The completion of Veterans Affairs Privacy Impact Assessments (PIAs) is mandated for any rulemaking, program, system, or practice that collects or uses PII under the authority of the E-government Act of 2002 (44 U.S.C. § 208(b)) and VA Directive 6508, Implementation of Privacy Threshold Analysis and Privacy Impact Assessment.

The PIA is designed to identify risk associated with the use of PII by a system, program, project or practice, and to ensure that vital data stewardship issues are addressed for all phases of the System Development Life Cycle (SDLC) of IT systems. It also ensures that privacy protections are built into an IT system during its development cycle. By regularly assessing privacy concerns during the development process, VA ensures that proponents of a program or technology have taken its potential privacy impact into account from the beginning. The PIA also serves to help identify what level of security risk is associated with a program or technology. In turn, this allows the Department to properly manage the security requirements under the Federal Information Security Management Act (FISMA).


Please note that the E-government Act of 2002 requires that a PIA be made available to the public. In order to comply with this requirement PIA will be published online for the general public to view. When completing this document please use simple, straight-forward language, avoid overly technical terminology, and write out acronyms the first time you use them to ensure that the document can be read and understood by the general public.
Privacy Impact Assessment for the VA IT System called:

Caribou Community Living Centers Suite (Cloud) Assessing Geriatrics and Extended Care (G&EC) Program Office

Date PIA submitted for review:

06/28/2021

System Contacts:

<table>
<thead>
<tr>
<th></th>
<th>Name</th>
<th>E-mail</th>
<th>Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Officer</td>
<td>Christian Loftus</td>
<td><a href="mailto:Christian.Loftus@va.gov">Christian.Loftus@va.gov</a></td>
<td>859-281-2470</td>
</tr>
<tr>
<td>Information System Security Officer (ISSO)</td>
<td>Neil Cruz</td>
<td><a href="mailto:Neil.Cruz@va.gov">Neil.Cruz@va.gov</a></td>
<td>202-632-7422</td>
</tr>
<tr>
<td>Information System Owner</td>
<td>Christopher Brown</td>
<td><a href="mailto:Christopher.Brown1@va.gov">Christopher.Brown1@va.gov</a></td>
<td>202-270-1432</td>
</tr>
</tbody>
</table>
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 increases productivity across the resident care team by integrating multiple VistA data points, while offering a low risk, high efficiency solution for healthcare professionals and OI&T resources

Overview

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

- The IT system name and the name of the program office that owns the IT system.
- The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.
- Indicate the ownership or control of the IT system or project.
- The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.
- A general description of the information in the IT system and the purpose for collecting this information.
- Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.
- Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.
- A citation of the legal authority to operate the IT system.
- Whether the completion of this PIA will result in circumstances that require changes to business processes
- Whether the completion of this PIA could potentially result in technology changes
- If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?
- What is the magnitude of harm if privacy related data is disclosed, intentionally or unintentionally? Would the reputation of the CSP or its customers (VA) be affected?

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 to support the collection of Minimum Data Set (MDS) Data to determine workload, identify quality measures as well as capture resident preferences for care.

The Caribou CLC Suite solution allows the Department of Veterans Affairs (VA) to move away from client-service technology and move towards web-based functionality.
Caribou CLC Suite provides a comprehensive and standardized assessment of each resident’s functional capabilities and help 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, replaced AccuCare, and is needed to ensure that VHA Handbook 1142.03 and the Joint Commission (TJC) standards are met for long-term facilities. This software is needed to complete comprehensive, electronic health care plans and assessments utilizing for all residents in Community Living Centers (CLCs). It also provides the capability to populate the Caribou CLC Suite tool with VistA admission, discharge and transfer 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 of Medicare and 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 of CLC residents’ quality of life.

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.


The legal authority to collect SSN was created by the Health Care Finance Administration (HCFA) now known as CMS (Centers for Medicare and 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 and Medicaid Services (CMS) to designate a RAI of 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. The physical location that will store this information is the Microsoft Azure Government Cloud in Central Texas, with fail over to Virginia.
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.

