



Privacy Impact Assessment for the VA IT System called:

## Salesforce - VA Integrated Enterprise Workflow Solution Case and Correspondence Management (VIEWS CCM)

Office of the Executive Secretariat (EXECSEC)

VA Central Office (VACO)

Date PIA submitted for review:

3/7/2024

### System Contacts:

	Name	E-mail	Phone Number
Privacy Officer	Gina Siefert	<a href="mailto:Gina.Siefert@va.gov">Gina.Siefert@va.gov</a>	(202) 632-8430
Information System Security Officer (ISSO)	James Boring	<a href="mailto:James.Boring@va.gov">James.Boring@va.gov</a>	(215) 842-2000 x4613
Information System Owner	Michael Domanski	<a href="mailto:Michael.Domanski@va.gov">Michael.Domanski@va.gov</a>	(727) 595-7291

### **Abstract**

*The abstract provides the simplest explanation for “what does the system do?”*

Salesforce - VA Integrated Enterprise Workflow Solution Case and Correspondence Management (VIEWS CCM) is used by the Office of the Executive Secretariat (EXECSEC) VA staff and program

offices to conduct administrative and correspondence-related work. VIEWS CCM is also used to coordinate documents and materials related to partnerships with other Federal organizations, state, local, tribal, and non-governmental organizations (NGOs) and individuals, as well as international governments and private sector organizations. VIEWS CCM is used to manage Congressional correspondence; internal documents such as reports, memoranda, and handbooks; respond to White House case mail; and assist Veterans making inquiries about VA programs, services, and benefits. VIEWS CCM is used by all VA administrations and program and staff offices and is a National Archives and Records Administration (NARA)-certified system of record.

## Overview

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

### 1. General Description

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

Salesforce - VA Integrated Enterprise Workflow Solution Case and Correspondence Management (VIEWS CCM). The Office of the Executive Secretariat (EXECSEC) is the VIEWS CCM business owner. The Office of Information and Technology (OIT) is the system owner.

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

VIEWS CCM supports Case and Correspondence Management within the VA and with the Veteran. The system facilitates correspondence of any form (emails, letters, and any other communication internal or external to the VA), workflow/tasking, case management, and project/event tracking. VIEWS CCM also provides managers with robust reporting, data management, and business intelligence capabilities to drive informed decision making.

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

VIEWS CCM is VA Owned and non-VA Operated.

### 2. Information Collection and Sharing

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

VIEWS CCM stores information on system users and other persons who have initiated a case or are involved in subsequent processing. There are approximately 1,800 system users. Currently, 300,000 to 400,000 persons' information may be stored in the system. These individuals, which could include any Veteran or other persons (VA employees and contractors) that have business with the Department, are related to the correspondence received by the VA.

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

VIEWS CCM collects, processes, or retains information on Veterans, their dependents, beneficiaries, caregivers, other related contacts as well as VA employees and contractors. VIEWS CCM also collects data associated with current and former Members of Congress, Officers, and their Staff. This information is collected from Congress KnowWho for Salesforce and is information that is publicly available. Data entered is directly related to correspondence received, including information on the person who sent the request and information contained within the correspondence. As the correspondence is being tracked, additional information may be added to the system regarding the response of the question(s).

Case records contain information about the correspondence, including summary description, associated contacts description, Veteran (if applicable), case progress, associated VA facilities, related emails and attachments (associated documents), and other details.

Each case is assigned a record type, which indicates if the case is external (Veteran, Congressional or Presidential) or internal documents (such as memos, reports, handbooks, or correspondence). A case team consists of organizations (groups of Salesforce users associated with a VA office, department or organization) or individuals that will work on a case. They can be added or removed as necessary by the case owner, other case team members and office coordinators. Case tasks are actions that are taken and assigned to case team members, such as reviewing, concurring, signing, or closing.

VIEWS CCM objects ("data tables") contain data associated with VA staff, cases, case team members, associated contacts, internal and external organizations (Accounts), VA Facilities, case-related emails, notes, meetings and tasks.

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

The system shares information with Identity and Access Management (IAM) and the Master Person Index (MPI), formerly known as Master Veterans Index (MVI). to validate the Veteran's identity. MPI is the VA's authoritative source for personal identity data, providing a universal, unique identification record for Veterans, dependents, caregivers, beneficiaries, and other associated persons. The MPI integration in VIEWS CCM also serves as a searchable database of verified Veteran contact information. VIEWS CCM maintains an integration with MPI, allowing users to search the MPI database, verify a Veteran's identity, and retrieve contact data from MPI into Salesforce. MPI contains PII, including name, email, social security number (SSN), birth date, eligibility status, and more. The legal authority is 38 U.S.C. 7601-7604 and U.S.C 7681-7683 and Executive Order 9397.

Congress KnowWho is a Salesforce App Exchange product that provides a directory of contact and biographical data on all Members of Congress (MOC), Capitol Hill staffers, committees, and caucuses. The Congress KnowWho integration allows case owners to search for and attach MOC, their staffers, and other VA facilities directly to a case as an associated contact.

