Privacy Impact Assessment for the VA IT System called:

Caribou CLC Suite (cloud) Assessing

Veterans' Health Administration (VHA)

12GEC Geriatrics and Extended Care (GEC)

Date PIA submitted for review:

August 17th, 2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Dennis Lahl	Dennis.lahl@va.gov	202-461-7330
Information System Security Officer (ISSO)	Neil Cruz	Neil.Cruz@va.gov	202-632-1432
Information System Owner	Tony Sines	Tony.sines@va.gov	316-249-8510

Abstract

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

Caribou CLC Suite, is utilized to assess residents of long-term care facilities that guide the development of individualized care plans, evaluate the quality of care provided and determine workload and Veterans Equitable Resource Allocation (VERA) reimbursements. This commercial off-the-shelf (COTS) software, produced by Document Storage Systems, Inc (DSS), interfaces with VistA and Millennium to support the collection of Minimum Data Set (MDS) Data to determine workload, identify quality measures as well as capture resident preferences for care.

Caribou CLC Suite provides a comprehensive and standardized assessment of each resident's functional capabilities and helps staff to identify health problems with real-time access to resident medical information. Information is captured, updated, and shared with providers in a timely and effective manner to ensure universal access to quality data as well as extend essential health care information to key clinical decision makers. Caribou CLC Suite is needed to ensure that VHA Handbook 1142.03 and the Joint Commission (TJC) standards are met for long-term care facilities. This software is needed to complete comprehensive, electronic health care plans and assessments utilized for all residents in Community Living Centers (CLCs). It also provides the capability to populate the Caribou CLC Suite tool with VistA and Millennium admission, discharge, and transfer (ADT) data as well as providing reporting functionality at the local, Veterans Integrated Service Network(s) (VISN) and national levels of MDS data.

Caribou CLC Suite ensures that VA remains in compliance with Centers for Medicare & Medicaid Services (CMS) requirements, provide accurate Resource Utilization Group (RUG) scores, assist with the calculations of Veterans Equitable Resource Allocations (VERA), document Quality Measures (QM) for long term care surveys, and improve ability to assess CLC residents' quality of life elements. This commercial off-the-shelf (COTS) software, produced by Document Storage Systems, Inc (DSS), interfaces with VistA and Millennium to support the collection of Minimum Data Set (MDS) Data to determine workload, identify quality measures as well as capture resident preferences for care.

Overview

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

1 General Description

A. The IT system name and the name of the program office that owns the IT system.

Caribou CLC Suite, 12GEC Geriatrics and Extended Care (GEC)

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

Caribou CLC Suite provides a comprehensive and standardized assessment of each resident's functional capabilities and helps staff to identify health problems with real-time access to resident medical information. Information is captured, updated, and shared with providers in a timely and effective manner to ensure universal access to quality data as well as extend essential health care information to key clinical decision makers. Caribou CLC Suite is needed to ensure that VHA Handbook 1142.03 and the Joint Commission (TJC) standards are met for long-term care facilities. This software is needed to complete comprehensive, electronic health care plans and assessments utilized for all residents in Community Living Centers (CLCs). It also provides the capability to populate the Caribou CLC Suite tool with VistA and Millennium admission, discharge, and transfer (ADT) data as well as providing reporting functionality at the local, Veterans Integrated Service Network(s) (VISN) and national levels of MDS data.

C. Indicate the ownership or control of the IT system or project.

VHA Geriatrics and Extended Care (GEC) (12GEC) VHA Geriatrics and Extended Care (GEC) (12GEC) owned. Operated by DSS on behalf of VA.

2. Information Collection and Sharing

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

The total number of patient records in Caribou as of 06/13/2023 is 172,287. These patients are all veterans receiving care in or at a VA community living center facility. The total number of patient records in Caribou as of 06/13/2023 is 172,287. These patients are all veterans receiving care in or at a VA community living center facility.