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

- Name
- Social Security Number
- Date of Birth
- Mother’s Maiden Name
- Personal Mailing Address
- Personal Phone Number(s)
- Personal Fax Number
- Personal Email Address
- Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- Financial Account Information
- Health Insurance Beneficiary Numbers Account numbers
- Certificate/License numbers
- Vehicle License Plate Number
- Internet Protocol (IP) Address Numbers
- Current Medications
- Previous Medical Records
- Race/Ethnicity
- Tax Identification Number
- Medical Record Number
- Other Unique Identifying Number (list below)

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.

Caribou CLC Suite will provide the ability to assess long-term residents, focus on individualized care plans, and evaluate the quality of care with the needed software support. It will provide a comprehensive and standardized assessment of each resident’s functional capabilities and help staff to identify health problems with real-time access to resident medical information.

Information will be 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.

PII Mapping of Components

Caribou CLC Suite consists of four (4) key components, MDS, Care Plans, ADL and Evaluation. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Caribou CLC Suite and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

<table>
<thead>
<tr>
<th>Components of the information system (servers) collecting/storing PII</th>
<th>Does this system collect PII? (Yes/No)</th>
<th>Does this system store PII? (Yes/No)</th>
<th>Type of PII (SSN, DOB, etc.)</th>
<th>Reason for Collection/Storage of PII</th>
<th>Safeguards</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL Server 10</td>
<td>Yes</td>
<td>Yes</td>
<td>Caribou Data*</td>
<td>Properly identify the resident for treatment</td>
<td>PII is visible based on security roles assigned in the software</td>
</tr>
<tr>
<td>SQL Server 11</td>
<td>Yes</td>
<td>Yes</td>
<td>Caribou Data*</td>
<td>Properly identify the resident for treatment</td>
<td>PII is visible based on security roles assigned in the software</td>
</tr>
<tr>
<td>SQL Server 12</td>
<td>Yes</td>
<td>Yes</td>
<td>Caribou Data*</td>
<td>Properly identify the resident for treatment</td>
<td>PII is visible based on security roles assigned in the software</td>
</tr>
</tbody>
</table>

Caribou Data* is as follows: 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

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

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

Describe why information from sources other than the individual is required. For example, if a program’s system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question 1.3 indicate why the system is using this source of data.
If the system creates information (for example, a score, analysis, or report), list the system as a source of information.  
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

There is a bi-directional flow of data from VistA to Caribou CLC Suite. Caribou collects data from the patient for use.

1.3 How is the information collected?

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

If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form’s OMB control number and the agency form number.  
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

Caribou CLC Suite creates and maintains a resident record based on Admit/Discharge/Transfer (ADT) information received from the VistA system via a bi-directional data flow from VistA to Caribou CLC Suite. Caribou collects data from the patient for use in methods as determined by the Resident Assessment Coordinator for that specific facility, such as verbally, digitally, paper form, or as otherwise determined best by the care provider. Those data elements are required for the completion of the MDS 3.0 form(s) and will be provided by both patient interviews and the bi-directional communication between VistA and Caribou CLC Suite. The completed MDS assessments and associated Care Plans then become a permanent part of the resident’s health record.

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

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

If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.  
This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.
A pre-defined set of resident data fields will populate the Caribou CLC Suite via the Inbound ADT interface. On the side of the application, the Caribou CLC Suite includes edit and error checking to ensure the data entered and subsequently submitted to the VAEC Azure Cloud.

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 authority was established by the Centers for Medicare and Medicaid Services (CMS) to comply with certain nursing home-related reforms required by the Omnibus Budget Reconciliation Act of 1987, Public Law (Pub. L.) No. 100-203, title IV, subtitle C, 101 Stat 1330 (1987) (OBRA ‘87). These requirements apply to all nursing homes in the United States (U.S.) that are certified by CMS. They require nursing homes to identify and act on risk factors to prevent functional decline in residents and to plan care that would delay any decline in residents’ function. The authority was implemented in all U.S. private sector nursing homes in 1990 and is updated periodically. As a matter of policy, VA uses the same CMS standardized assessment and treatment instrument for its CLC program as a means of ensuring consistency with national nursing home standards and facilitating comparisons between VA CLCs and nursing homes in the community and private sector. Legal authority to collect the data as well as what is mentioned above is 38 USC Section 501 Federal Register/Vol. No. 59/ Wednesday, March 26, 2008/Notices 16103

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

Principle of Individual Participation: Does the program, to the extent possible and practical, collect information directly from the individual?
**Principle of Data Quality and Integrity:** Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current? This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

**Privacy Risk:** SPI being transmitted to and stored at a VA hosted environment on the Business Partner Extranet. There is a possibility of ePHI being compromised once it leaves the VA network and is being transferred through the extranet to external business partners.