The Congress KnowWho database includes publicly available information which includes Congressional mailing address, phone number, fax number, email addresses, social media URLs, committee memberships and other information. Congressional data provided by the Congress KnowWho is used to coordinate legislative proposals, manage activities with Congress, or respond to congressional constituents. The directory delivers daily updates to VIEWS CCM as a commercial service. Congress KnowWho uses Salesforce standard objects for loading publicly available information.

The Functional Organization Manual (FOM) System, another VIEWS CCM integration, maintains a hierarchy of organizations (queues) that can be assigned to a case. A VIEWS CCM user can associate persons within an organization to a case via case team functionality. The Functional Organization Manual (FOM) System does not contain PHI/PII.

*G. Is 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?*

All VA administrations, program and staff offices use VIEWS CCM. System users may also log in remotely. VIEWS CCM is operated at VA Central Office (VACO) in several Washington, DC locations. User controls built into the system manage PII identically at all locations. No regions, hospitals, medical centers, or any other agency use the system.

### *3. Legal Authority and SORN*

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

The legal authority is 38 U.S.C. 7601-7604, U.S.C 7681-7683, Executive Order 9397 and System of Record Notice (SORN): Case and Correspondence Management (CCM)-VA 75VA001B/ 87 FR 36584

VIEWS CCM has a FedRAMP agency authorization date of November 2, 2020. The Federal Information Processing Standards (FIPS) 199 classification is Moderate. An ATO was granted on August 7, 2023 and expires on August 8, 2025.

*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 does not require amendment or revision and approval.

### *4. System Changes*

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

Completion of this PIA is not expected to require changes to any business processes.

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

Completion of this PIA is not expected to require any 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://vaww.va.gov/vapubs/>). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.

This question is related to privacy control AP-1, Authority To Collect, and AP-2, Purpose Specification.

*The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1. It must also match the information provided in question 3.4 of the PTA.*

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

- |                                                                      |                                                                   |                                                                      |
|----------------------------------------------------------------------|-------------------------------------------------------------------|----------------------------------------------------------------------|
| <input checked="" type="checkbox"/> Name                             | Number, etc. of a different individual)                           | <input type="checkbox"/> Tax Identification Number                   |
| <input checked="" type="checkbox"/> Social Security Number           | <input type="checkbox"/> Financial Information                    | <input type="checkbox"/> Medical Record Number                       |
| <input checked="" type="checkbox"/> Date of Birth                    | <input type="checkbox"/> Health Insurance Beneficiary Numbers     | <input type="checkbox"/> Gender                                      |
| <input checked="" type="checkbox"/> Mother's Maiden Name             | Account numbers                                                   | <input type="checkbox"/> Integrated Control Number (ICN)             |
| <input checked="" type="checkbox"/> Personal Mailing Address         | <input type="checkbox"/> Certificate/License numbers <sup>1</sup> | <input type="checkbox"/> Military History/Service Connection         |
| <input checked="" type="checkbox"/> Personal Phone Number(s)         | <input type="checkbox"/> Vehicle License Plate Number             | <input type="checkbox"/> Next of Kin                                 |
| <input checked="" type="checkbox"/> Personal Fax Number              | <input type="checkbox"/> Internet Protocol (IP) Address Numbers   | <input checked="" type="checkbox"/> Other Data Elements (list below) |
| <input checked="" type="checkbox"/> Personal Email Address           | <input type="checkbox"/> Medications                              |                                                                      |
| <input type="checkbox"/> Emergency Contact Information (Name, Phone) | <input type="checkbox"/> Medical Records                          |                                                                      |
|                                                                      | <input type="checkbox"/> Race/Ethnicity                           |                                                                      |

Other PII/PHI data elements:

- VA Email Address

---

<sup>1</sup> \*Specify type of Certificate or License Number (e.g., Occupational, Education, Medical)

- VA Work Phone Number
- Place of Birth

**PII Mapping of Components (Servers/Database)**

VIEWS CCM consists of one key component. This component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by VIEWS CCM and the reasons for the collection of the PII are listed in the table below.

**Note:** Due to the PIA being a public facing document, please do not include server names in the table.

The first table of 3.9 in the PTA should be used to answer this question.

*Internal Components Table*

<b>Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI</b>	<b>Does this system collect PII? (Yes/No)</b>	<b>Does this system store PII? (Yes/No)</b>	<b>Type of PII (SSN, DOB, etc.)</b>	<b>Reason for Collection/ Storage of PII</b>	<b>Safeguards</b>
VA Salesforce Development Platform (SFDP) VA SFGCP, via Business Partner Extranet (BPE) Connection	Yes	Yes	Name, Personal Phone, Personal Email, Date of Birth, Personal Mailing Address, SSN, Gender, Mother’s Maiden Name	To support case and correspondence management within the VA and with the Veteran, Verification of Identity	Access to VIEWS CCM is strictly controlled by Single Sign On (SSO) to authorized VA personnel only. Salesforce is FedRAMP (Moderate) approved. SFGCP uses cryptography that is compliant with Federal laws and regulations FIPS 140-2. All PII is encrypted in transport and at rest. Profile-based permissions govern access. User profiles are reviewed regularly to ensure appropriate access.

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
					VA employees and contractors are required to complete the VA Privacy and Information Security training annually.

