Privacy Impact Assessment for the VA IT System called:

Community Care Veterans Billing System Cloud (CC VBS Cloud)

Digital Experience
Veterans Health Administration

Date PIA submitted for review:

09/23/2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Rhonda Spry	Rhonda.Spry@va.gov	615-355-3408
Information System Security Officer (ISSO)	Mark Farris	Mark.Farris.@va.gov	407-599 8521
Information System Owner	Christopher Johnston	Christopher.Johnston2@va.gov	202-503-6267

Abstract

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

The Community Care Veteran Billing System Cloud (CC VBS Cloud) is hosted within the VAEC AWS Cloud platform. CC VBS Cloud displays billing and medication information via MyHealtheVet. CC VBS Cloud receives a flat file from Consolidated Copayment Processing Center (CCPC) via SFTP. This file provides veteran name, mailing address, current medication, and billing information. This information is displayed on the MyHealtheVet website for the veteran. The system integrates with the MyHealtheVet system via URL via the Identity and Access Management (IAM).

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* VAEC Amazon.
- *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?*

The Veterans Billing System Cloud (CC VBS Cloud) System is a Web Application that has the following functionality and configuration:

1. Provides a Graphical User Interface (GUI) allows Veterans to view their billing statements from an Internet Browser.

2. Interfacing with MyHealtheVet (MHV) provides Veterans secure online access to CC VBS Cloud. To access the CC VBS system, the Veteran must have a VA access.

3. CC VBS is a major system hosted within the VAEC AWS Cloud platform.

4. The system is covered by the same set of SORNs as CBSS and are listed in GRC (HQ) under the Veteran Billing Statement Assessment. SORN 114VA17, The Revenue Program-Billing and Collections Records-VA and Title 38, United States Code, section 1710 and 1729.

5. Completion of this PIA will not result in a change of business processes.

6. The magnitude of unintentional or intentional disclosure of privacy related data will have limited impact to the VA or the Veteran. Should a system breach occur directly to CC VBS Cloud, there is no Veteran data stored within the system. Data is stored on AWS Dynamo DB.

7. Users of the CC VBS Cloud system are Veterans who are looking to view their billing statements online. Once the Veteran's CC VBS Cloud's web session has ended (either by log out or time out), CC VBS will not retain these statements.

8. CC VBS Cloud is hosted at the VA Enterprise Cloud (VAEC-AWS) deployed at Amazon Web Services (AWS). This commercial cloud environment is FedRAMP accredited. An agreement between CC VBS Cloud and VAEC-AWS defines the security and VA-ownership of all data in the CC VBS system.

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 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
- ☐ Gender
- ☐ Integration Control Number (ICN)
- ☐ Military History/Service Connection
- ☐ Next of Kin
- ☒ Other Unique Identifying Information (list below)
  - Data File Number
  - Zip Code
  - Billing Information

PII Mapping of Components

Veterans Billing System Cloud consists of 1 key component. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Veterans Billing System Cloud and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

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.

PII Mapped to Components

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
CC VBS Web Application	No	Yes (Receives a PDF that contains PII)	• Name • Mailing • Address • Zip Code • Medication and billing information	Information is visible only to the veteran accessing the application	They log in via Access VA. In order to access the CC VBS Cloud system the CC VBS users must have an IAM compatible login [Id.me, DoD Self Service (DS) login, MHV Login] Credential from the Identity and Access Management Services

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.

CC VBS Cloud interfaces with Consolidated Co-payment Processing Center (CCPC) and VA CCPC Access via AccessVA but does not collect Sensitive Personal Information (SPI), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy-Protected Information per se'. CC VBS Cloud provides the dissemination of billing statements for the Veteran to view via MHV. CC VBS Cloud does not collect any Sensitive Personal Information (SPI), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy Protected Information per se'. CC VBS Cloud receives data from

Consolidated Co-payment Processing Center (CCPC) system. Veterans Health Information Systems Technology Architecture (VistA) transmit data to CCPC.

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.

CC VBS Cloud receives information in a file from CCPC via SFTP. It is only displayed on the MyHealtheVet Portal.

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.