**Mitigation:** SPI will be transmitted via secure and encrypted electronic messaging and meets Federal Information Processing Standards (FIPS) Publication 140-2, “Security Requirements for Cryptographic Modules” The hosting facilities are FISMA High certified as required by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3 for compliance with FISMA.

**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.

The CARIBOU CLC SUITE generates Quality Measures (QMs), 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 QMs are a data source for performance measures and process improvement activities for TJC and VHA required quality improvement activities. The RAIMDS provides a structure for meeting accreditation standards. Furthermore, data from RAIMDS have increasingly become an important source of research in the development of evidence-based care for CLC residents.

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. The following data elements are collected per required protocol:

**Name:** Used to identify the patient during appointments and in other forms of communication

**Mailing Address:** Used to contact the patient or family by paper
**Phone Number:** Used to contact the patient or family by phone

**Emergency Contact Info:** Used to contact person(s) that can help provide information on the patient

**Health Insurance Beneficiary Account Numbers:** Used to identify any beneficiaries under the patient's insurance plan.

**Previous Medical Records:** Used to augment care a patient receives from medical professionals.

**Medical Record Number:** Used to verify patient identity

**Tax Identification Number:** Used to verify patient identity

**Social Security Number:** Used as a patient identifier and as a resource for verifying income information with the Social Security Administration

**Date of Birth:** Used to identify age and confirm patient identity

**Gender:** Assists in correct identification

**Ethnicity:** Provides demographic race/ethnicity specific health trend identification

**Marital status:** Allows understanding of the formal relationship the resident has and can be important for care and discharge planning

**Occupation:** helps staffs personalize interactions with the resident and are helpful for care planning purposes

**Medicare/Medicaid Number:** Assists in correct resident identification

**ICD-10 codes:** supplements active diagnoses if not listed on the form

**Admit reason:** assists with care planning

**Religion:** assists staff in understanding faith based medical decisions and providing religious services while in the nursing home

**Admission date:** to document the date of admission into the nursing home Patients ward: required for delivering medications and meals

**Room:** required for delivering medications and meals

**Bed number:** required for delivering medications and meals

**Treating specialty:** identifies the general category of services provided

**Death date:** used to identify the day the resident died

**Current Medications:** used to complete multiple MDS assessment sections. For example, Section E: Behavior (did resident reject evaluation or care, e.g. taking medications), Section J: Health Conditions (received PRN pain medications), Section N: Medications. This information is viewed based on a lookback period (5 days) and is not retained in the Caribou CLC Suite database.

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

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

If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the
individual’s existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

The resident data maintained in the Caribou CLC Suite will be used for the creation on the standardized MDS 3.0 forms. Data to complete the MDS records are electronically submitted to the Verizon Hosting facility in Culpepper, VA and will be backed up to the Verizon Data Center in Miami, FL. Progress Notes are created for assessments and returned through secure channels to be saved with the patient’s health record in VistA. No analysis is conducted within the application, data is input into datasets which are saved to patient’s health records.

2.3 How is the information in the system secured?
   2.3a What measures are in place to protect data in transit and at rest?
   
   2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs?

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

Data is transmitted via TLS 1.2 and stored on Microsoft Azure Gov Cloud servers, therefore encrypted at the disk level.

SSNs are only viewable in partial form, IE the last four digits are viewable to only to those with permission to view the patient’s record. Permissions to patient’s records within a facility are determined by the Resident Assessment Coordinator (RAC) who can grant care Providers with the ability to see a patient’s record as need-be for care. SSNs are encrypted at rest and in transit.

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

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

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

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


Access to PII is determined by VA IAM through assignment of predefined roles within Caribou. VA IAM manages their requirements for granting access to roles with access to PII, Caribou provides documentation of what level of information each role has to the VA IAM.

Access is determined through VA IAM procedures

Assurance of safeguards to PII is a hybrid responsibility between the vendor, VA, and Cloud Service Provider.