**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 system receives information from the entry of cases with data provided from any type of correspondence with the VA (email, regular mail, phone call, and so on). Additionally, the system consumes Global Address List (GAL) (Outlook email account) data that contains email and work phone number information for VA employees and contractors. Veteran information is brought into the system via lookup through a real-time interface with MPI. Information about current and former Members of Congress, Officers and Staff is brought in via Congress KnowWho for Salesforce.

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

Information in the VIEWS CCM application is manually entered or uploaded as documents by an authorized VIEWS CCM user, who can be a VA employee or contractor. Email-to-case functionality allows related emails to be entered with the case. In cases where validation of Veteran status is needed, the information and data will be collected from the incoming correspondence and validated by the system’s access to the MPI integration. Information that cannot be validated will be saved as non-verified and contact information will be retained for the correspondence.

If Congressional data is needed for a case, Congress KnowWho provides a lookup capability of biographical data on all MOCs, Capitol Hill staffers, committees, and caucuses. This data is also publicly available.

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

Yes, Salesforce has native report and dashboard creating functionality. Users can use these features to create list views, reports and dashboards from any of the data collected in Salesforce.

### **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?*

Information in the VIEWS CCM application is manually entered or uploaded as documents by an authorized VIEWS CCM user, who can be a VA employee or contractor. Email-to-case functionality allows related emails to be entered with the case. In the cases where validation of Veteran status is needed, the information and data will be collected from the incoming correspondence and validated by the system's access to the MPI integration. Information that cannot be validated will be saved as non-verified, and contact information will be retained for the correspondence.

If Congressional data is needed for a case, Congress KnowWho provides a lookup capability of biographical data on all MOCs, Capitol Hill staffers, committees, and caucuses. This data is also publicly available.

*1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, what is the form's OMB control number and the agency form number?*

Information is not collected on a form and is not subject to the Paperwork Reduction Act.

### **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.*

VIEWS CCM uses the MPI database to verify and confirm Veteran identity. The VIEWS CCM user interface includes a visual workflow for users to enter Social Security Number and date of birth, which makes a call to the MPI database to verify the identity and pull the information into a verified Veteran contact record type. The contact record is marked as a verified Veteran and contains the MPI



external ID, which is used to match against the MPI database and update information from MPI to Salesforce.

Other SPI information may be stored as part of routine case management but not validated by the system for data accuracy or corruption.

*1.4b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?*

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

### **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*

- 5 U.S.C. § 552a, Freedom of Information Act of 1996, As Amended by Public Law No. 104---231, 110 Stat. 3048
- 5 U.S.C. § 552a, Privacy Act of 1974, As Amended
- Public Law 100---503, Computer Matching and Privacy Act of 1988
- E---Government Act of 2002 § 208
- Federal Trade Commission Act § 5
- 44 U.S.C. Federal Records Act, Chapters 21, 29, 31, 33
- Title 35, Code of Federal Regulations, Chapter XII, Subchapter B
- OMB Circular A---130, Management of Federal Information Resources, 1996
- OMB Memo M---10---23, Guidance for Agency Use of Third---Party Websites
- OMB Memo M---99---18, Privacy Policies on Federal Web Sites
- OMB Memo M---03---22, OMB Guidance for Implementing the Privacy Provisions
- OMB Memo M---07---16, Safeguarding Against and Responding to the Breach of PII
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) State Privacy Laws

The legal authority is 38 U.S.C. 7601-7604 and U.S.C 7681-7683 and Executive Order 9397.

### **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.

**Privacy Risk:** SPI, including personal contact information, and SSN may be released to unauthorized individuals. Unsecured SPI, including personal contact information, and SSN may be exposed.

**Mitigation:** Profile-based permissions govern user access to information. The profiles are reviewed bi-Annual basis to ensure that information is shared only with appropriate users. All employees with access to Veterans' information are required to complete the VA Privacy and Information Security Awareness and Rules of Behavior training annually. VIEWS CCM ensures that only authorized users can access SPI. Assigned data security rules determine which data users can access. All data is encrypted in transfer. Access is governed via Single Sign On (SSO). All passwords are stored in Secure Hash Algorithm (SHA) 256 one-way hash format.

## Section 2. Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

### 2.1 Describe how the information in the system that will be used in support of the program's business purpose.

Identify and list each use (both internal and external to VA) of the information collected or maintained. This question is related to privacy control AP-2, Purpose Specification.

PII/PHI Data Element	Internal Use	External Use
Name	Verify person's identity	Not used
Social Security Number	Verify person's identity	Not used
Date of Birth	Verify person's identity	Not used

<b>PII/PHI Data Element</b>	<b>Internal Use</b>	<b>External Use</b>
<b>Mother's Maiden Name</b>	Verify person's identity	Not used
<b>Mailing Address</b>	Used for communication	Not used
<b>Phone Number(s) (Personal and VA)</b>	Used for communication	Not used
<b>Email Address (Personal and VA)</b>	Used for communication	Not used
<b>Gender</b>	Verify person's identity	Not used
<b>Place of Birth</b>	Verify person's identity	Verify person's identity

**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.*

VIEWS CCM does not include tools to perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting or pattern analysis.

*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?*

There is no Integrated or built-in analysis tool that is analyzing the data or providing summary details related to it. VIEWS CCM does not include tools to perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting or pattern analysis.

