Privacy Impact Assessment for the VA IT System called:

Community Care (CommCare) Customer Relationship Management (CRM)

Veteran Health Administration

Office of Integrated Veteran Care (IVC)

eMASS ID #2362

Date PIA submitted for review:

6/27/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Eller Pamintuan	Eller.Pamintuan@va.gov	303-331-7512
Information System Security Officer (ISSO)	Albert Estacio	Albert.Estacio@va.gov	(909) 583-6309
Information System Owner	Bill Walsh	Bill.Walsh2@va.gov	727-318-2330

Abstract

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

Community Care (CommCare) Customer Relationship Management (CRM) is a project under the Veterans Experience Services (VES) portfolio established to provide users with more efficient ways of managing call center volume and business processes, while enhancing the customer experience. Customer Service Representatives (CSRs) access the web-based Microsoft Dynamics Customer Relationship Management (CRM) application to record information regarding inquiries received concerning Non-VA Medical Care.

Veteran Exposure Team-Health Outcomes Military Exposures (VET-HOME) is a project under the Veterans Relationship Management (VRM) Customer Relationship Management (CRM) umbrella. Vet-

Home consists of a centralized intake center to serve as the national hub for information and services on military environment exposures and a network of 40 clinicians specially trained in military environmental exposures to perform telehealth registry exams and other military environmental exposure assessments and consultations. The intake center welcomes inquiries from Veterans, clinicians, VSOs, and other parties with questions or concerns about military environmental exposures.

The VET-HOME application is a component of CommCare-CRM.

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?

Community Care (CommCare) Customer Relationship Management (CRM)
Office of Integrated Veteran Care (IVC)

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

The Office of Integrated Veteran Care Call Centers (which uses the CommCare-CRM application) receives calls from Veterans, Beneficiaries (i.e., Family Members), and Midical Providers regarding traditional Community Care and Choice Program claims, benefits eligibility, and billing inquiries. Community Care provides users with more efficient ways of managing call center volume and business processes, while enhancing the customer experience. CommCare-CRM is a Work Item system for the IVC. Its userbase includes the IVC Front Office as well as its Directorates. This includes staff at the VA Medical Centers, Community Care Contact Centers, and the rest of the Community Care organizations. This system allows for the work origination staff to create work items for tracking the effort needed to resolve the inquiries from partners.

Client Relations & Action Manager (CRAM) provides a single web-based platform that eases day-to-day management of IVC program office, Veteran, and Beneficiary inquiries. CRAM provides one location to manage IVC Action Taskers and allows cross-system coordination between directorate action teams, improving efficiencies and customer service.

VET-HOME is a new national Veteran Health Administration (VHA) program composed of two parts: 1. A centralized intake centers in eastern CO to serve as the national hub for information and services on military environmental exposures. The intake center welcomes inquiries from Veterans, clinicians, VSOs, and other parties with questions or concerns about military environmental exposures. 2. A geographically distributed network of 40 clinicians specially trained in military environmental exposures to perform telehealth registry exams and other military environment exposure assessments and consultations. Veterans needing in-person examination and additional diagnostic studies (including labs, imaging, breathing tests, and specialty consultations) will be offered these services at the VA facility closest to their location

VET-HOME will collaborate with Veterans' primary care providers and appropriate specialties to promote the timely diagnosis and optimal treatment of any health conditions related to military environmental exposures.

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

The CommCare-CRM application is VA owned and 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?

Currently, CommCare-CRM receives an average of 25,000 per day of inbound calls, and CSRs maintain an average of 500,000 interactions each month. CommCare-CRM uses metrics to represent usage of the CommCare-CRM application. Each incoming call documented in CommCare-CRM and may be regarding multiple Veterans. Request regarding Adverse Credit Reporting (ACR) issues are resolved by filed office staff nationwide. System training and access controls are consistent across all sites

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

CommCare-CRM collects and stores caller information needed to resolve caller request; including first and last name, address, phone number, Social Security (SSN), Date of Birth (DOB), Electronic Data Interchange Personal Identifier (EDIPI), claim numbers, dates of service, and claim amounts. The application utilizes web services from the Master Person Index (MPI), formerly Master Veteran Index (MVI) provides information required to identify proofing and Veteran Integration Control Number (ICN) for subsequent web service requests. MPI information required for identity proofing and Veteran ICN for subsequent web service requests to confirm Veteran identity and obtain corresponding identifiers for other systems, Health Data Repository (HDR) to access Veteran health information from all VistA Veterans Integrated Service Network (VISN) sites, Eligibility and Enrollment (E&E) to access Veteran demographic information, and Claims Processing and Eligibility (CP&E) to access medical billing information, financial information, and employee information. Information is retrieved and displayed through the CommCare-CRM application. The CommCare-CRM application is not a system of record about Veterans, Beneficiaries, or Medical Providers. CommCare-CRM only records contact made by the Veteran, Beneficiary, or their representatives to the Call Center. Because of the nature of Medical Provider inquiries (i.e., calls) each Caller Interaction records may contain information of multiple Veterans. CommCare-CRM uses a combination of Dynamics 365 Customer Engagement, and User Interface (UI) hosting and web service utilization of existing VA systems, CommCare-CRM applications functionality provides consolidated interface and means answering, tracking, and reporting calls from Veterans, beneficiaries, and applicable veteran stakeholders. Microsoft Dynamics 365 CommCare-CRM is the underlying Commercial off the Shelf (COTS) application providing the ability to configure the CommCare-CRM agent desktop clint application and enabling agent to log calls and issues in a single repository that can be search and reported from.

VET-HOME collects and stores caller information needed to resolve caller requests, including first and last name, residence address, correspondence address, home phone number, mobile phone number, work phone number, fax number, email address, and marital status. This data is sourced from Enrollment System Redesign (ESR)

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

The CommCare-CRM application is hosted on the Microsoft Azure Government Cloud (MAG). It is a Software-as-a-Service (SaasS) application that operates as hybrid-cloud deployment model per NIST SP800-145 definition. System is under the Veteran Experience Integration Solution (VEIS) Authority to Operate (ATO). ATO system ID is 2314. A written ISA/MOU is not provided due to this being on a FEDRAMP cloud. FEDRAMP reference: Microsoft – Azure Government Assessing – ATO expires February 26, 2023.

- The Azure for Government HIGH Information as a Service (IaaS) cloud service platform is covered under the Federal Risk and Authorization Management Program (FedRAMP) P-ATO and the VA associated Cloud Service Provider (CSP) ATO documentation.
- The Azure Government General Support Global Operations Services are covered under the Microsoft – Azure for Government JAB FedRAMP ATO package ID F1209051525 and the VA associated ATO.
- The Microsoft Azure Government (includes Dynamics 365) SaaS Platform services are covered under the FedRAMP ATO for Microsoft Azure Government (includes Dynamics 365) JAB FedRAMP ATO package ID F1603087869 and the associated VA CSP-ATO.
- The VA General Support Systems are covered under the VA Regions 1-6 General Support System (GSS) ATO. The VA underlying applications are covered under their respective system owner's ATO documentation.

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?

The CommCare application is hosted on the Microsoft – Dynamics CRM (Dynamics 365) Online (CRMOL) for Government Cloud. The latest release of Microsoft Customer Relationship Management (CRM) is Microsoft Dynamics 365 (D365); references to CRM and D365 are synonyms with the Microsoft platform on which CommCare is built. It is a Software-as-a-Service (SaaS) offering as defined in National Institute of Standards and Technology (NIST) SP800-145. Both the primary and backup data centers are owned by Microsoft, who is the VA contracted Cloud Service Provider (CSP) at those sites with direct connections to the VA Trusted Internet Connections (TIC) from each respective location. Personally Identifiable Information (PII) is maintained consistently, and the same controls are used across all sites utilizing the CommCare application.

Application location information is as follows:

Application	Component Name	Location at Which Component is Run	Type
CommCare-CRM	Main Facility	For security reasons, Microsoft does not provide a Physical address for its data centers. However, redundant Microsoft Government cloud	Production Host: Application and Data Store

		regions exist in both Boydton, Virginia and Des Moines, Iowa	
CommCare-CRM	Default Failover Facility	For security reasons, Microsoft does not provide a Physical address for its data centers. However, redundant Microsoft Government cloud regions exist in both Boydton, Virginia and Des Moines, Iowa	Production Host: Application and Data Store

3. Legal Authority and SORN

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

The CommCare-CRM application has legal authority to operate under:

SORN: 23VA10NB3, *Non-VA Care (Fee) Records* - VA (7-30-2015), https://www.govinfo.gov/content/pkg/FR-2015-07-30/pdf/2015-18646.pdf

Legal Authority: Title 5 U.S.C 301, Title 26 U.S.C 61. Title 38, U.S.C. sections 31, 109, 111, 501, 1151 1703, 1705, 1710, 1712, 1717, 1720, 1721, 1724, 1725, 1727, 1728, 1741–1743, 1781, 1786, 1787, 3102, 5701 (b)(6)(g)(2)(g)(4)(c)(1), 5724, 7105, 7332, and 8131–8137. 38 Code of Federal Regulations 2.6 and 45 CFR part 160 and 164. Title 44 U.S.C and Title 45 U.S.C. Veterans Access, Choice, and Accountability Act of 2014.

SORN: 54VA10NB3, *Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files* - VA (3-3-2015), https://www.govinfo.gov/content/pkg/FR-2015-03-03/pdf/2015-04312.pdf

Legal Authority: Title 38, United States Code, sections 501(a), 501(b), 1703, 1720G, 1724, 1725, 1728, 1781, 1787, 1802, 1803, 1812, 1813, 1821, Public Law 103–446 section 107 and Public Law 111–163 section 101.

SORN: 58VA21/22/28, *Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records* – VA (11/8/2021), https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

Legal Authority: Title 10 U.S.C. chapters 106a, 510, 1606 and 1607 and title 38, U.S.C. §501(a) and Chapters 3, 11, 13, 15, 18, 19, 21, 23, 30, 31, 32, 33, 34, 35, 36, 37, 39, 51, 53, 55 and 77. Title 5 U.S.C. 5514.

SORN: 121VA10, *National Patient Database* - VA (4-12-2023), https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf

Legal Authority: 38 U.S.C. 501.

SORN: 155VA10, *Customer Relationship Management System (CRMS)* - VA (9-15-2023), https://www.govinfo.gov/content/pkg/FR-2023-09-15/pdf/2023-20044.pdf

Legal Authority: 38 U.S.C. 501(1), 1705, 1710, 1722, 1722(a), 1781 and 5 U.S.C 552(a).

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 system of record notices does not require amendment

4. System Changes

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

Completion of the PIA will not require changes in the business process.

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

Completion of the PIA will not require changes to 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:

☒ Name
☒ Social Security Number
☒ Date of Birth
☒ Mother's Maiden Name

☒ Personal Mailing Address
☒ Personal Phone Number(s)
☒ Personal Fax Number
☒ Personal Email Address
☒ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
☒ Financial Information
☒ Health Insurance Beneficiary Numbers Account numbers

☐ Certificate/License numbers[1]
☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☐ Medications
☐ Medical Records
☐ Race/Ethnicity
☒ Tax Identification Number
☐ Medical Record Number
☐ Gender

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

Other PII/PHI data elements:

- Veteran and Beneficiary: claim information, referral information, relationship to veteran or beneficiary, Department of Defense (DoD) Electronic data interchange personal identifier (EDIPI), sensitivity, determination, eligibility status, enrollment status, claim status, corresponding ID
- Members of the Public/Individuals: office address, relationship to 'customer"

PII Mapping of Components (Servers/Database)

CommCare CRM consists of **three** key components (servers/databases/instances/applications/software/application programming interfaces (API). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **CommCare CRM** and the reasons for the collection of the PII are in the table below.

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

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
Azure cloud database	Yes	No	Veteran and Beneficiary:	Caller identification;	Managed by Microsoft as

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

			SSN, name, phone number, claim number, claim information, referral information, email address, mailing address, relationship to veteran or beneficiary, provider taxpayer identification number	Veteran identity verification	a SaaS application. No direct access is given to the Azure server by Microsoft to users or customers.
Connection (TIC) from each respective location	Yes	No	SSN, Name, Date of Birth, Phone Number, Claim Number, Claim Information, Referral Information, Email Address, Mailing Address, Relationship to Veteran or Beneficiary, Provider Taxpayer Identification Number, DoD EDIPI, Fax number	Veteran identity verification	Access to system is limited; access requires PIV; access to system and components is audited.
VET-HOME	Yes	No	SSN, Name, Date of Birth, Phone Number, Claim Number, Claim Information, Referral Information, Email Address, Mailing Address,	Veteran identity verification; Customer service (retrieval of claims, appointments, consults, notes)	Access to system is limited; access requires PIV; access to system and components is audited

			Relationship to Veteran or Beneficiary, Provider Taxpayer Identification Number, DoD EDIPI, Fax number		

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 sources of Information for the CommCare-CRM application are as follows:

- Caller Interaction/confirmation
- MPI
- Integrated VHA System including HDR, E&E and CP&E

The primary source of information in the CommCare-CRM application is direct interaction/confirmation via telephone communication with CSRs. Callers provide at least three (3) identification factors for the Veteran (first name, last name, DoB, SSN) to search MPI. MPI returns basic personal data about a Veteran (name, SSN, address, etc.). Information is passed from MPI to pull data from internal VHA systems. These systems are E&E, HDR, and CP&E. Information is pulled from these sources to ensure CSRs receive all information necessary to assist the caller. Information is verified with the caller during the telephone interaction. CommCare-CRM does not store or modify data from integrated systems, therefore synchronization between the Microsoft Dynamics CRM system and other system integrations is not required.

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 is passed from MPI to pull data from internal VHA systems. These systems are E&E, HDR, and CP&E. Information is pulled from these sources to ensure CSRs receive all information necessary to assist the caller. Information is verified with the caller during the telephone interaction. CommCare-CRM does not store or modify data from integrated systems, therefore synchronization between the Microsoft Dynamics CRM system and other system integrations is not required.

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

The information comes from the Veteran or from systems already storing Veteran information. The Sources of Information for the CommCare-CRM application are as follows:

- Caller interaction/confirmation

- MPI
- Integrated VHA Systems, including HDR, E&E, and CP&E

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 used in the CommCare-CRM application is collected from Veterans, Veteran family members, and Health Care Providers over the phone and entered into the system by a CSR. The CSR may conduct a search against MPI, which returns a Veteran's name, SSN, ICN and other details. Additional Veteran information from HDR, E&E, and CP&E are collected by searching those interfaces using the ICN returned by MPI. The HDR, E&E and CP&E information is not stored by the system. Any request that requires information pulls it via the specified interface when that request is opened and clears the cache of data when the web browser is closed. During the CSR's interaction with the caller, the CSR may discover that additional actions outside of the CSR's purview is required to resolve a caller's inquiry about a claim(s) or eligibility for benefits. As such, the CSR can make an annotation in the CRM Notes field and forward the call record to a supervisor or a colleague in a different VHA department, such as Debt Management, for follow-up. Although the Notes field is not intended to document PII, the CommCare-CRM application does not preclude PII from being stored because it is a free form text field.

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

No, information is not collected on a form and it is not subject to the Paperwork Reduction Act. Information used in the CommCare-CRM application is collected from Veterans, Veteran family members, and Health Care Providers over the phone and entered into the system by a CSR.

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

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

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

The Veteran's Name, DOB, and SSN are collected within the Veteran's record in CommCare-CRM. The purpose of the information is to:

- Conduct an MPI search for identity proofing in MPI;
- Look up information regarding the Veteran in various other systems, particularly claim amounts and statuses.

E&E, HDR, and CP&E data are not stored in CommCare-CRM. This information is used while interacting with a caller to assist with various call flows. The CommCare-CRM system is used to display information for completing tasks such as answering a caller's question, recording an interaction, and adding notes.

Email Address and Phone Number are also stored on the Interaction and Request. This information is used to contact the caller if the call is disconnected or there is additional follow up required. CSRs use free text fields to document notes while interacting with a caller. This free text field is used to document the following:

- Specifics regarding the assistance provided to the Veteran/caller
- Specifics regarding the steps another user needs to take to complete the Veteran/caller's request.

The above information is collected and used to fulfil the Call Center CSRs mission to provide resolution to Veteran and Provider Community Care issues. CommCare-CRM, including all lines of business (LOB) and components, do not collect, use, disseminate, or maintain publicly available or commercial data.

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?

Veteran identity is checked for accuracy through MPI. Verification requires at least three (3) identifiers to conduct a successful MPI search. This ensures that the correct Veteran is associated to a Request. The CommCare CRM CSR verifies with the Veteran or Beneficiary whether their information is correct. MPI is the authoritative source to validate a Veteran. CommCare-CRM does system check for accuracy by accessing internal systems, e.g., MPI, HDR, and CP&E to validate the Veteran's Name, DOB, and SSN are collected within the Veteran's record in CommCare-CRM. The purpose of the information is to:

- Conduct an MPI search for identity proofing in MPI;
- Look up information regarding the Veteran in various other systems, particularly claim amounts and statuses, HDR, and CP&E data are not stored in CommCare-CRM. This information is used while interacting with a caller to assist with various call flows. The CommCare-CRM system is used to display information for completing tasks such as answering a caller's question, recording an interaction, and adding notes. Email Address and Phone Number are also stored on the Interaction and Request. This information is used to contact the caller if the call is disconnected or there is additional follow up required. CSRs use free text fields to document notes while interacting with a caller. This free text field is used to document the following:
    - Specifics regarding the assistance provided to the Veteran/caller
    - Specifics regarding the steps another user needs to take to complete the Veteran/caller's request.

The above information is collected and used to fulfil the Call Center CSRs mission to provide resolution to Veteran and Provider Community Care issues. CommCare-CRM does not collect, use, disseminate, or maintain publicly available or commercial data.

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 CommCare-CRM application complies with the following federal regulations and/or departmental policies and guidelines, as follows:

- Authority for maintenance of the system: Title 38, United States Code, Chapter 73, section 7301(b).
- Title 38, United States Code, Section 501-Veterans' Benefits.
- VHA Directive 1906- Data Quality Requirements for Healthcare Identity Management and the Master Veterans Index Functions.
- VHA Directive 2009-021 Data Entry Requirements for Administrative Data.
- VHA Directive 2006-036 Data Quality Requirements for Identity Management and the Master Patient Index Functions.
- VHA Directive 2007-037 Identity Authentication for Health Care Services.
- OMB Circular A-130, Management of Federal Information Resources, Appendix III, November 2000.
- VA Directive 6300, Records and Information Management.
- VA Handbook 6500, VA6500 AC-8: System Use Notification.
- The Privacy Act of 1974.

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: Caller (i.e., Veteran, Beneficiary, or Provider) may provide incorrect identity information. Data pulled by the CommCare-CRM application contains PII. If the data were accessed by an unauthorized individual or otherwise breached, serious harm or even identity theft might result.

Mitigation: Veteran information is validated through MPI, as the authoritative source, before call proceeds and any information are provided. Additional information gathered and provided is based on MPI-returned identifiers. The CSR does not provide PII from the errant MPI search to the caller as a means of selecting the correct Veteran or Beneficiary. The CommCare-CRM application ensures strict access to information by enforcing thorough access control and requirements for end users. Access to the application is by Personal Identity Verification (PIV) authentication. Individual administrator user IDs and access are provided based on need. The Call Center limits access rights and controls only to valid end users. There are rigorous securities monitoring controls to prevent unauthorized access and intrusion, and to protect all information. Furthermore, all end users are required to take VA Privacy and Information Security Awareness and Rules of Behavior (VA 10176) and Privacy and HIPAA Training (VA 10203) training annually. All users with access to CommCare-CRM are responsible in assuring safeguards for the PII.

Section 2. Uses of the Information

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

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

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

PII/PHI Data Element	Internal Use	External Use
Name	Used to verify Veteran identity	Not used
Social Security Number	Used to verify Veteran identity	Not used
Date of Birth	Used to verify Veteran identity	Not used
Mother's Maiden Name	Used to verify Veteran identity	Not used
Personal Mailing Address	Used to correspond with the Veteran or Caller	Not used
Personal Phone Number(s)	Used to correspond with the Veteran or Caller	Not used
Personal Fax Number	Used to correspond with the Veteran or Caller	Not used
Personal Email Address	Used to correspond with the Veteran or Caller	Not used
Emergency Contact	Used to correspond with the Veteran or Caller	Not used

Financial Information	Used to confirm Eligibility information	Not used
Health Insurance Beneficiary Information	Used to associate Veteran with Beneficiary	Not used
Tax Identification Number (TIN)	Used to verify Veteran identity and as a file number for Veteran	Not used
Integrated Control Number (ICN)	Used to verify Veteran identity and as a file number for Veteran	Not used
Claim Information	Used to confirm claim information	Not used
Referral Information	Used to confirm claim information	Not used
Relationship to Veteran or Beneficiary	Used to confirm beneficiary information	Not used
DoD Electronic Data Interchange Personal Identifier (EDIPI)	Used to verify Veteran identity and as a file number for Veteran	Not used
Sensitivity	Used to confirm claim information	Not used
Determination	Used to confirm claim information	Not used
Eligibility Status	Used to determine Veteran Eligibility for VA care	Not used
Enrollment Status	Used to determine Veteran enrollment in VA programs	Not used
Claim Status	Used to confirm Eligibility information	Not used
Corresponding ID	Used to confirm Eligibility information	Not used
Office Address	Used to confirm Eligibility information	Not used
Relationship to "customer"	Used to confirm information	Not used

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

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

In general, the information stored in CommCare-CRM are various management, tracking, and follow-up reports. Microsoft CommCare-CRM has internal tools to generate graphs and reports of specific data.

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.

CommCare-CRM provides out-of-the-box reporting capabilities which can provide analysis and reports of data housed in the system. The data analysis capabilities of CommCare-CRM Platform allow users to generate configurable reports on an ad-hoc or scheduled basis. These reports consist of a summary data that lists the number of records that meet various criteria, and basic analysis including call resolution totals and percentages. This is the only data analysis tool being used by the CommCare-CRM application this time. There is no reporting on Veterans or Beneficiaries, or their inquiries.

CommCare-CRM does not create or make available any new or previously un-utilized clinical or benefits information about any individual. CommCare-CRM does record interaction details between CSR and customer. These details may include free-form notes and comments about the customer service issue.

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?

Data within the VA network is FIPS 2.0 encrypted.

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

Access to system is limited, requires PIV; and access to system and components are audited in accordance with VA 6500. The information received from the VA systems identified are encrypted during transmission, and all data is encrypted during communication from a call agent's desktop to all VA endpoints.
CommCare - CRM: There is encrypted electronic transmission and at rest using FIPS 2.0 encryption and 256-bit encryption. Access to system is limited, access requires PIV.

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

Contractor and VA employees are required to take Privacy, HIPAA, and information security training annually. HTTPS using SSL encryption is used between internal VA systems. Personnel accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB prior

to gaining access to any VA information system or sensitive information. VEIS uses HTTPS, TLS, Auth tokens and OSP APIM for additional encryption.

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?

Access to PII is limited by the CommCare-CRM (including all CommCare Line of Business (LOBs) and components) application to only those data items deemed necessary for a CSR to perform their job, as determined by their management team and their job description.

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

Access to PII is limited by the CommCare-CRM (including all CommCare LOBs and components) application to only those data items deemed necessary for a CSR to perform their job, as determined by their management team and their job description.

System documentation includes detailed system design and user guides that specify those areas of the system that contain PII and PHI, as well as how it is to be used by the CSR. Additionally, user roles are implemented to restrict user's access to only the specific information required to perform their job function.

2.4c Does access require manager approval?

Roles within the system are determined and requested by Approved Submitters – Call Center supervisors (Senior Program Analyst or higher) or Non-VA Community Care (NVCC) Office management (Supervisors and Business Implementation Managers). User access is provided by CommCare CRM System Administrators following receipt of request from appropriate individuals. The CommCare CRM application implements auditing which tracks user access to the system and all data accessed.

Access requests go through many layers of approvals. D365 Licenses must be approved by the OI&T Product Manager, and Provisioning is performed via the self-service User Management App by select number of users with elevated permissions in leadership roles.

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

Yes, it is the responsibility of the project making the request to ensure compliance with VA regulations and policies regarding configurations, privacy restrictions, network access and authorities or operates. (Including but not limited to: VA 6500, TIC, PIA/PTAs, SORN, and application ATOs).

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

System documentation includes detailed system design and user guides that specify those areas of the system that contain PII and PHI, as well as how it is to be used by all CommCare CRM users. Additionally, user roles are implemented to restrict user's access to only the specific information required to perform their job function. Roles within the system are determined and requested by Call Center supervisors (Senior Program Analyst or higher) or Non-VA Community Care (NVCC) Office management (Supervisors and Business Implementation Managers). User access is provided by CommCare-CRM System Administrators following receipt of request from appropriate individuals. The CommCare-CRM application implements auditing which tracks user access to the system and all data accessed. The information is mapped in the audit record by Call Center agent identifier and Veteran identifier used for data access. VHA and VBA ensure that the practices stated in the PIA are reinforced by requiring Contractors and VA employees to complete all VA trainings including VA Privacy and Information Security Awareness and Rules of Behavior (VA 10176) and Privacy and HIPAA Training (VA 10203). Contractors and VA employees are required to agree to all rules and regulations outlined in trainings, along with any consequences that may arise if failure to comply.

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*

The following data collected and verified from the caller will be stored in the CommCare-CRM application to create a call history of the caller. The data pulled from the source applications is used to verify the information provided by the caller.

- Name: Veteran identification
- Social Security Number: Used to verify Veteran identity and as a file number for Veteran
- Date of Birth: Used to verify Veteran identity
- Mailing Address: Used to correspond with the Veteran or Caller
- Zip Code: Part of the mailing address
- Phone Number(s): Used to correspond with the Veteran or Caller
- Location of caller: Used to associate Veteran with the nearest Facility
- Free Text Notes: Used to collect Case Notes for each Veteran Interaction

- Electronic Data Interchange Personal Identifier (EDIPI)

When a CommCare-CRM session is complete and has ended, data retrieved from E&E, HDR, and CP&E are not saved. Only minimal, critical information is retained by the CommCare-CRM, as the system of record for phone interactions. This information gives management the ability to report on types of calls, first call resolution, and time to solve Veteran issues, as well as accuracy and precision for unattended search scenarios and Veteran sensitivity checks.

Information regarding calls that come into CommCare-CRM is retained for call tracking purposes. Veteran, Beneficiary, or Provider data is also stored to facilitate call tracking.

Other information retained by the CommCare-CRM application, including all LOBs and components, is associated with CommCare-CRM business operations metrics. The CommCare-CRM application retains information including, but not limited to, duration of each call, whether the caller's inquiry was resolved, if the call required escalation to a supervisor and whether the call resulted in a complaint. Only minimal, critical information is retained by the CommCare-CRM application, as the system of record for phone interactions. This information enables CommCare-CRM management the ability to report on types of calls, first call resolution, and time to solve Veteran, Beneficiary, or Provider issues. Moreover, data stored in the CommCare-CRM solution's database are not deleted.

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.*

The stakeholders are responsible in purging the data within the system in accordance with the established records control schedule established in VHA Records Control Schedule 10-1. Data is stored in the Microsoft Azure Government Cloud (MAG).

Dynamics 365 native Backup/restore capabilities (see https://docs.microsoft.com/enus/dynamics365/customer-engagement/admin/backup-restore-instances) and industry best practices. At a minimum, the plan includes the requirement to save data for the backup and recovery of information stored on the cloud storage infrastructure to meet related Service Level Agreements (SLAs), and the retention of records as required by VA Handbook 6300.1 (Records Management Procedures) and VA Directive 6300 (Records and Information Management). CommCare-CRM production data is retained for 14 days before being archived and restored to each application's Production environment per request. Backups are conducted on a daily basis and as needed per the CommCare-CRM application team's request.

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, refer to paragraph 3.2, listing of all RCS utilized by the system with the disposition authority approved by NARA.

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

Records for CommCare-CRM, including all LOBs and components, are retained in accordance with VHA Records Control Schedule (RCS) 10-1 with the following RCS:

- 1001.1. Administrative Records Maintained in Any Agency Office. Temporary; destroy when business use ceases, (3 years for business use). (DAA-GRS-2016-0016-0001)
- 1001.2. Non-recordkeeping Copies of Electronic Records. Temporary; destroy immediately after copying to a recordkeeping system or otherwise preserving, but longer retention is authorized if required for business use, (3 years for business use). (DAA-GRS-2016-0016-0002)
- 1002.1. Internal Administrative Accountability and Operational Management Control Records. Temporary; destroy 1 year after submission or when superseded, as appropriate, but longer retention is authorized if required for business use, (5 years for business use). (DAA-GRS-2017-0008-0001)
- 1004.1. Tracking and Control Records. Temporary; destroy when no longer needed. (DAA-GRS-2013-0002-0016)
- 1004.2. Records Management Program Records. Temporary; destroy no longer than 6 years after the project, activity, or transaction is completed or superseded, but longer retention is authorized if needed for business use. (DAA-GRS-2013-0002-0007)
- 1006.2. Access and Disclosure Request Files. Temporary; destroy 6 years after final action or 3 years after final adjudication by the courts, whichever is later, but longer retention is authorized if required for business use. (DAA-GRS-2016-0002-0001)
- 1006.5. Privacy Act Accounting of Disclosure Files. Temporary; dispose of in accordance with the approved disposition instructions for the related subject individual's records, or 5 years after the disclosure for which the accountability was made, whichever is later. (NC1-64-77-1, item 27)
- 1006.19. Privacy Complaint Files (PSET). Temporary; destroy 3 years after resolution or referral, as appropriate, but longer retention is authorized if required for business use. (DAA-GRS-2019-0001-0004)
- 1100.17. Audit Case Files (OIG). Temporary; cutoff when case is closed. Destroy 8 years after cutoff. (N1-15-99-3, item 1)

- 1170.12. Government Accountability Office (GAO) Audit/Performance Review Files. Temporary; retain until no longer needed for business purposes. Destroy 8 years after issuance or the final GAO report. (DAA-0015-2013-0003-0001)
- 1170.2. Congressional Case Work. Temporary; cutoff when response is sent. Destroy 7 years after cutoff. (DAA-0015-2013-0004-0003)
- 1170.9. Investigative Case Files. Temporary; cutoff at end of FY. Destroy 10 years after cutoff. (DAA-0015-2013-0004-0010)
- 1180.1. Correspondence. Temporary; cutoff file at end of third fiscal year. Destroy 3 years after cutoff if no additional material is received. (N1-15-06-02, item 1)
- 1300.1. Patient Representation Program Records. Temporary; destroy when 7 years old. (N1-15-05-2, item 1)
- 1900.2. Testimony of All Other Officials at the VHA Headquarters Level not Covered in Item 1a above. Temporary; cutoff at end of CY. Destroy 7 years after cutoff. (DAA-0015-2016-0003, item 0002)
- 1925.1. Public Customer Service Operations Records. Temporary; destroy 1 year after resolved, or when no longer needed for business use, whichever is appropriate, (7 years for business use). (DAA-GRS-2017-0002-0001)
- 1925.2. Customer/Client Records. Temporary; delete when superseded, obsolete, or when customer requests the agency to remove the records, (10 years for business use). (DAA-GRS-2017-0002-0002)
- 1930.3. Contract/Finance-Related Call Center Records such as but not limited to: Chief Business Office Purchase Case (CBOPC). Temporary; cutoff at end of FY. Destroy 6 years old, based on financial need of the Call Center. (DAA-2015-2017-0001-0003)
- 1930.4. Veterans Administration and/or Veteran Benefits Call Centers not covered in other schedules. Temporary; cutoff at end of FY. Destroy 2 years old. (DAA-2015-2017-0001-0004)
- 3010.2. Position Descriptions. Temporary; destroy 2 years after position is abolished or description is superseded, but longer retention is authorized if required for business use. (DAA-GRS-2014-0002-0002)
- 4001.1b(3). Financial Transaction Records Related to Procuring Goods and Services, Paying Bills, Collecting Debts, and Accounting, (Bids and Neither Solicited nor Accepted). Temporary; destroy when no longer required for business use, (3 years for business use). (DAA-GRS-2016-0001-0001)
- 4110.1. Budget Formulation, Estimates, Justification, and Submission Records, Fiscal Year 2017 and Forward. Temporary; destroy 6 years after close of fiscal year, but longer retention is authorized if required for business use. (DAA-GRS-2015-0006-0001, item 010)

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.

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 the Department of Veterans' Affairs Handbook 6500.1, Electronic Media Sanitization (November 3, 2008). 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 per VA Handbook 6500.1. Digital media is shredded or sent out for destruction per VA Handbook 6500.1 and NIST SP800-88r1 as evidenced in the FedRAMP Audit reports. Additionally, the system adheres to the retention of records as required by VA Handbook 6300.1 (Records Management Procedures) and VA Directive 6300 (Records and Information Management). CommCare-CRM employees are required to maintain and dispose of records, according to the VHA approved records schedules. Retirement of records requires the use of a VA Form 7468, *Request for Disposition of Records*, which is authorized for paper and local electronic records.

The CommCare-CRM application will follow NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process of any IT storage hardware used in the CommCare-CRM application. The Guidelines establish three levels of data destruction: Clear, Purge, and Destroy, that can be applied to different data storage devices. An appropriate destruction method will be chosen based on the memory type (Flash Memory, Magnetic Drives, Optical Devices, Hard Copies etc.) used for the storage. It is VA policy that all Federal records contained on paper, electronic, or other medium are properly managed from their creation through their final disposition, in accordance with Federal laws.

Regarding temporary paper records, those that contain PII, and VA sensitive information, which are under the jurisdiction of VA, will be handled securely, economically, and effectively and disposed of properly. Written documentation that attests to the completion of the destruction process after the final destruction is required, which could be in the form of a letter, memo, or any format attesting to its complete destruction. This certification is not considered a valid certification of destruction if completed and submitted before the final destruction of the records. The certification should contain sufficient information to attest to the final destruction of the temporary paper records – what temporary records were destroyed, the date when they were destroyed, what destruction method was used, where they were destroyed, and who was responsible for their final destruction.

Paper records are destroyed on site, destruction verification of secure shred containers is verified by the logistics department. The VHA Office of Integrated Veteran Care (IVC) program office has a current shredding contract. No documents leave the facility, and system users are unable to print from a remote location.

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.

PII is not used during testing or training. Test Veterans with artificial data are used to test the application. Test Veterans are provided by MPI, HDR, E&E, and CP&E. End-users utilize the same test Veterans during training. Additionally, all training materials display example data using test Veterans. At this time, CommCare-CRM, including all LOBs and components, data is not used for Research. The project team plans to deidentify all data to minimize the risk to privacy when using PII for research.

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: If data is maintained within the CommCare-CRM application, including all LOBs and components, for a longer time-period than what is needed or required, then the risk that the information will be compromised, breached, or unintentionally released to unauthorized individuals increases.

Mitigation: The CommCare-CRM application only retains information necessary for its purpose of helping Veterans, Beneficiaries, and Medical Providers with their questions regarding non-VA medical care, claims, and claims processing. When a session is complete, the cache is cleared. This production data is retained for 14 days. Information retained by the system gives management the ability to report on types of calls, first call resolution, and time to solve Veteran and Beneficiary issues. Because these data are retained indefinitely, a Backup Plan and Restore Plan is implemented for the cloud hosted environment using industry best practices. At a minimum, the plan includes the requirement to save data for the backup and recovery of information stored on the cloud storage infrastructure to meet related Service Level Agreements (SLAs), and the retention of records. All primary production servers are backed up on a daily incremental and weekly full basis employing

Dynamics 365 native backup/restore capabilities with the data stored in georedundant Microsoft Government data centers.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Master Person Index (MPI)	Veteran identity confirmation and return of system identifiers	Shared: • First Name • Last Name • DOB • SSN • EDIPI • Received: • ICN • Corresponding IDs	HTTPS

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
Health Data Repository (HDR)	Retrieve VistA data required to assist Veteran/caller	Received: • VistA Consults • VistA Appointments • VistA Notes • VistA Postings • VistA Orders	HTTPS
Eligibility and Enrollment (E&E)	Retrieve VistA data required to assist Veteran/caller	Received: • Sensitivity • Determination • Addresses • Contact Information • Eligibility Status • Enrollment Status • Insurance Information	HTTPS
Claims Processing and Eligibility (CP&E)	Retrieve VistA data required to assist Veteran/caller	• Claims status • Payments • Eligibility	HTTPS
Enrollment System Redesign (ESR)	Retrieve VistA data required to assist Veteran/caller	• Name • SSN • DOB • Phone Number(s) • EDIPI • Mailing Address • Zip Code • Email Address	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.

Follow the format below:

Privacy Risk: Disclosure of information from a third party. Privacy information may be inadvertently released to unauthorized individuals or the VistA source applications (i.e., E&E, HDR, MPI, and CP&E) with which the CommCare-CRM application interfaces with may inadvertently release privacy information. If such an instance should occur the impact is considered low.

Mitigation: An Interconnection Security Agreement / Memorandum of Understanding (ISA/MOU) defining the system and data transmission in is in place. Access to the data is limited to appropriate personnel who are required to be trained in the handling of VA PII/PHI and sensitive information. The CommCare-CRM application ensures strict access to information by enforcing through access control and requirements for end users. Access to the application is by PIV authentication. Individual administrator user IDs and access are provided only based on need. CommCare-CRM limits access rights and controls only to valid end users. Rigorous security monitoring controls are in place to prevent unauthorized access and intrusion, and to protect all information. Furthermore, all end users are required to take VA Privacy and Information Security Awareness and Rules of Behavior (VA 10176) and Privacy and HIPAA Training (VA 10203) training annually. The VA IT office is responsible in assuring safeguards for the PII.

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?

CommCare-CRM does not share information externally.

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

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

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

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

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

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

Data Shared with External Organizations

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

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: <<ADD ANSWER HERE>>

Mitigation: <<ADD ANSWER HERE>>

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.

The VA policy is not to disclose any personal information to third parties outside VA without their consent, except to facilitate the transaction, to act on caller's behalf at their request, or as authorized by law. Any questions or concerns regarding VA privacy policy or use of patient information can be made by contacting via email at Contact VA Privacy Service, or by mailing questions or concerns at Department of Veterans Affairs, Privacy Service, 810 Vermont Avenue, N.W. (005R1A) Washington, DC 20420.

VHA Notice of Privacy Practices is located here.

It is Veterans Health Administration (VHA) policy that the VHA Notice of Privacy Practices (Information Bulletin 10-163) is created, maintained, and distributed in compliance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule at 45 C.F.R. § 164.520, to inform Veterans, beneficiaries, caregivers, and non-Veteran patients of the use and disclosure of their health information without authorization, their rights to access and restrictions on certain uses and disclosures and VHA's legal duties to maintain the privacy of their health information. AUTHORITY: 45 C.F.R. parts 160 and 164.

The SORN for CommCare CRM is as follows:

https://www.oprm.va.gov/privacy/systems_of_records.aspx

- 23VA10NB3, Non-VA Care (Fee) Records-VA (7/30/2015); https://www.govinfo.gov/content/pkg/FR-2015-07-30/pdf/2015-18646.pdf
- 54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files-VA (3/3/2015); https://www.govinfo.gov/content/pkg/FR-2015-03- 03/pdf/2015-04312.pdf

- 58VA21/22/28, Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records-VA (11/8/2021); https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf
- 121VA10, National Patient Databases-VA (4/12/2023): https://www.govinfo.gov/content/pkg/FR-2018-02- 12/pdf/2018-02760.pdf
- 155VA10 Customer Relationship Management System (CRMS)-VA (9/15/2023): https://www.govinfo.gov/content/pkg/FR-2023-09-15/pdf/2023-20044.pdf

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

VHA Notice of Privacy Practice
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946.

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.

All callers are informed via the Interactive Voice Recognition (IVR) that each call is being recorded. CSRs are trained to utilize guidelines established by Routine Use 27 (RU27) which describe 27 different routine use categories allowing for the release of information to different agencies or persons for different reasons. All calls are recorded and may be monitored for quality assurance.

CSRs collect information directly from Veterans, Beneficiaries, and Providers. If the caller asks, notice of what information is required is provided at the time of the call. Providers or Beneficiaries must provide at least three (3) identifiers in order for the CSR to conduct an MPI search. This ensures that the correct Beneficiary is associated to a phone call record being created in CommCare-CRM. Personal information from the Veteran or Beneficiary is then populated into the phone call form. The CSR can then verify with the caller whether the information is correct. The CommCare-CRM application logs all interactions that the Veteran, Beneficiary, or Provider has with the Call Center, the reasons for the contact, and how the Call Center supported the caller. PII, including SSN, DOB, and names, can be saved as part of the call log.

VHA Notice of Privacy Practices is located here.

(Full link for reference: https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946).

Applicable SORNs are as follows:

SORN: 23VA10NB3, *Non-VA Care (Fee) Records* - VA (7-30-2015), https://www.govinfo.gov/content/pkg/FR-2015-07-30/pdf/2015-18646.pdf

SORN: 54VA10NB3, *Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files* - VA (3-3-2015), https://www.govinfo.gov/content/pkg/FR-2015-03-03/pdf/2015-04312.pdf

SORN: 58VA21/22/28, *Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records* – VA (11/8/2021), https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24372.pdf

SORN: 121VA10, *National Patient Database* - VA (4-12-2023), https://www.govinfo.gov/content/pkg/FR-2023-04-12/pdf/2023-07638.pdf

SORN: 155VA10, *Customer Relationship Management System (CRMS)* - VA (9-15-2023), https://www.govinfo.gov/content/pkg/FR-2023-09-15/pdf/2023-20044.pdf

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress.

VHA Directive 1605.1, Privacy and Release of Information, paragraph 5, lists the Individuals' Rights of the Veterans and Beneficiaries to request VHA to restrict the use and/or disclosures of individually identifiable health information to carry out treatment, payment, or health care operations. Veterans have the right to refuse to disclose their SSNs to VHA. The individual is denied any right, benefit, or privilege provided by law because of refusal to disclose to VHA an SSN (please refer to the: 38 Code of Federal Regulations CFR 1.575(a)).

If a caller does not wish to provide their SSN, they may provide their EDIPI. Alternatively, they may provide their First Name, Last Name, and Date of Birth. If the caller does not wish to provide any of this information, there is no denial of service; however, the CSR will be unable to:

- Create a request in CommCare-CRM to be routed to another user to work on
- Effectively categorize the call type and details
- Retrieve data from MPI, E&E, HDR, and CP&E.

Inability to perform these actions may restrict or prevent the CSR's ability to assist the caller

6.3 Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

This question is directed at whether an individual may provide consent for specific uses, or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use? This question is related to privacy control IP-1, Consent.

VHA Handbook 1605.1, Privacy and Release Information, paragraph 5 lists the Individual's rights of Veterans and Beneficiaries to request VHA to restrict the uses and/or disclosures of individually identifiable health information to carry out treatment, payment, or health care operations. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the records.

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: If CSRs do not provide notice to callers, then they will not know how the information they provide to the CommCare-CRM is being used. The magnitude of impact is low if Veterans and Beneficiaries are not provided this notice because the CSRs are not collecting new data. The CSRs are merely verifying authoritative data stored in MPI, E&E, HDR, and CP&E. Privacy Information is used or disclosed outside of its intended purpose.

Mitigation: Contractor and VA employees are required to take VA Privacy and Information Security Awareness and Rules of Behavior (VA 10176) and Privacy and HIPAA Training (VA 10203) training annually. In addition, this PIA, which will be available online as required by the eGovernment Act of 2002, Pub. L. 107–347§208(b)(1)(B)(iii), serves to notify Beneficiaries and Providers calling into the Call Center about the collection and storage of personal information. This PIA serves to notify Veterans calling into the Call Center about the collection and storage of personal information. All callers are informed via the Interactive Voice Recognition (IVR) that each call is being recorded.
1. Beneficiaries are provided notice of Privacy Practices upon enrollment. A form of this notice is provided in the CHAMPVA Guide at:
https://www.va.gov/COMMUNITYCARE/docs/pubfiles/programguides/champva_guide.pdf
2. Privacy notices are provided at the point of service at the medical center where the Veteran and Beneficiary receive care in accordance with VHA Handbook 1605.4, Notice of Privacy Practices.
3.Notice of Privacy Practices are available on the VA's website at:
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946
Each of the above notices include information on how to report any miss use of information which is not in accordance with the collection.

The Customer Service Center (CSC), i.e., Call Center, has as part of their call script and procedure in accordance with the Systems of Records Notice

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.***

VHA Directive 1605.01, *Privacy and Release of Information* states the rights of Veterans and Beneficiaries to request access to review their records. VA Form 10-5345a, Individual's Request for a Copy of Their Own Health Information, may be used as the written request requirement. All requests to review or seek copies of records must be received by direct mail, fax, in person, or by mail referral from another agency or VA office. All requests for access to data must be delivered to, and reviewed by, the System Manager for the concerned VHA system of records, the facility Privacy Officer, or their designee. Each request must include the signature of the requester, date of birth, copy of signed government identification, state what is request and the period of the information requested. Mail requests for eligibility information/records to: CHAMPVA Eligibility PO Box 469028 Denver, CO 80246-9028. Mail requests for CHAMPVA billing/claim records to: VHA Office of Integrated Veteran Care Privacy/FOIA Office, PO Box 469060 Denver, CO 80246-9060. Requests for medical and pharmacy records contact your servicing medical provider and for Community Care authorizations/authorization numbers are located at the referring VA Medical Center. For Veteran claim payment information will need to be submitted to the VA Financial Services Center (FSC) Privacy Office by first contacting them via email at vafscprivacyofficer@va.gov for secure submission methods. For Veteran Explanation of Benefits maintained by the VA's Third-Party Administrators may be requested by the Veteran registering and requesting their records from either (TriWest Healthcare Alliance) (https://veteran.triwest.com/bizflowappdev/apps/veteranportal/?tz=GMT-0700 or Optum (https://veteran.vacommunitycare.com/start). Medical and pharmacy records should be sought from the medical facility where the patient received care.and Veteran and Beneficiary (CHAMPVA) lien or subrogation requests should be submitted to the respective action office via the instructions located at https://www.va.gov/OGC/Collections.asp.

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.

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?

VHA Directive 1605.01, *Privacy and Release Information*, paragraph 5 states the rights of Veterans to request access to review their records. VA Form 10-5345a, *Individual's Request for a Copy of Their Own Health Information*, may be used as the written request requirement. All requests to review must be received by direct mail, fax, in person, or by mail referral from another agency or VA office. All requests for access to CommCare-CRM records must be delivered to and reviewed by the System Manager for the concerned VHA system of records, the facility Privacy Officer, or their designee. Each request must be date stamped and reviewed to determine whether the request for access should be granted.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed? If the correction procedures are the same as those given in question 7.1, state as much. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Veterans and beneficiaries have the right to amend their records by submitting their request in writing. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request must be mailed or delivered to the VBA organization that maintains the record. The data from Veterans and Beneficiaries who call the CommCare-CRM Contact Center are used primarily for call tracking and Veteran, Beneficiary, or Provider verification. The authoritative sources for the data are MPI, HDR, E&E, and CP&E. In the event that data stored in the authoritative sources are erroneous, the CommCare-CRM CSR can take a note, but the CommCare-CRM application cannot be used to correct inaccurate or erroneous information stored in MPI, HDR, E&E, or CP&E. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned system of records, and the facility Privacy Officer, or designee, and needs to be date stamped; and filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579.

Individuals have the right to request an amendment (or correction) to information in the CommCare-CRM records if they believe it is incomplete, inaccurate, untimely, or unrelated to operations. The information collected from individuals calling in to CommCare-CRM is used primarily for call tracking, so the information is not typically corrected. Each call is logged individually. If the individual discovers that incorrect information was provided during intake, they simply follow the same contact procedures as before, and state that the documentation they are now providing supersedes those previously provided.

VHA Handbook 1605.1, *Privacy and Release Information*, paragraph 5 lists the rights of Veterans and Beneficiaries to request that the VHA restrict the uses and/or disclosures of individually identifiable health information to carry out treatment, payment, or health care operation.

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.

CommCare-CRM CSRs will notify the callers that they may request changes to their information in accordance with VHA Handbook 1605.1, *Privacy and Release of Information*, paragraph 5 states the rights of Veterans and Beneficiaries to amend their records by submitting VA Form 10-5345a, Individual's Request for a Copy of Their Own Health Information, which may be used as the written request requirement. This includes designated record sets, as provided in 38 CFR 1.579 and 45 CFR 164.526. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the facility Privacy Officer, or designee, to be date stamped; and is filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579.

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

If a Veteran or Beneficiary discovers that incorrect information was provided during the intake process, they must submit an information amendment request. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the facility Privacy Officer, or designee, to be date stamped; and is filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

involved might change their behavior. *(Work with your System ISSO to complete all Privacy Risk questions inside the document this section).*

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

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

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

Follow the format below:

Privacy Risk: There is a risk that incorrect information is accidentally recorded in an individual's record. An individual may want to review the content of their record to check for data accuracy. The magnitude of harm associated with this risk to the VA is low.

Mitigation: Application mitigates the risk by requiring all applicable Contractors and VA employees who engage with CommCare-CRM to complete all of the following data security and privacy VA trainings: VA Privacy and Information Security Awareness and Rules of Behavior Training, and Privacy and HIPAA focused training. Contractors and VA employees are required to agree to all rules and regulations outlined in trainings, along with any consequences that may arise if failure to comply.

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?

The supervisor/Contracting Officer's Representative (COR) documents and monitors individual information system security training activities, including basic security awareness training and specific information system security training. This documentation and monitoring is performed through the use of the Talent Management System (TMS). Access to the system is granted to VA employees and contractors the supporting IT for the application after theh supervisor/COR authorizes this access once requirements have been met. Only the IT system administrators authorized by VA IT will have the security role to modify the CommCare-CRM application. This PIA will not result in technology protocol changes, additional controls, or single sign on, as per privacy control AR-7, Privacy-Enhanced System

Design and Development. All CommCare-CRM users must take the following steps before they are granted access to the system:

- Individuals must take and pass training on VA Privacy and Information Security Awareness and Rules of Behavior (VA 10176) and Privacy and HIPAA Training (VA 10203), and government ethics.
- Individuals must have a completed security investigation.
- After the training and the security investigation are complete, a request is submitted for 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?

There are no CommCare-CRM users from other agencies; only VA employees are granted access.

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.

There are three types of users who use the system on a daily basis: CSRs, Supervisors, and Sr. Supervisor. CSRs can only create files in the system and have limited access to the data. Supervisors have the supervisor security role granted in the CommCare-CRM system for the purpose of creating Call Center reports. Senior Supervisors can create reports regarding Supervisor and CSR business operations performance metrics. Currently, user roles are defined by business leadership.

Developer Access: Developers account management processes should further ensure that only end users are able to access the environment. Developers and CommCare-CRM Project teams will work to create, update, access and disable developer accounts for project teams. Additionally, there shall be a review of user access periodically to evaluate whether users are active in the environment; if the user is not active, their account is terminated. All requests for access must be delivered to and reviewed by the System Manager for the concerned VHA system of records, the facility Privacy Officer, or their designee. Roles within the system are determined and assigned by Call Center management. A designated VA Project Point of Contact (POC) is the only person who may submit account creation requests and submitted for accountability purposes.

End-User and Tester Access: All individuals requesting developer access are required to complete all VA trainings (VA Privacy and Information Security Awareness and Rules of Behavior (VA 10176) and Privacy and HIPAA Training (VA 10203)) and applicable role-based training. This may include but is not limited to Information Security for IT Specialists Training) and must be authorized by VA Project Manager. To ensure that this requirement is met, the designated VA Project POC must submit a signed Access Request Form for an individual or a group. At minimum, the following information should be provided for each VA Project Team member requesting access to the CommCare-CRM application Environments: First Name, Last Name, Primary E-mail, Main Phone, Manager, current on VA Training, VA Employee or Contractor, VA Active Directory Username, Environment,

Access Permissions, and Contract End date, access justification and completed training certifications.

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.

VA contractors have access to the pre-production environments for development purposes. Contractors also have access to the live production system for maintenance activities. The following steps are required before contractors can gain access to the system:

- Contractors must take and pass training on VA Privacy and Information Security Awareness and Rules of Behavior (VA 10176) and Privacy and HIPAA Training (VA 10203), and government ethics and role-based training based on support role to the system.
- Contractors must have signed the Non-Disclosure Agreement (NDA) and Rules of Behavior (RoB).
- Contractors must have successfully completed VA contractor background security investigation as per the Position Designation Automated Tool (PDT).
- Once complete, a request is submitted for access. Before access is granted to the production environment; this request must be approved by the supervisor, and OIT.

VA owns the data that the CommCare-CRM application extracts from the source applications, and Microsoft manages and secures the CommCare-CRM application data. The VA and Microsoft Project Managers, CORs have weekly meetings for the review of the contract details and this contract is reviewed at least on an annual basis. There shall be a regular review of user access to evaluate whether users are active in the environment. If a user is not active, the account will be terminated. A designated VA Project POC is the only person who may submit account creation requests for accountability purposes. Contractor access to the system expires at the end of the contract duration or earlier.

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.

All CommCare CRM personnel who will be accessing information systems must read and acknowledge their receipt and acceptance of the VA Information Security Rules of Behavior (RoB)

prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training that all personnel must complete via the VA's TMS. After the CommCare-CRM user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training. Acceptance obtained through electronic acknowledgement is tracked through the TMS system. All VA employees must complete annual Privacy and Security training. This training includes but is not limited to, the following TMS Courses:

- VA 10176: Privacy and Info Security Awareness and Rules of Behavior
- VA 10203: Privacy and HIPAA Training
- VA 3812493: Annual Government Ethics Role-based Training Includes, but is not limited to and based on the role of the user:
- VA 1016925: Information Assurance for Software Developers IT Software Developers
- VA 3193: Information Security for Chief Information Officers (CIOs) Executives, Senior Managers, CIOs and Chief Financial Officers (CFOs)
- VA 1357084: Information Security Role-Based Training for Data Managers
- VA 64899: Information Security Role-Based Training for IT Project Managers
- VA 3197: Information Security Role-Based Training for IT Specialists
- VA 1357083: Information Security Role-Based Training for Network Administrators
- VA 1357076: Information Security Role-Based Training for System Administrators
- VA 3867207: Information Security Role-Based Training for System Owners

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* June 14, 2024
3. *The Authorization Status:* Approved, Assess Only
4. *The Authorization Date:* July 11, 2024
5. *The Authorization Termination Date:* July 27, 2027
6. *The Risk Review Completion Date:* July 11, 2024
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Low/Low/Low

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.***

The Assess Only Authorization have been completed for the system.

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)*

CommCare CRM is a Dynamics 365 SaaS that leverages the PaaS interface platform to interface with VA Services in the 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.*

All Dynamics 365 CRM applications are hosted in Microsoft Azure Government (MAG) including CommCare – CRM, which is under Dynamics 365 VA Enterprise Contract. Government (includes Dynamics 365) JABFedRAMP ATO package ID F1603087869 and the associated VA CSP- ATO.

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 VA Azure Government General Support Global Operations Services 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.

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 Azure Government General Support Global Operations Services 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".

9.5 If the system is utilizing Robotics Process Automation (RPA), please describe the role of the bots.

Robotic Process Automation is the use of software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. For example, will the automation move or touch PII/PHI information. RPA may also be referred to as "Bots" or Artificial Intelligence (AI).

The use RPAs or "bots" are not implemented within the CommCare CRM application.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

Signature of Responsible Officials

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

ELLER PAMINTUAN

Digitally signed by ELLER PAMINTUAN
Date: 2024.07.18 12:22:01 -06'00'

Privacy Officer, Eller Pamintuan

ALBERTINO ESTACIO

Digitally signed by ALBERTINO ESTACIO
Date: 2024.07.24 13:37:03 -07'00'

Information Systems Security Officer, Albert Estacio

WILLIAM WALSH

Digitally signed by WILLIAM WALSH
Date: 2024.07.25 07:41:32 -04'00'

Information Systems Owner, Bill Walsh

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).

VHA Notice of Privacy Practices is located here.

(Full link for reference: https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946).

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