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

The information collected is for the creation of the standardized minimum data set (MDS) assessments and treatment planning process designed to identify the functional and health care needs of the resident and to help develop a plan of care where services are individualized to meet the needs of each resident. The Resident Assessment Instrument (RAI)/ MDS generates Quality Measures (QM), and Resource Utilization Groups (RUGs). The QMs are used for monitoring VA CLC quality at the facility, Veterans Integrated Services Network (VISN), and national levels. The RUGs reflect a Veteran's assessed needs for care and the resources required to provide such care. RUGs are used in the nurse staffing methodology to determine the amount and type of nursing staff necessary to provide the appropriate level of care. The RUGs and Bed Days of Care (BDOC) are the basis for Veterans Equitable Resource Allocation (VERA) classification in VA CLCs. Caribou CLC Suite collects a wide range of patient data including the name, date of birth, gender, ethnicity, marital status, SSN, occupation, Medicare/Medicaid Number, ICD-10 codes, admit reason, religion, admission date, patients ward, room bed number, treating specialty and death date. SORN – 79VA10 – https://www.oprm.va.gov/privacy/systems_of_records.aspx The legal authority to collect SSN was created by the Health Care Finance Administration (HCFA) now known as CMS (Centers for Medicare & Medicaid Services). Omnibus Budget Reconciliation Act (OBRA) of 1987 Public Law (Pub. L.) No. 100-203, title IV, subtitle C, 101 Stat 1330 (1987) (OBRA '87) required the Centers for Medicare & Medicaid Services (CMS) to designate an RAI for nursing home patients that includes an MDS. AUTHORITY: Public Law 100-203, title IV, subtitle C and title 38 United States Code 7301.

VHA Directive 2012-035, VHA Social Security Number Reduction are individualized to meet the needs of each resident.

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

Caribou exchanges information with VA's VistA EHR and with Oracle Millennium EHR via APIs and allows for syncing of patient records between the system to track resident care.

G. Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.

The physical location that will store this information is the Microsoft Azure Government Cloud in Central Texas, with fail over to Virginia.

3. Legal Authority and SORN

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

Caribou CLC Suite collects a wide range of patient data including the name, date of birth, gender, ethnicity, marital status, SSN, occupation, Medicare/Medicaid Number, ICD-10 codes, admit reason, religion, admission date, patients ward, room bed number, treating specialty and death date.

SORN – 79VA10 – https://www.oprm.va.gov/privacy/systems_of_records.aspx

The legal authority to collect SSN was created by the Health Care Finance Administration (HCFA) now known as CMS (Centers for Medicare & Medicaid Services). Omnibus Budget Reconciliation Act (OBRA) of 1987 Public Law (Pub. L.) No. 100-203, title IV, subtitle C, 101 Stat 1330 (1987) (OBRA '87) required the Centers for Medicare & Medicaid Services (CMS) to designate an RAI for nursing home patients that includes an MDS.

AUTHORITY: Public Law 100-203, title IV, subtitle C and Title 38 United States Code 7301(a).

VHA Directive 2012-035, VHA Social Security Number Reduction rating specialty and death date.

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?

No revision needed.

D. System Changes

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

No changes needed.

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

The system is being updated to a newer Operating System (OS) and database system as part of this change.

Section 1. Characterization of the Information

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

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

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

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

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

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

- ☒ Name
- ☒ Social Security Number
- ☒ Date of Birth
- ☐ Mother's Maiden Name
- ☐ Personal Mailing Address
- ☐ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☐ Personal Email Address
- ☒ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☐ Financial Information
- ☒ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers*
- ☐ 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)

Marital Status
Date of Death
Period of service
Primary eligibility code
Admission Date & Time, Admission Type, Admitting Diagnosis, Attending Physician, Primary Care Physician, Room Bed,
Occupation,

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

PII Mapping of Components (Servers/Database)

Caribou consists of two components (servers & database). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Caribou and the reasons for the collection of the PII are in the table below.

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

Internal Database Connections

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
Caribou Database	**yes**	**yes**	**Name Social Security Number Date of Birth Gender Integrated Control Number (ICN) Military History/Service Connection Emergency Contact Health Insurance Numbers**	**Required for medical records**	**Encryption, network segmentation, role-based access**

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?