*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 VIEWS CCM user policy states that only authorized users can access sensitive personal information, including SSNs, and then only for legitimate authorized business purposes. Data security rules, including the use of electronic permission sets within the Salesforce platform, determine which information users can access. Technical controls include secure encryption using

VA Personal Identity Verification (PIV) credential procedures, role-based authentication, firewalls, and virtual private networks which protect the data in transit and during storage. Access to information in VIEWS CCM is also governed by password security policies and dual-factor authentication. A government issued PIV card with PIN number are required to log in to VIEWS CCM and these login activities are recorded in log file.

### **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?*

Technical controls include secure encryption using VA Personal Identity Verification (PIV) credential procedures, role-based authentication, firewalls, and virtual private networks which protect the data in transit and during storage. Access to information in VIEWS CCM is also governed by password security policies and dual-factor authentication. A government issued PIV card with PIN number are required to log in to VIEWS CCM and these login activities are recorded in log file. VIEWS CCM has different user roles (CCM Standard User, VOC User, ExecSec Team User, Super User). Each user role has varying levels of Permission Sets that determine (a) what records they have access to and (b) what fields within those records they have visibility of.

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

The VIEWS CCM user policy states that only authorized users can access sensitive personal information, including SSNs, and then only for legitimate authorized business purposes. Data security rules, including the use of electronic permission sets within the Salesforce platform, determine which information users can access. SSN is encrypted in Transit and at Rest. It's masked when at rest (only the last four are show, in this format: \*\*\*.\*\*.\*\*\*\*). \*\*\*\* is the number visible to people working on Sensitive cases for Veterans.

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

Users are directed to set the record "Sensitivity" level based on the presence of PII/PHI/SPI. If a VIEWS CCM Case is set to "Sensitive", its visibility is limited on a need to know basis: only the record owner and case team members (users specifically assigned to the case) are able to view the record.

### **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.*

VIEWS CCM utilizes the Salesforce Government Cloud Plus. Users must be approved by their manager to have a user login created. Once access is granted, users must log into Salesforce via Single Sign On (SSO) for verification.

Controls are in place to ensure data is used and protected in accordance with legal requirements, VA policies, and VA's stated purpose for data usage. Controls include mandatory training completion for all employees, volunteers, and contractors.

All system access is logged. Users of the system (VA employees and contractors) are individually responsible for appropriate system usage. Misuse of information may result in employment termination or legal or civil penalties, as appropriate by law.

Additionally, audits are performed to ensure information is accessed and retrieved appropriately. New accounts added to VIEW CCM must be approved by a manager. VA and Salesforce have implemented required security and privacy controls for Federal information systems and organizations according to NIST SP 800-53 and VA Directive 6500.1, Risk Management Framework for VA Information Systems. All controls are per the approval of the Acting Assistant Secretary for information Technology [the VA Designated Accrediting Authority (DAA)].

*2.4a How is access to the PII determined?*

Access to CCM and PII stored therein is limited to VA employees who have a bona fide business need to use the system, and only after they have completed the required training and obtained written permission from their manager. Ongoing access to CCM is reviewed and re-validated on a quarterly basis. Access to PII in VIEWS CCM is determined by the use of case category selections and business rules associated with the "Case Sensitivity" field, one of the standard database fields on the Case object. All cases must be designated as "Sensitive" or "Not Sensitive" by the selection of an option on the Case Sensitivity field. A case designated as "Sensitive" can be accessed (located, viewed, and updated) only by CCM users who are designated as a "Case Team Member" for that specific case. CCM users who are not a "Case Team Member" cannot view or edit these cases. Cases designated as "Not Sensitive" can be located, viewed, and updated by any CCM user, regardless of whether they are a Case Team Member. Further, CCM users select from among 21 different case record types, or categories, when creating new cases. Case categories are used to classify, organize, and secure correspondence and similar records and associated information. Five specially designated case record types are deemed likely to contain PII or other sensitive information and have been configured to automatically be designated as "Sensitive" when they are created. These five case record types are: (1) Congressional Letter, (2) Investigations and Audits (Non-GAO), (3) Personnel Matters, (4) Veteran and Congressional Case Mail, and (5) White House Case Mail. Users may not change the Case Sensitivity field on these cases by themselves, however they may request, under very limited circumstances, to change the Case Sensitivity on Congressional Letter cases changed to

“Not Sensitive.” Such change requests are logged along with the business rationale or justification for making the change. The other 16 case record types of default to “Not Sensitive” upon creation. Any Case Team Member may upgrade the Case Sensitivity to “Sensitive” when needed to align with PII and SPI data security rules if such information is ever added to these cases.

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

VA and Salesforce have implemented required security and privacy controls for Federal information systems and organizations according to NIST SP 800-53 and VA Directive 6500.1, Risk Management Framework for VA Information Systems. All controls are per the approval of the Acting Assistant Secretary for information Technology [the VA Designated Accrediting Authority (DAA)]

*2.4c Does access require manager approval?*

New accounts added to VIEW CCM must be approved by a manager. Managers must also approve users to have a user login created. Once access is granted, users must log into Salesforce via Single Sign On (SSO) for verification.