**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 resident record in the Caribou CLC Suite includes: Name, Social Security Number, Date of Birth, Mailing Address, Zip Code, Phone Number, Health Insurance Beneficiary Numbers Account numbers, Emergency Contact Information (Name, Phone Number, etc of a different individual) and Race/Ethnicity

### 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.

This question is related to privacy control DM-2, Data Retention and Disposal.
Records will be maintained throughout the term of the contract. Upon the conclusion of the contract and subsequent terms, the information will be transitioned to the VA for retention in accordance with RCS 10-1. https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so please indicate the name of the records retention schedule.

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner.

This question is related to privacy control DM-2, Data Retention and Disposal.

Yes, these records will be maintained in accordance with RCS 10-1 and are retained for 75 years. https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf. The system is live in PROD and the retention schedule has been approved.

3.4 What are the procedures for the elimination of SPI?

Explain how records are destroyed or eliminated at the end of the retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc?

This question is related to privacy control DM-2, Data Retention and Disposal

When the Caribou CLC Suite system owner decides the data is no longer needed, Caribou CLC Suite will follow the data deletion policies set forth by the VA for eliminating privacy data. VA Directive 6500 requires the removal of sensitive information on automatic data processing equipment (ADPE) storage media shall be conducted prior to disposal of the equipment. VA shall ensure that all offices and facilities include policy and procedures in their computer security programs for the protection of sensitive information on automatic data processing equipment (ADPE) storage media during the disposal of storage media. Procedures for implementing the policies in this section are found in VA Handbook 6500.

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

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?

This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research
For testing, development and training Caribou CLC Suite does not utilize PII. The environment for Development and pre-production do not have access to any other systems that contain PII.

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.

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

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

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

**Principle of Data Quality and Integrity:** Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged? This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:

**Privacy Risk:** There is a risk that information may be archived longer than necessary

**Mitigation:** PHI or SPI will be maintained throughout the duration of the project, but only as required in order to support the project. At which time, any PHI or SPI will be returned to the VA for retention in accordance with RCS 10-1, therefore the records will be retained for 75 years. https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA. NOTE: Question 5 on Privacy Threshold Analysis should be used to answer this question.

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 3.10 (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

<table>
<thead>
<tr>
<th>List the Program Office or IT System information is shared/received with</th>
<th>List the purpose of the information being shared/received with the specified program office or IT system</th>
<th>List the specific data element types such as PII/PHI that are shared/received with the Program Office or IT system</th>
<th>Describe the method of transmittal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vista</td>
<td>Caribou CLC Suite provides a comprehensive and standardized assessment of each resident’s functional capabilities and help staff to identify health problems with real-time access to resident medical information</td>
<td>FirstName, LastName, MiddleName, Sex, SSN, Race, MaritalStatus, DateOfBirth, DateOfDeath, PeriodOfService, PrimaryEligibilityCode, Status, AdmissionDateTime, AdmissionType, AdmittingDiagnosis, AttendingPhysician, PrimaryCarePhysician, RoomBed, MedicaidNumber, Occupation, MedicareNumber</td>
<td>VistA Service Oriented Architecture uses a direct Transmission Control Protocol connection to VistA by specifying the IP address or Fully Qualified Domain Name of the VistA server and port in the VSOA config.xml file</td>
</tr>
</tbody>
</table>
4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks.

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

Follow the format below:

Privacy Risk: Minimum Data Set (MDS) 3.0, the Care Area Assessments (CAA) and Care Plan documents are transmitted out of VistA to a non-VA hosted environment.

Mitigation: All documentation is transmitted to a Federal Information Security Management Act High hosted environment via secure SOA Application Programming Interface messages. In addition, all personnel with access to Veteran information must complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually.

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 3.11 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

<table>
<thead>
<tr>
<th>List External Program Office or IT System information is shared/received with</th>
<th>List the purpose of information being shared / received / transmitted with the specified program office or IT system</th>
<th>List the specific data element types such as PII/PHI that are shared/received with the Program or IT system</th>
<th>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</th>
<th>List the method of transmission and the measures in place to secure data</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

If specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16, note them here.

