	NA	NA

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Privacy Risk: None.

Mitigation: None

Section 5. External Sharing/Receiving and Disclosure

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

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

Is the sharing of information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal

mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.

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

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

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

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

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.

This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

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

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 no data being shared outside of the Department.

Mitigation: None.

Section 6. Notice

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

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

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

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

All information will be gathered from other SOR's or agency records. The notices if applicable will be provided by the other VA services that are responsible for their respective SOR's. SORN 162VA10E1B "Investigative Database—OMI—VA" applies to this system and it is available to the public in the federal register. <https://www.govinfo.gov/content/pkg/FR-2020-02-07/pdf/2020-02482.pdf>

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

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



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

The information obtained may be included in systems of records, including, but not limited to, “Veteran, Employee, and Citizen Health Care Facility Investigation Records,” 32VAOO, and is subject to the routine uses of such systems. These uses may include internal administration of the Department of Veterans Affairs, correction of systemic problems, determination of liability for claims and benefits, administrative or disciplinary action, actions affecting professional licenses and employment, and provision of information about the matter investigated to other federal and state agencies, Congress, and the public.

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 witnesses have the right to decline to provide information and there is no penalty for not responding.

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.

Individuals do not have the right to consent to particular uses of the information.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

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

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

Follow the format below:

Privacy Risk: Content Manager will contain both PII, PHI and a variety of other Sensitive Personal Information (SPI). Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious personal, professional, or financial harm may result.

Mitigation: In mitigation of moderate risk, the project shall adhere to all applicable security controls and ongoing patching recommendations. These controls include, but are not limited to: NIST, FIPS, STIG and administrative oversight, as assessed and directed by appointed VA Security Officers. All additional mitigation requirements shall be governed by on-site, VA NSOC and VA security professionals.

Section 7. Access, Redress, and Correction

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

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

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

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

A FOIA request for records can be made to the VHA Privacy Office.

https://department.va.gov/foia/foia-requests/#toc_How_are_VA_FOIA_Requests_Handled

7.1b If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR).

The system is not exempt from the access provisions of the Privacy Act.

7.1c If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information.

The system is not exempt from the access provisions of the Privacy Act.

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.

If records requested under the FOIA were determined to be inaccurate or erroneous, individuals would be referred to the Privacy Officer at the facility where the records were created. Individuals are required to provide a written request to amend or correct their records to the appropriate Privacy Officer or System Manager as outlined in the Privacy Act SORN. Every Privacy Act SOR contains information on Contesting Record Procedure which informs the individual who to contact for redress. Further information regarding access and correction procedures can be found in the notices listed in Appendix A. The VHA Notice of Privacy Practices also informs individuals how to file an amendment request with VHA.

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.

Veterans are informed of the amendment process by many resources to include the VHA Notice of Privacy Practice (NOPP) https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946 which states:

Right to Request Amendment of Health Information.

You have the right to request an amendment (correction) to your health information in our records if you believe it is incomplete, inaccurate, untimely, or unrelated to your care. You must submit your request in writing, specify the information that you want corrected, and provide a reason to support your request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains your information.

If your request for amendment is denied, you will be notified of this decision in writing and provided appeal rights. In response, you may do any of the following:

- File an appeal
- File a “Statement of Disagreement”
- Ask that your initial request for amendment accompany all future disclosures of the disputed health information

Additional notice is provided through the SORS listed in 6.1 of this PIA and through the Release of Information Office where care is received.

7.4 If no formal redress is provided, what alternatives are available to the individual?

*Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. **Example: Some projects allow users to directly access and correct/update their information online. This helps ensure data accuracy.***

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

Redress is provided via the processes outlined in questions 7.2 and 7.3.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

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

Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?

This question is related to privacy control IP-3, Redress.

Follow the format below:

Privacy Risk: Content Manager will contain both PII, PHI and a variety of other Sensitive Personal Information (SPI). Due to the highly sensitive nature of this data, there is a risk that, if

the data were accessed by an unauthorized individual or otherwise breached, serious personal, professional, or financial harm may result.

Mitigation: In mitigation of moderate risk, the project shall adhere to all applicable security controls and ongoing patching recommendations. These controls include, but are not limited to: NIST, FIPS, STIG and administrative oversight, as assessed and directed by appointed VA Security Officers. All additional mitigation requirements shall be governed by on-site, VA NSOC and VA security professionals.

Section 8. Technical Access and Security

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

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

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

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

User roles identify the information and applications a user can access. To receive access to the CONTENT MANAGER the system administrator must grant them access.

8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

No one other than those assigned to the Office of the Medical Inspector will have access to CONTENT MANAGER.

8.1c Describe the different roles in general terms that have been created to provide access to the system. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

The Office of the Medical Inspector staff is comprised of Physicians, Nurses and Administrative support staff. All staff assigned to the Office of the Medical Inspector have full access to CONTENT MANAGER

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.

No, VA contractors will not have access to CONTENT MANAGER.

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.

Initial and annual Security Awareness Training to include HIPAA Privacy and Security training, includes security best practices, threat recognition, privacy, compliance and policy requirements, and reporting obligations. Upon completion of training, personnel must complete a security and privacy quiz with a passing score. All required VA privacy training must be completed in the VA Talent Management System prior to the user being provisioned.

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

8.4a Yes, provide:

- 1. The Security Plan Status: Complete.*
- 2. The System Security Plan Status Date: 05/23/2023*
- 3. The Authorization Status: Authorization to Operate (ATO)*
- 4. The Authorization Date: 07/16/2023*
- 5. The Authorization Termination Date: 07/07/2025*
- 6. The Risk Review Completion Date: 07/07/2023*
- 7. The FIPS 199 classification of the system (LOW/MODERATE/HIGH): Moderate*

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

Section 9 – Technology Usage

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

9.1 Does the system use cloud technology? If so, what cloud model is being utilized?

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1. (Refer to question 3.3.1 of the PTA)

The system does not utilize cloud.

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

The system does not utilize cloud.

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.

The system does not utilize cloud.

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

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

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

The system does not utilize cloud.

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).

NA

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.

Privacy Officer, Phillip Cauthers

Information Systems Security Officer, Kehinde A. Talabi

Information Systems Owner, Elmer Clark

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).

SORN 162VA10E1B “Investigative Database—OMI—VA”, <https://www.govinfo.gov/content/pkg/FR-2020-02-07/pdf/2020-02482.pdf>

The VHA Notice of Privacy Practice (NOPP),
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946

HELPFUL LINKS:

Record Control Schedules:

<https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf>

General Records Schedule 1.1: Financial Management and Reporting Records (FSC):

<https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf>

National Archives (Federal Records Management):

<https://www.archives.gov/records-mgmt/grs>

VHA Publications:

<https://www.va.gov/vhapublications/publications.cfm?Pub=2>

VA Privacy Service Privacy Hub:

<https://dvagov.sharepoint.com/sites/OITPrivacyHub>

Notice of Privacy Practice (NOPP):

[VHA Notice of Privacy Practices](#)

[VHA Handbook 1605.04: Notice of Privacy Practices](#)