Transfer of files between CC VBS Cloud and CPCC is done via SFTP service as detailed in the System Design Document (SDD). CC VBS Cloud does not collect any Sensitive Personal Information (SPI), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy- Protected Information per se'. As information is imported from existing VA systems, the accuracy is verified by the original source.

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

Public Law 99-272, Consolidated Omnibus Budget Reconciliation Act of 1985, April 7, 1986, allowed VA to bill health insurance companies for all non-service-connected (NSC) veterans. The law also established the Means Test Program. Means Testing enables the VA to categorize veterans, according to income, and to collect appropriate copayments for outpatient and inpatient healthcare services. CC VBS Cloud operates under system of record notice (SORN) 114VA17, The Revenue Program-Billing and Collections Records-VA and Title 38, United States Code, section 1710 and 1729.

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.

Privacy Risk: Sensitive personal information (SPI), if breached or accidentally released to inappropriate parties or the public, could result in financial, personal, and/or emotional harm to the individuals whose information is contained in the system.

Mitigation: The Department of Veterans Affairs is careful to only collect the information necessary to identify the parties involved in an incident, identify potential issues and concerns, and offer assistance to the affected parties so that they may find the help they need to get through their crisis. By only collecting the minimum necessary information, the VA is able to better protect the individual's information.

• CC VBS adheres to information security requirements instituted by VA Office of Information and Technology (OIT)

• All employees with access to the PII/PHI are required to complete the VA Privacy Information Security Awareness Training and Rules of Behavior, annually.

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.

Name: Patient Identifier
Personal Mailing Address: Used to contact the individual
Medication: Itemized billing list
Data File Number: Part of account number
Billing Information: Used to contact the individual
Zip Code: Used to contact the individual

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 CC VBS Cloud application increases Veterans' satisfaction, by allowing them to view their monthly billing statement online. Veteran will logon via AccessVA to My HealtheVet and select CC VBS. CC VBS will use the data file number (DFN) supplied by Identity and Access Management Services (IAM) to retrieve a list of available billing statements received from Consolidated Copayment Processing Center (CCPC). The Veteran will select the desired billing statement to display. The PDF billing statement may contain: Name, Mailing Address, Zip Code, and Medications.

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 CC VBS Cloud application will not be used for data analytics. The GUI will not have features that allow for data extraction. The functions of the system are for receiving billing data and displaying PDF billing statements received from the Consolidated Copayment Processing Center (CCPC) to the Veteran.

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?

The VAEC AWS High protects the confidentiality and integrity of sensitive and confidential data while at rest. All sensitive and confidential data is encrypted using FIPS 140-2 compliant algorithms. The VAEC AWS High system only utilizes products from the TRM that has the capability to ensure protection of information at rest. The SS CC VBS Cloud application relies on the VAEC AWS High protection of information at rest.

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

n/a CC VBS Cloud does not access/ utilizes SSNs

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

Each VA employee or contractor of the VA is required to undergo annual Privacy and Security training (PISA), annual HIPAA training, as well as signing the Contractor Rules of Behavior (CROB) upon initial hire.

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

2.4 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u> 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.

As described in section 2.2, there are no tools for data analytics. Access is restricted to the Veteran's own information. To gain access to CC VBS Cloud, Veteran will logon via AccessVA to My HealtheVet and select CC VBS. Logon Credential is managed by the Identity and Access Management Services.

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

CC VBS Cloud is not the source of record for billing statements and does not retain billing statements or any of the individual information displayed on the billing statement. There are no data elements retained.

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. If the system is using cloud technology, will it be following the NARA approved retention length and schedule?

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.

CC VBS Cloud is not the source of record for billing statements and does not retain billing statements. A Veteran will log into the CC VBS application will logon via AccessVA to My HealtheVet and select CC VBS .CC VBS electronically received a PDF billing statement for the Veteran. The PDF statement is only available while the Veteran's web session is active. The PDF statement is not retained once the Veteran's web session has ended.

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.