None

### 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:** Personal demographic information being transmitted to and stored in a non-VA hosted environment

**Mitigation:** Personal demographic information will be transmitted via secure SOA API messages. All personnel with access to Veteran’s information are required to complete the VA Privacy and Information Security Awareness training and Rules of Behavior annually and to complete and pass a Federal background investigation. Information is shared in accordance with VA Handbook 6500.
Section 6. Notice

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

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

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

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

Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection. This question is related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

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

The method of collection will vary per facility; however, the patient will be notified by form or by notice dependent on the facility and the care providers choice. The PIA and SORN will serve as a form of notice.


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

The individuals have already provided answers to the questions and the information is pulled from VistA therefore they have already given their implied consent. If the person does not want to participate, they do not get the service. However, if an individual wish to remove consent for
a particular use of their information, they should contact the nearest VA regional office, a list of which can be found at http://benefits.va.gov/benefits/offices.asp

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

Once information is provided to the VA, the records are used, as necessary, to ensure the administration of statutory benefits to all eligible Veterans, Service members, reservists, and their spouses, surviving spouses and dependents. As such, the CARIBOU CLC SUITE does not provide individuals with the direct opportunity to consent to particular uses of information. However, if an individual wish to remove consent for a particular use of their information, they should contact the nearest VA regional office, a list of which can be found at http://benefits.va.gov/benefits/offices.asp

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.

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: There is a risk that a veteran may not be aware that their information is being used or collected.

Mitigation: VA mitigates this risk by providing veterans and other beneficiaries with multiple forms of notice of information collection, retention, and processing. The three main forms of notice are discussed in detail in question 6.1 and include the Privacy Act statement, a System of Record Notice, and the publishing of this Privacy Impact Assessment.
Section 7. Access, Redress, and Correction

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

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

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

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

If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information. This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

All information that is submitted becomes part of the health record. Requests for information can be requested through the privacy officer at their facility. A list of regional VA offices may be found at: http://benefits.va.gov/benefits/offices.asp

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.

All information that is submitted becomes part of the health record. An amendment request may be requested if the information is incorrect, the process is that the individual must make the request in writing to the Privacy Officer at the facility where they are receiving care and then it will be amended if the information is incorrect.

7.3 How are individuals notified of the procedures for correcting their information?

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.
The individual goes to the Privacy Officer where they receive their care and requests an amendment to their record. They are notified in their Notice of Privacy Practice as well as asking someone at the facility and then they will be referred to the Privacy Officer. This Privacy Impact Assessment (PIA) also serves as notice of CARIBOU CLC SUITE. As required by the eGovernment Act of 2002, Pub.L. 107–347§208(b)(1)(B)(iii), the Department of Veterans Affairs “after completion of the [PIA] under clause(ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means.”

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems.

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

Example: Some projects allow users to directly access and correct/update their information online. This helps ensure data accuracy.

The Privacy Act and HIPAA law allow right of access to the individual’s record as well as for making an amendment request. This is done through the facility Privacy Officer and there is a formal redress process in place.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

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

This question is related to privacy control IP-3, Redress.
Follow the format below:

**Privacy Risk:** There is a risk that members of the public will not know the relevant procedures for gaining access to, correcting or contesting their information.

**Mitigation:** The privacy risk is mitigated by this Privacy Impact Assessment (PIA) which also serves as notice of CARIBOU CLC SUITE. The individual goes to the Privacy Officer where they receive their care and requests an amendment to their record. They are notified in their Notice of Privacy Practice as well as asking someone at the facility and then they will be referred to the Privacy Officer.

**Section 8. Technical Access and Security**

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

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

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

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

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

*This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.*

Caribou CLC Suite user roles are created based on VA Clinical Living Center (CLC) job titles. Each user is assigned a user role and provided the appropriate level of access to the system. Caribou CLC Suite is accessed via the internet web browser after authentication and authorization using VA Identity Access Management protocols. Only VA System Owner approved users with VA network approved access will have the ability to log into Caribou CLC Suite.

There are 3 basic categories of User Roles:

1. **Full Access** - These “Super Users” are limited to the system owner and VA Subject Matter Experts for each CLC a. These users also can add new approved users

2. **Limited Access** – These users are provided read/write access to specific application modules based on their Job Title and User Role a. These users have read/write capabilities to specific system modules
3. Read Only Access - These users can review only their site information. They do not have the ability to modify the system or its information

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.