Information is entered by clinicians and aides in the CLC for the patients they are responsible for. Data is also received from VistA and Oracle / Cerner EHR.

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

The individuals are residents in VA care facilities and are receiving care from VA staff. That care is documented and tracked by VA staff and shared with the EHRs as part of the patients record.

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

Caribou is used by CLC staff to record information on the residents that are in their facility. The information is an addendum to the resident's electronic health record in VistA.

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?

Direct interaction with the patients, directly from clinicians, and electronic transmission from the EHRs.

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

The information is not captured on a form and is not subject to the Paperwork Reduction Act.

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

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

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

The information is manually verified by the clinician that is entering it into the system. Information received from the EHRs is checked before it is shared with Caribou. The data fields also have parameters that limit what can be entered in each field.

1.4b If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

The system does not access an aggregator of information.

1.5 What specific legal authorities, arrangements, and agreements defined the collection of information?

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders. This question is related to privacy control AP-1, Authority to Collect

The legal authority to collect SSN was created by the Health Care Finance Administration (HCFA) now known as CMS (Centers for Medicare & Medicaid Services). Omnibus Budget Reconciliation Act (OBRA) of 1987 Public Law (Pub. L.) No. 100-203, title IV, subtitle C, 101 Stat 1330 (1987) (OBRA ‘87) required the Centers for Medicare & Medicaid Services (CMS) to designate an RAI for nursing home patients that includes an MDS.

AUTHORITY: Public Law 100-203, title IV, subtitle C and title 38 United States Code 7301.

VHA Directive 2012-035, VHA Social Security Number Reduction. le C, 101 Stat 1330 (1987) (OBRA ‘87) required the Centers for Medicare & Medicaid Services (CMS) to designate an RAI for nursing home patients that includes an MDS.

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

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks. (*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: The data in the Caribou system includes PHI and PII on CLC residents used for assessment and treatment purposes and shares that data with the two current EHR systems so there is sensitive data throughout the system.

Mitigation: In order to ensure that the data in the system is heavily protected, the DSS team uses defense in depth to layer on protections. Hardware encryption, firewalls, encryption in transit using TLS 1.2 or higher, and role-based access are used to keep the data safe and secure.

Section 2. Uses of the Information

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

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

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

Name – Patient name
Social Security Number – to identify the individual patient
Date of Birth – used for patient matching
Gender - used for patient matching

Integrated Control Number (ICN) - used for patient matching
Military History/Service Connection - used for patient matching
Emergency Contact – used to contact residents family in case of problems
Health Insurance Numbers – to determine if other funding is available to cover the resident's care

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.

No additional tools are used

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.

Data that is entered into the Caribou system is written back to the patients record in VistA. Data is also exchanged programmatically with the new Oracle EHR via APIs and listeners and is saved to the patients record in that EHR.

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?

Caribou utilizes data at rest encryption (hardware level encryption) and in transit (TLS 1.2 or higher cert based encrypted traffic), network segmentation, and role-based access controls to protect the data.

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

SSNs are obfuscated on displays and only accessible by special admin privileges.

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

In order to ensure that the data in the system is heavily protected, the DSS team uses defense in depth to layer on protections. Hardware encryption, firewalls, encryption in transit using TLS 1.2 or higher, and role-based access are used to keep the data safe and secure.

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?

In order to get an account in Caribou, users must have a VistA account and a PIV badge. Then facility administrators designate those users within the Caribou application before they can access any information. This creates 3 layers of verification of users' roles and need for access to protect the data roles and need for access to protect the data.

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

Yes. Caribou SOPs define the process within the system. There are published SOPs on verifying your identity to get a PIV and on getting an account in VistA with role assignment.

2.4c Does access require manager approval?

Yes. Manager's approval is required at all steps taken to get an account.

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

Yes. Caribou has a robust auditing system with logs being saved and monitored for unauthorized actions.