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

All system access is logged, including access to PII. Audits are performed to ensure information is accessed and retrieved appropriately.

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

Users of the system (VA employees and contractors) are individually responsible for appropriate system usage. Misuse of information may result in employment termination or legal or civil penalties, as appropriate by law.

## **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 (Last four digits)
- Date of Birth (DoB)
- Mother’s Maiden Name
- Mailing Address

- Phone Number (Personal and VA)
- Email Address (Personal and VA)
- Gender

### **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.*

Information retained pursuant to the VIEWS record schedule, under Disposition Authority Number DAA-0015-2018-0002, is retained permanently.

### **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.*

Yes, the retention schedule was approved by the VA Office of Information Technology – Enterprise Records Office on 1/9/2018 and by the National Archives and Records Administration (NARA) on 2/13/2019.

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

Yes, VIEWS CCM complies with all VA retention and disposal procedures specified in VA Handbook 6300 and VA Directive 6300.1. Records Management Procedures. Records contained in the Salesforce FedRAMP cloud will be retained as long as the information is needed in accordance with a NARA-approved retention period. VA manages Federal records in accordance with NARA statutes, including the Federal Records Act (44 U.S.C. Chapters 21, 29, 31, 33) and NARA regulations (36 CFR Chapter XII Subchapter B).

VIEWS CCM records are retained according to:

**Disposition Authority Number:** DAA-0015-2018-0002

**Product Name:** Veterans Affairs Integrated Enterprise Workflow Solution (VIEWS)

**Records subject to this schedule:** Program office primary program records including the following: all documents signed by mast-head VA employees and/or if these records meet the following requirements: •Programs specially listed in the Secretary of VA goals and/or specifically listed in the goals of the VA Deputy Secretary, Undersecretaries or Assistant Secretaries. •High level plans and policies that affect the long term ((25) years) delivery of healthcare and benefits to Veterans and their families. •Programs specially ordered by the President through Executive Order or Congress of the United States. •Briefings or reports to Congress of new VA policies or innovations that have a major impact on benefits delivered by VA.

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

**Series:**

1.0 Primary Program Files of VA Program Offices

Schedule:

Program Offices may be found at VA Central Office in Washington DC or in other locations such as medical centers and regional offices throughout the United States. Program Offices may be led by a member of the Senior Executive Service (SES) or a General Schedule (GS) 15. This records schedule applies to PERMANENT items. Records not identified as High Value are convenience copies of records maintained elsewhere under VA records schedules, with flexibility for retention according to business need built into the temporary item. The system employed to manage VIEWS will maintain the records organized based on the records' meta-data. This disposition applies to the predecessor tracking systems that VA has employed since 1995, including DTS, EDMS, CSIMS, WebCIMS, and VAIQ/Sims.

Final Disposition:

Permanent

**Series:**

1.1 High Value Primary Program Records Maintained in VIEWS and Predecessor Systems

Schedule:

Program office primary program records may include the following, but are not limited, to: all documents approved by mast-head VA employees and/or if these records meet the following requirements: •Programs specially listed in the Secretary of VA goals and/or specifically listed in the goals of the VA Deputy Secretary, Undersecretaries or Assistant Secretaries. •High level plans and policies that affect the long term (25 years) delivery of healthcare and benefits to Veterans and their families. •Programs specially ordered by the President through Executive Order or Congress of the United States. •Briefings or reports to Congress of new VA policies or innovations that have a major impact on benefits delivered by VA.

Final Disposition:

Permanent

**Disposition Authority Number:** DAA-0015-2018-0002

**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.*

Active data stays on disk until deleted or changed by the VA. The information is retained following the policies and schedules of VA's Records Management Service and National Archives and Records Administration (NARA) in "Department of Veterans Affairs General Records. VA exports and retains data to meet VA/NARA retention requirements and disposes of the exported data at the end of the retention period.

When hard drives and backup tapes reach end of life, the media is sanitized based on Salesforce's Media Disposal Policy. Hard drives are overwritten using a multi-pass write of complementary and random values. Successfully wiped disks or arrays will be returned to the vendor. Disks or arrays that fail during the wiping process will be retained and destroyed (in other words., degaussed, shredded, or incinerated). Backup tapes are degaussed prior to disposal. Specifics on the sanitization process are described below.

Salesforce has an established process to sanitize production backup disks and hard drives prior to disposal, release from Salesforce's control or release to the vendor for reuse. Production backup disks and hard drives are sanitized or destroyed in accordance with Salesforce's Media Handling Process. All data is handled and located in VA's own Salesforce servers in Herndon, VA and Chicago, IL in the Salesforce Government Cloud server classification. This information is handled with proper authority and scrutiny. Hard drives are sanitized within the data center facility using a software utility to perform a seven-pass overwrite of complementary and random values. Drives wiped successfully will be returned to the lessor. Drives that fail during the wiping process are retained in a locked container within the Salesforce data center facilities until onsite media destruction takes place. Leasing equipment allows Salesforce to use the latest equipment available from vendors.

Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and VA Handbook 6500.1 Electronic Media Sanitization. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destruction.

[https://www.va.gov/vapubs/search\\_action.cfm?dType=1](https://www.va.gov/vapubs/search_action.cfm?dType=1).

When required, this data is deleted from their file location and then permanently removed from the deleted items or Recycle Bin. Magnetic media is wiped and sent out for destruction per VA Directive 6500.1. Digital media is shredded or sent out for destruction per VA Directive 6500.1. The OIT Chief/CIO is responsible for identifying and training OIT staff on VA media sanitization policy and procedures. The Information Security Officer (ISO) coordinates and audits this process and documents the audit on an annual basis to ensure compliance with National media sanitization policy.

### **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.*

VIEWS CCM does use techniques to minimize the risk to privacy by avoiding the use of PII for research, testing, and training. VIEWS CCM is not used for research purposes; it is neither used for managing research projects nor is the database used for research project source material. VIEWS CCM test environments do not use PII. The VIEWS CCM testing teams do not have access to PII and are bound by policies strictly prohibiting its use for testing purposes of any kind. Rather than using PII, fictitious usernames and mock data are used in the testing databases to simulate software performance using data similar to that which is used in the production database. For example, when people's names are needed for Contact records, fictitious names such as "Mary Approver," "John Doe," and "Sally Sample" are used. Similarly, databases used for training purposes also use fictitious names and related mock biographical data where needed in training manuals, presentations, instructor guides, demonstrations, and student exercises. Access to all production databases or copies of production systems (the Staging database) that may contain PII is protected using two factor authentication (2FA), including Single Sign-On (SSO) technology to verify the user, and data access is granted based on permissions configured for each user and their approved, assigned role on the application.

### **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.*

**Privacy Risk:** There is a risk that PII is retained for longer than it is useful. If the data contained within VIEWS CCM does not follow the Records Control Schedule for data types, it could increase the risk that individually identifiable information can be inappropriately released or breached.

**Mitigation:** VIEWS CCM adheres to the VA Record Control Schedules for each category or data it maintains. VIEWS CCM also adheres to the NARA disposition authority. When the retention date is

Version date: October 1, 2023

Page 18 of 35

reached for a record, the VIEWS CCM team will carefully dispose of the data by the determined method.

**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>
Identity and Access Management Assessing (eMASS ID 0842)	Verify access credentials	Data Elements Sent: Name, VA Email address, VA Work Number	HTTPS
Master Person Index (MPI)	Verify person's identity	Data Elements Received: Name (First Name, Last Name, Middle Name, Suffix), SSN, Date of Birth, Gender, Address, Mother's Maiden Name, Personal Phone Number, Personal Mailing Address	HTTPS

<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>
VA Salesforce Government Cloud Plus (SFGCP)	Verify person's identity	Name, Personal Phone Number, Personal Email Address, Date of Birth, Personal Mailing Address, SSN, Gender, Mother's Maiden Name	HTTPS

#### **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:** Information may be shared with unauthorized VA personnel.

**Mitigation:** Safeguards, including employee security, privacy training, and required reporting of suspicious activity, are implemented to ensure data is not sent to unauthorized VA employees. VIEWS CCM security measures include secure passwords, access on a need-to-know basis, Personal Identification Verification (PIV) cards, Personal Identification Numbers (PIN), encryption, and access authorization.

## **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>
Congress KnowWho for Salesforce	Verify person's identity	Name, Date of Birth, Gender, Place of Birth	SORN 75VA001B Salesforce MOU	HTTPS

**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.

If no External Sharing listed on the table above, (**State there is no external sharing in both the risk and mitigation fields**).

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

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

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

Follow the format below:

**Privacy Risk:** The system does receive information (publicly available) from Congress KnowWho for Salesforce, if combined with other sensitive information can cause harm to the individual.

**Mitigation:** Safeguards are implemented to ensure data is used appropriately within the organization. To include employee security and privacy training and awareness and required reporting of suspicious activity. The use of secure passwords, access for need-to-know purposes, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption and access authorization are all measures that are utilized within VA.

## Section 6. Notice

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

**6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an Appendix-A 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.*

Notice is provided with publication in the Federal Registrar of the Case and Correspondence Management (CCM)-VA 75VA001B/ 87 FR 36584 SORN and the publicly available Privacy Impact Assessment (PIA) for the system.

[Privacy Act System of Records Notices \(SORNs\) - Privacy](#)

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

This is not applicable as notice is provided with publication in the Federal Registrar of the Case and Correspondence Management (CCM)-VA 75VA001B/ 87 FR 36584 SORN and the publicly available Privacy Impact Assessment (PIA) for the system

[Privacy Act System of Records Notices \(SORNs\) - Privacy](#)

*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.*

Case and Correspondence Management (CCM)-VA 75VA001B/ 87 FR 36584 SORN explains the purpose of the system, the categories of individuals covered by the system and how the information that is collected will be used. The SORN states: The purpose of the system is to permit VA to identify and respond to individuals and/or organizations who have submitted correspondence or documents to VA. The system contains documents generated within VA that may contain the names, addresses and other identifying information of individuals who conduct business with VA. The categories of individuals covered by the system are: Individuals who voluntarily provide personal contact information when submitting correspondence or other documents to the Department, including, but not limited to: Members of Congress and their staff, officials and representatives of other Federal agencies, State, local and tribal governments, foreign governments, and veterans service organizations; representatives of private or commercial entities; veterans and other VA beneficiaries; VA employees; and other individuals who correspond with the VA Secretary and Deputy Secretary and other VA officials.