Yes, contractors will have access to Caribou CLC Suite in order to provide Help Desk and application support throughout the duration of the contract. The contract will be reviewed throughout the project lifecycle by DSS project stakeholders. All confidentiality agreement and non-disclosure agreements have been signed and collected. They are available from DSS Privacy and Security Officer and have been delivered to the VA’s Privacy and Security Office.

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 contract Project Management, Implementation, Education and Help Desk employees working on VA contracts are required to take privacy and security training as well as HIPAA training upon hire and annually thereafter in the VA’s TMS system as well as on the DSS Cornerstone training site.

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

If Yes, provide:

1. The Security Plan Status,
2. The Security Plan Status Date,
3. The Authorization Status,
4. The Authorization Date,
5. The Authorization Termination Date,
6. The Risk Review Completion Date,
7. The FIPS 199 classification of the system (LOW/MODERATE/HIGH).

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

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

1) Approved
2) 21-Dec-2020
3) Authorization to Operate
4) 27-May-2021
5) 26-May-2024
6) 27-Apr-2021
7) High

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, 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.

This question is related to privacy control UL-1, Information Sharing with Third Parties.

Yes, Caribou is hosted in the VAEC

9.2 Identify the cloud model being utilized.

Example: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS).

This question is related to privacy control UL-1, Information Sharing with Third Parties.

Caribou is Commercial-of-the-Shelf (COTS)
9.3 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract)

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

Yes, per page 50/77 and page 73/77 of contract 36C10B21C0010 respectively

“Contractor shall train all of their employees involved in the performance of this contract on their roles and responsibilities for proper handling and nondisclosure of sensitive VA or proprietary information. Contractor personnel shall not engage in any other action, venture or employment wherein sensitive information shall be used for the profit of any party other than those furnishing the information. The sensitive information transferred, generated, transmitted, or stored herein is for VA benefit and ownership alone.”

“Ownership of PHI. PHI is and remains the property of Covered Entity as long as Business Associate creates, receives, maintains, or transmits PHI, regardless of whether a compliant Business Associate agreement is in place.”

9.4 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.

Ancillary or auxiliary data is not explicitly referred to within the contract.

9.5 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.
Per page 56/77 of the contract

“The vendor shall ensure the security of all procured or developed systems and technologies, including their subcomponents (hereinafter referred to as “Systems”), throughout the life of this contract and any extension, warranty, or maintenance periods. This includes, but is not limited to workarounds, patches, hot fixes, upgrades, and any physical components (hereafter referred to as Security Fixes) which may be necessary to fix all security vulnerabilities published or known to the vendor anywhere in the Systems, including Operating Systems and firmware. The vendor shall ensure that Security Fixes shall not negatively impact the Systems.”

Any further security and privacy requirements established by the VA regarding data held by a cloud provider are covered under VAEC AWS MAG - Risk Acceptance Memo CA-3, the latest as of time of completion of the PIA was March 5, 2021, which states

“Risk Acceptance Duration and Conditions: Based on this rationale, the ECSO approves this Risk Acceptance for VAEC AWS GovCloud High Accessing & VAEC MAG High Accessing from the date of this memo. This memo is valid until the ECSO rescinds this Risk Acceptance. VAEC users or any other project teams within the environment should contact the ECSO immediately if any material changes occur regarding any connections which could negatively impact the security or performance of the VAEC.”

9.6 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**

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

Version Date: May 1, 2021

Page 26 of 29
<table>
<thead>
<tr>
<th>ID</th>
<th>Privacy Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>UL-1</td>
<td>Internal Use</td>
</tr>
<tr>
<td>UL-2</td>
<td>Information Sharing with Third Parties</td>
</tr>
</tbody>
</table>
Signature of Responsible Officials

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

CHRISTIAN D LOFTUS 222466
Digitally signed by CHRISTIAN D LOFTUS 222466
Date: 2021.08.03 11:06:57 -04'00'

Privacy Officer, Christian Loftus

Neil F. Cruz 341838
Digitally signed by Neil F. Cruz 341838
Date: 2021.07.28 12:17:10 -04'00'

Information System Security Officer, Neil Cruz

Christopher Brown 101386
Digitally signed by Christopher Brown 101386
Date: 2021.07.28 14:15:09 -05'00'

Information System Owner, Chris Brown
APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy, a Privacy Act notice on forms).