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

The system ISO, ISSO, and steward(s) in conjunction with the DSS Caribou team work together to protect the system.

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 data elements that Caribou retains are: First Name, Last Name, Middle Name, Sex, SSN, Race, Marital Status, Date Of Birth, Date Of Death, Period Of Service, Primary Eligibility Code, Status, Admission Date Time, Admission Type, Admitting Diagnosis, Attending Physician, Primary Care Physician, Room Bed, Medicaid Number, Occupation, Medicare Number, Primary Care Physician, Room Bed.

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 patient data is retained for the same amount of time that the patients' records are maintained. Audit logs for the system are retained for 7 years as required by NARA.

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.
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

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

VistA is the SOR for patient records and it has approved retention plans on file. Caribou is not the SOR for any of this information. Caribou records are maintained for at least 7 years per NARA requirements and are disposed of at VA direction after that time period has elapsed.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: RCS 10–1, Item 2000.2 Information Technology Operations and Maintenance Records destroy 3 years after agreement, control measures, procedures, project, activity, or when transaction is obsolete, completed, terminated or superseded, but longer retention is authorized if required for business use (DAA–GRS–2013–0005– 0004, item 020). RCS10–1, Item 2100.3 2100.3, System Access Records destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use (DAA–GRS–2013–0006– 0004, item 31). https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf

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

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 VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and VA Handbook 6500.1 Electronic Media Sanitization. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destruction. https://www.va.gov/vapubs/search_action.cfm?dType=1 "

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.

Testing and training are conducted on systems designated for that purpose that do not contain actual live data. Research and analysis are not conducted against the Caribou system.

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: Caribou stores PHI and PII so if the data were to be accessed it could lead to theft of identity and financial or legal consequences for the resident whose records were accessed.

Mitigation: Caribou is only accessible from within the VA network and is fully encrypted, both in transit and at rest. Long term record storage is on encrypted stores and monitored for unauthorized access.

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***
Vista	To retrieve and update the patient's health record	FirstName, Last Name, Middle Name, Sex, SSN, Race, Marital Status, Date of Birth, Date Of Death, Period Of Service, Primary Eligibility Code, Status, Admission Date Time, Admission Type, Admitting Diagnosis, Attending Physician, Primary Care Physician, Room	TCP/IP

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***
		Bed, Medicaid Number, Occupation, Medicare Number	
OPENLink, FHIR Ignite	To retrieve and update the patient's health record	FirstName, Last Name, Middle Name, Sex, SSN, Race, Marital Status, Date of Birth, Date Of Death, Period Of Service, Primary Eligibility Code, Status, Admission Date Time, Admission Type, Admitting Diagnosis, Attending Physician, Primary Care Physician, Room Bed, Medicaid Number, Occupation, Medicare Number	SSL/TLS

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: Caribou stores PHI and PII so if the data were to be accessed it could lead to theft of identity and financial or legal consequences for the resident whose records were accessed.

Mitigation: Caribou has an Authority to Connect (ATC) agreement with Oracle for the information exchanged between the systems and all exchanges are logged and monitored. The ATC documents all the safeguards in place by both parties to protect the data and communications.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received /***	***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***	***List the method of transmission and the measures in place to***

	transmitted with the specified program office or IT system		***use, etc. that permit external sharing (can be more than one)***	***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.

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: N/A

Mitigation: N/A.

Section 6. Notice

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

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

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

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

Notice is given to Veterans at the point of admission or care and is saved in the VistA system. Caribou is not the system of record for that information.

notice_privacy_practices.pdf

SORN – 79VA10 – https://www.oprm.va.gov/privacy/systems_of_records.aspx
Veterans Health Information Systems and Technology Architecture (VistA) Records - VA

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

Caribou does not provide notices to patients. That action is performed at intake and stored in VistA.

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.

Caribou does not provide notices to patients. That action is performed at intake and stored in VistA.

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.

Residents can decline to provide information to the CLC coordinators in the facilities. Caribou does not provide a forum for this to patients.

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.