**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.*

Individuals communicating with the VA do have the opportunity and right to decline to provide information. However, failure to provide requested identifying information may cause the denial of services, based on the totality of circumstances for each situation. Individuals may communicate with the VA anonymously, and they may decline to provide additional identifying information at their discretion. These situations may also cause the denial of service, or VA's inability to provide a response to anonymous correspondence. These situations are handled on a case-by-case basis. Information about individuals who correspond with VA is collected and stored in the system as described in the System of Record Notice (SORN). Both the SORN for Case and Correspondence Management (CCM)-VA 75VA001B/ 87 FR 36584 and Privacy Impact Assessment serve as public notice of these data collection policies.

[2022-13066.pdf \(govinfo.gov\)](#)

**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.*

Yes, Individuals have a right to consent to uses of their information. Individuals voluntarily provide information when submitting correspondence or other documents to the Department. If information is disclosed, it is done on behalf of the individual with a written request.

Per SORN 75VA001B: VA's authorization to disclose individually identifiable information to Members of Congress, or a staff person acting for the Member, when the Member or staff person requests the records on behalf of and at the written request of the individual.

#### **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.*

**Privacy Risk:** VA employees, Veterans and individuals that submit information for Veterans will not know that applications built on the SFDP collect, maintain and/or disseminate PII and other SPI about them.

**Mitigation:** The VA ensures that it provides individuals with a notice of information collection and notice of the system's existence through the methods discussed in question 6.1 which are through the System of Records Notice (SORN), Case and Correspondence Management (CCM)-VA 75VA001B/87 FR 36584. The VA provides the public with two forms of notice that the system exists, including the Privacy Impact Assessment (PIA) and the SORN. This PIA is a form of notice.

[2022-13066.pdf \(govinfo.gov\)](https://www.gpo.gov/foia/2022-13066.pdf)

## **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.***

Individuals may request information that VIEWS CCM may have on them either via a Freedom of Information Act (FOIA) (via the VA Freedom of Information Act Public Access Website, <https://vapal.foia-host.com/app/Home.aspx>) or a Privacy Act Request. Individuals who wish to determine whether a record is being maintained in this system under his or her name or other personal identifier, or wants to determine the contents of such record, should submit a written request to the U.S. Department of Veterans Affairs, 810 Vermont Avenue, NW., Washington, DC 20420.

*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)?*

This system is not exempt from the access provisions of the Privacy Act. Individuals seeking information on the existence and content of records in this system pertaining to them should refer to Case and Correspondence Management (CCM)-VA 75VA001B/ 87 FR 36584 SORN to contact the system manager in writing, Office of the Executive Secretary, Office of the Secretary, Department of Veterans Affairs, 810 Vermont Avenue NW, Washington, DC 20420, (202) 461-4869, [VAExecSec@va.gov](mailto:VAExecSec@va.gov).) A request for access to records must contain the requester's full name, address, telephone number, be signed by the requester, and describe the records sought in sufficient detail to enable VA personnel to locate them with a reasonable amount of effort. [2022-13066.pdf \(govinfo.gov\)](#)

*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?*

Individuals seeking information on the existence and content of records in this system pertaining to them should contact the system manager in writing Office of the Executive Secretary, Office of the Secretary, Department of Veterans Affairs, 810 Vermont Avenue NW, Washington, DC 20420, (202) 461-4869, [VAExecSec@va.gov](mailto:VAExecSec@va.gov).) A request for access to records must contain the requester's full name, address, telephone number, be signed by the requester, and describe the records sought in sufficient detail to enable VA personnel to locate them with a reasonable amount of effort.

## **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.*

Individuals seeking to contest or amend records in this system pertaining to them should contact the system manager in writing as indicated above. A request to contest or amend records must state clearly and concisely what record is being contested, the reasons for contesting it, and the proposed amendment to the record.

### **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.*

The SORN and the PIA are ways that individuals are notified. Individuals seeking to contest or amend records in this system pertaining to them should contact the system manager in writing as indicated above. A request to contest or amend records must state clearly and concisely what record is being contested, the reasons for contesting it, and the proposed amendment to the record.

### **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.*

Operations managers and privileged users can update information on the Veteran's behalf.

Individuals who discover that incorrect information was provided during intake can state that the documentation they are now providing supersedes that 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.** (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.*

**Privacy Risk:** Veterans whose records contain incorrect information may not receive notification of any changes. Furthermore, incorrect information in a Veteran's record may result in improper identification.

**Mitigation:** No personal data is collected directly from individuals. Information in documents loaded to Salesforce - VA Integrated Enterprise Workflow Solution Case and Correspondence Management (VIEWS CCM) may contain PII gathered by users from other systems. PIAs of other systems are available to be referenced as needed. The PIA of the system from which the document creator originally captured the data would cover the information access procedures.

## **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 accessible information and applications. A user of the SFGCP with appropriate permissions must sponsor other users to receive VIEWS CCM access. The sponsor will describe which applications the user needs to access, the user's role, and any applicable security caveats.

#### *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?*

All VA administrations and program and staff offices use VIEWS CCM. System users may also log in remotely. VIEWS CCM is operated at VA Central Office (VACO) in several Washington, DC locations. User controls built into the system manage PII identically at all locations. No regions, hospitals, medical centers, or any other agency use the system.

#### *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.*

User roles are governed by permission sets that allow field-level control of the information and data. Detailed user access policies and descriptions address prohibiting unauthorized disclosure and requirements for data breach notification, for payment of liquid damages in the event of a data breach, for security/privacy training, and for signing the VA Rules of Behavior. The application has basically four levels of users in the system, standard users, VLC users who are privileged users with a little bit extra permission, exec users and super users. There are four different roles standard user,

VLC, user, exec, user and superuser in the view CCM and those users have different levels of permissions which grant them different levels of record access and or different levels of field visibility.

**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.*

User roles identify accessible information and applications. A user of the SFDP with appropriate permissions must sponsor other users to receive VIEWS CCM access. The sponsor will describe which applications the user needs to access, the user's role, and any applicable security caveats.

These roles are governed by permission sets that allow field-level control of the information and data. Detailed user access policies and descriptions address prohibiting unauthorized disclosure and requirements for data breach notification, for payment of liquid damages in the event of a data breach, for security/privacy training, and for signing the VA Rules of Behavior.

A Business Associate Agreement (BAA) has been developed and signed by all contractors, which is a standard protocol for all contractors working on VA information systems.

**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 includes security best practices, threat recognition, privacy, Health Insurance Portability and Accountability Act (HIPAA) 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 Talent Management System (TMS) prior to the user being provisioned.

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

Yes

8.4a If Yes, provide:

1. The Security Plan Status: Completed.
2. The System Security Plan Status Date: 11/29/23
3. The Authorization Status: Yes, Authorized to Operate
4. The Authorization Date: 08/07/2023
5. The Authorization Termination Date: 06/05/2024
6. The Risk Review Completion Date: 08/07/23
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.

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

An ATO has been obtained, to expire 06/05/2024.

## 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)**

VIEWS CCM runs in the Salesforce Government Cloud Plus (SFGCP). Salesforce has been FedRAMP-certified for Software as a Service (SaaS) since 2014. All SFGCP customers are on the same version, patch set, and code base, minimizing security risk and lowering complexity. More than 40 other Federal agencies have issued an Authority To Operate (ATO) for solutions deployed on the Salesforce Government Cloud. In addition, security levels and permissions have been implemented to ensure workflow owners have access to the information they need while protecting sensitive data, such as PII and Protected Health Information (PHI).

### 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 VA Salesforce contract establishes VA ownership rights of all data. The contract stipulates that the contractor shall not retain any copies of data, in full or in part, at the completion of the

performance period. The data shall contain no proprietary elements that would preclude the VA from migrating the data to a different hosting environment or from using a different case management system in the future.

The Salesforce contract addresses the National Institute of Standards (NIST) 800-144 principle that states, “Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf.”

### **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.*

VIEWS CCM system objects contain information that could be used to identify VA employees and VIEWS CCM users, such as email addresses, names, and phone numbers. This information also includes case emails, case queue ownership, case notes, case team names, associated contacts, contact roles, and functional queue members. The CSP does not collect any ancillary data about VIEWS CCM users, which is stored encrypted in the Salesforce databases.

### **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.*

VA has contracted Salesforce to deliver services that include maintaining VA data. A contract in place clearly articulates Salesforce’s roles and responsibilities. Authorized personnel access user-level data to provision and provide the Salesforce service. Access is controlled by authentication and is restricted to authorized individuals. Salesforce’s policies address the required security controls that must be followed to protect PII. Salesforce Development Platform Assessing will be connected to Equinix (the VA’s Trusted Internet Connection, otherwise known as TIC) for data transfer purposes.

Equinix will provide details of the security event, the potential risk to VA-owned sensitive information, and the actions that have been or are being taken to remediate the issue. Activities that will be reported include event type; date and time of event; user identification; workstation identification; success or failure of access attempts; and security actions taken by system administrators or security officers.

Equinix will also provide VA with a written closing action report once the security event or incident has been resolved. VA will follow this same notification process should a security event occur within the VA boundary involving Equinix's provided data. Designated POCs will follow established incident response and reporting procedures, determine whether the incident warrants escalation and comply with established escalation requirements for responding to security incidents.

**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).*

Salesforce - VA Integrated Enterprise Workflow Solution Case and Correspondence Management (VIEWS CCM) does not utilize Robotics Process Automation (RPA).

## Section 10. References

### Summary of Privacy Controls by Family

*Summary of Privacy Controls by Family*

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

---

**Information Systems Security Officer, James Boring**

---

**Information Systems Owner, Michael Domanski**

## **APPENDIX A-6.1**

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy; a Privacy Act notice on forms; screen shot of a website collection privacy notice).

## **HELPFUL LINKS:**

### **General Records Schedule**

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

### **National Archives (Federal Records Management):**

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

### **VA Publications:**

<https://www.va.gov/vapubs/>

### **VA Privacy Service Privacy Hub:**

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

### **Notice of Privacy Practice (NOPP):**

[VHA Notice of Privacy Practices](#)

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