CC VBS follows the requirement of RCS 10–1 Chapter 4 Item 4000.1 a & b. 4000.1 Financial transaction records related to procuring goods and services, paying bills, collecting debts, and accounting. a. Official record held in the office of record. Temporary; destroy six (6) years after final payment or cancellation, but longer retention is authorized if required for business use. (GRS 1.1, Item 010) (DAA–GRS–2016–0001–0002) b. All Other copies Temporary; destroy or delete when six (6) years old, but longer retention is authorized if required for business use. (GRS 1.1 item 013, this should be listed as item 11.) (DAA–GRS–2016– 0001–0002)

CC VBS Cloud is not the source of record for billing statements and does not retain billing statements. A Veteran will log into the CC VBS application via AccessVA to My HealtheVet and select CC VBS. CC VBS electronically received a PDF billing statement for the Veteran. The PDF statement is only available while the Veteran's web session is active. The PDF statement is not retained once the Veteran's web session has ended.

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

CC VBS Cloud is not the source of record for billing statements and does not retain billing statements or any of the individual information displayed on the billing statement. Follow the requirement of RCS 10–1 Chapter 4 Item 4000.1 a & b. 4000.1 Financial transaction records

related to procuring goods and services, paying bills, collecting debts, and accounting. a. Official record held in the office of record. Temporary; destroy six (6) years after final payment or cancellation, but longer retention is authorized if required for business use. (GRS 1.1, Item 010) (DAA–GRS–2016–0001–0002) b. All Other copies Temporary; destroy or delete when six (6) years old, but longer retention is authorized if required for business use. (GRS 1.1 item 013, this should be listed as item 11.) (DAA–GRS–2016– 0001–0002)

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

Real PII is not used for these purposes. The only information used for research, testing and training is that which is created specifically for these purposes and uses only made up names and other entry field information.

3.6 <u>PRIVACY IMPACT ASSESSMENT: Retention of information</u>

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:

<u>Principle of Minimization:</u> 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?

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

Privacy Risk: There is a risk that the information maintained by CC VBS could be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached.

Mitigation: To mitigate the risk posed by information retention, CC VBS does not retain billing statements once the Veteran's CC VBS Cloud web session has ended (either by logout or timeout)

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***
Consolidated Copayment Processing Center (CCPC)	Information received from CCPC is the PDF billing statement to be displayed in CC VBS	Name, Mailing Address, Zip Code, Current Medications, Billing Information	SFTP
Debt Resolution/ VODA	Purpose is so Veterans can view their Patient Statements on the VA Site	Billing information is shared with the VODA application	API

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.

Privacy Risk: The privacy risk associated with maintaining SPI is that sharing data within the Department of Veterans' Affairs could happen and that the data may be disclosed to individuals who do not require access and heightens the threat of the information being misused.

Mitigation: CC VBS Cloud users only have access to their own data being displayed in the CC VBS application. User access is restricted to Veteran's with IAM compatible (Id.me, DS login, MHV Login) Credential from the Identity and Access Management Services. There are no CC VBS Cloud Administrative roles that would allow its personnel to view a Veteran's data.

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 / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
none	n/a	n/a	n/a	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

Privacy Risk: The privacy risk associated with maintaining SPI is that sharing data outside of the Department of Veteran's Affairs could increase the risk that data may be disclosed to individuals who do not require access and heightens the threat of the information being misused.

Mitigation: CC VBS Cloud users only have access to their own data being displayed in the CC VBS application. User access is restricted to Veteran's with IAM compatible (Id.me, DS login, MHV Login) Credential from the Identity and Access Management Services

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.

The System of Record Notice (SORN) 114VA17 - The Revenue Program Billings and Collection Records-VA

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

6.2 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

No information is directly collected from the Veteran by CC VBS Cloud, so there is no opportunity to decline to provide information. A Veteran may have the opportunity or notice of the right to decline to provide information to the source systems that collects the information from the Veteran. By declining to supply information to the source system, the Veteran would also be declining the information to the CC VBS Cloud system.

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

Any right to consent to particular uses of the information would be handled by the source systems that collect the information from the Veteran and feed CC VBS Cloud with information.

6.4 <u>PRIVACY IMPACT ASSESSMENT: Notice</u>

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:

<u>Principle of Transparency:</u> Has sufficient notice been provided to the individual?

<u>Principle of Use Limitation:</u> Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?
This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use

Privacy Risk: There is a risk that an individual may not receive notice that their information is being Version collected, maintained, processed, or disseminated by CC VBS.

Mitigation: The information displayed in CC VBS Cloud is the individuals billing statement which is identical to the billing statement mailed to the individual. Additional mitigation is provided by making the System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) available for review online, as discussed in question 6.1.

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.

To gain access to the CC VBS Cloud application, Veterans must obtain an IAM compatible login (Id.me, DS login, MHV Login) Credential from the Identity and Access Management Services. These processes and procedures are external to the CC VBS application and are managed by the Identity and Access Management Services.

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.

Under the jurisdiction of VHA, VHA Handbook 1605.1 Appendix D 'Privacy and Release Information', section 8 states the rights of the Veterans to amend to their records via submitting VA Form 10-5345a, Individual's Request for a Copy of Their Own Health Information, may be

used as the written request requirement, which includes designated record sets, as provided in 38 CFR 1.579 and 45 CFR 164.526. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the facility Privacy Officer, or designee, to be date stamped; and is filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579.

7.3 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.

Any correction/update to an individual's information would have to adhere to the source system's protocols. Individuals are not notified if there is missing or inaccurate information in their record. An individual who wishes to determine whether a record is being maintained under his or her name in the CC VBS Cloud system or wishes to determine the contents of such records should submit a written request or apply in person to the VA facility where the records are located.

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 ensures data accuracy.

There are no provisions for correcting inaccurate or erroneous information in CC VBS Cloud. The information in CC VBS Cloud is obtained electronically from other VA systems. Individuals would not gain access to correct/update information in CC VBS; and instead they would have to go through the source system's protocols to correcting the data

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.

Privacy Risk: There is a risk that erroneous information is displayed in CC VBS if erroneous data is placed in the upstream VA systems.

Mitigation: The information displayed in CC VBS is obtained directly from CCPC which obtains all of its information from other VA systems. If there is erroneous or inaccurate information, it should be addressed in the upstream systems. Any validation performed would merely be the Veteran personally reviewing the information before they provide it. Individuals are allowed to provide updated information for their records by submitting new forms or correspondence and indicating to the VA that the new information supersedes the previous data

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.

The CC VBS Cloud application only has a single role and to access CC VBS Cloud users must have an IAM compatible login (Id.me, DS login, MHV Login) Credential from the Identity and Access Management Services.

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.

Only Veterans will have access to the CC VBS Cloud application. Contractors would only have access to CC VBS Cloud if they are a Veteran with an IAM compatible login (Id.me, DS login, MHV Login) Credential from the Identity and Access Management Services would be accessing the application as a Veteran, not in their capacity as a Contractor. These processes and procedures are external to the CC VBS Cloud application and are managed by the Identity and Access Management Services.

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.

Users of CC VBS Cloud are Veterans who login thru the My HealtheVet portal using IAM compatible login (Id.me, DS login, MHV Login) Credential from the Identity and Access Management Services. These processes and procedures are external to the CC VBS application and are managed by the Identity and Access Management Services. Veterans who access CC VBS are only able to access their own billing statements

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

If Yes, provide:

1. *The Security Plan Status: Approved*
2. *The Security Plan Status Date: 10/16/2020*
3. *The Authorization Status: Current*
4. *The Authorization Date: 12/17/2020*
5. *The Authorization Termination Date:12/17/2023*
6. *The Risk Review Completion Date:09/30/2020*
7. *The FIPS 199 classification of the system: MODERATE*

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

Section 9 – Technology Usage

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

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

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS).

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.

CC VBS Cloud is hosted within the VAEC AWS HIGH.

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)

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

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.

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.

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).

.

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 they provided in this Privacy Impact Assessment is true and accurate.

RHONDA SPRY-WOMACK

Digitally signed by RHONDA SPRY-WOMACK
Date: 2022.11.18 09:50:28 -06'00'

Privacy Officer, Rhonda Spry

MARK B. FARRIS 1637602

Digitally signed by MARK B. FARRIS 1637602
Date: 2022.11.22 13:52:32 -05'00'

Information System Security Officer, Mark Farris

Digitally signed by Christopher M. Johnston 1593443
Date: 2022.11.22 15:27:46 -05'00'

Information System Owner, Christopher Johnston

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).