Residents have the right to consent to the use of their information, but this is not a Caribou function. Consent to use is captured and stored in VistA.

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 notice isn't provided to patients, they may be unaware of their rights and obligations. This could result in inaccurate information or compromise of their record.

Mitigation: Information about notice given to veterans is stored in VistA.

Section 7. Access, Redress, and Correction

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

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

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

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

Individuals are able to request copies of their records from the designated VA offices. Caribou staff are not authorized to release information unless requested by those offices and it is only released back to those offices for return to the individual.

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).

Caribou is not a privacy act system because the Caribou system is not a SOR and Caribou staff are not authorized to release any information from the system without a request and approval from the VA privacy offices in charge of that release.

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.

Caribou is not a system of record and there is no provision for individuals to access their own records in the Caribou suite. Requests for access to records would need to go through the VA Privacy Office who could then retrieve records for release to the patient.

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.

Caribou is not a system of record and there is no provision for individuals to access their own records in the Caribou suite. Requests for changes to records would need to go through the VA Privacy Office who could then retrieve records for release to the patient. Correction of records would go through the VistA system.

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.

Individuals are able to request copies of their records from the designated VA offices. Caribou staff are not authorized to release information. Individuals making a request directly to a Caribou staff member would be directed to the VA privacy office to file the request.

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.

Caribou does not provide alternative means of access to patients.

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: The data in the Caribou system includes PHI and PII on CLC residents used for assessment and treatment purposes and shares that data with the two current EHR systems so there is sensitive data throughout the system. Since Access, Redress, and Correction are provided outside the Caribou suite, the risk is that there might be a delay in syncing data between the systems.

Mitigation: The Caribou system does not have any provision for individual access to the data. Individuals requesting changes to their data must go through the correct VA offices to request the change.

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.

In order to get an account in Caribou, users must have a VistA account and a PIV badge. Then facility administrators designate those users within the Caribou application before they can access any information. This creates 3 layers of verification of user's roles and need for access to protect the daters roles and need for access to protect the data.

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 users from other agencies within Caribou.

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.

Caribou has three roles,

Administrator – limited to system admins that have full access to the servers and database for operations and maintenance.
Resident Access Coordinator (RAC) – can create and delete accounts for their facilities, access to records.
Provider – This is staff at the CLC that have access to the resident records for the patients they are responsible for in their facility.

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.

DSS personnel are the only contractors who would have access to the system as they are the technical support and management of the system. They have all had background checks, training, and signed ROB and NDAs. DSS has a BAA on file between the company and the VA that covers this system the VA that covers this system.

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 users and admins of the Caribou system receive privacy training annually from the VA on HIPAA, Cybersecurity, and Rules of Behavior and DSS staff also are required to complete extensive training given by the company every year.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Complete
2. *The System Security Plan Status Date:* August 30, 2023
3. *The Authorization Status:* Full ATO
4. *The Authorization Date:* 08/17/2023
5. *The Authorization Termination Date:* 08/17/2025
6. *The Risk Review Completion Date:* 08/17/2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

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

N/A

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)*

VAEC Microsoft Azure Government (MAG)

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.*

Please provide response here

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.

Please provide response here

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.

Please provide response here

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).

N/A

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

ID	Privacy Controls
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

DENNIS LAHL Digitally signed by DENNIS LAHL
Date: 2023.12.11 13:40:05 -05'00'

Privacy Officer, Dennis Lahl

NEIL CRUZ Digitally signed by NEIL CRUZ
Date: 2023.12.07 15:22:01 -05'00'

Information Systems Security Officer, Neil Cruz

Tony L. Sines 167047 Digitally signed by Tony L. Sines 167047
Date: 2023.12.07 13:10:47 -06'00'

Information Systems Owner, Tony Sines

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).

notice_privacy_practices.pdf

HELPFUL LINKS:

Record Control Schedules:

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

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

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

National Archives (Federal Records Management):

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

VHA Publications:

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

VA Privacy Service Privacy Hub:

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

Notice of Privacy Practice (NOPP):

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices