Privacy Impact Assessment for the VA IT System called:

Veteran Copayment Lockbox (VAEC)

Veterans Health Administration (VHA)

Revenue Operations (vha-104RO)

eMASS ID 2111

Date PIA submitted for review:

05/23/2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Akeel Omari	Akeel.Omari@va.gov	404-432-3171
Information System Security Officer (ISSO)	Amine Messaoudi	Amine.Messaoudi@va.gov	202-815-9345
Information System Owner	Jeffrey Rabinowitz	Jeffrey.Rabinowitz@va.gov	732-720-5711

Abstract

The abstract provides the simplest explanation for "what does the system do?".
Veteran Copayment Lockbox (VCPL) is modernization of the legacy Lockbox (VCPL) system, which will modernize the Lockbox graphical user interface (GUI), and provide a technical refresh to continue to automatically post payments to the patients account and subsequently report payments to the VA's account system, Financial Management System (FMS) and for the Financial Services Center (FSC). Personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive inform.

Overview

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

1   *General Description*
      A.   What is the IT system name and the name of the program office that owns the IT system?
Veteran Copayment Lockbox (VCPL); Revenue Operations (VHA-104RO)

      B.   What is the business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?
The system supports the centralized collection of checks and credit card payments at a lockbox bank and automates the steps necessary to apply those funds to a patient's account that resides at the VA Medical Centers (VAMC's)

      C.   Who is the owner or control of the IT system or project?
The Veteran Copayment Lockbox (VCPL) is owned by Department of Veterans Affairs (VA), Veterans Health Administration (VHA); specifically, the VHA Chief Business Office

2. Information Collection and Sharing
      D.   What is the expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual?
Approximately 7,471,935 Veterans or dependents who have visited a VAMC have their information.

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

The Veteran Copayment Lockbox (VCPL) system supports the centralized collection of checks and credit card payments at a lockbox bank.

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

The Veteran Copayment Lockbox (VCPL) system supports the centralized collection of checks and credit card payments at a lockbox bank. Each month, VAMC Accounts Receivable (AR) locations send a transmission via DMI (Data Management Interface) to the Austin-based Consolidated Co-payment Processing Center (CCPC) System. The transmission file contains patient identifying information and accounts receivable copayment charges (which may include prescriptions, late fees, etc.). The patient file is shared with VCPL. CCPC generates and mails the Patient Statements (equivalent to a "bill"). At the bottom of the statement is a tear-away return coupon. The payment is mailed to the lockbox bank, US Bank. Once the payment information is processed, US Bank deposits the funds in the VA's Treasury account, scans the payment coupons and account information on checks (when used) and creates a file of electronic payment information that retrieves each workday (Monday through Friday). These transactions are distributed to the appropriate VAMC via the mainframe for automatic posting to the patient's account and subsequent reporting into the VA's accounting system, Financial Management System (FMS). The browser based VCPL uses the VA Intranet to provide online database queries and update features for the Financial Services Center (FSC) to resolve unidentified payments. In addition to online query capabilities, VCPL provides browser- based reporting functionality.

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

All the components pertaining to VCPL are within the Cloud. Therefore, the same controls are used across sites.

3. Legal Authority and SORN
> *H. What is the citation of the legal authority to operate the IT system?*

VCPL operates under system of record notices (SORN):
SORN 114VA10, "The Revenue Program-Billing and Collections Records-VA",
https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01541.pdf. **Authority for maintenance of the system can be found in Title 38, United States Page 4 of 31**

Code, section 1710 and 1729
SORN 79VA10, "Veterans Health Information Systems and Technology
Architecture (VistA) Records-VA",
https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf.
Authority for maintenance of the system can be found in Title 38, United States
Code, section 7301(a)

> I.   *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?*

The SORNs do not need to be updated at this time.

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

The completion of this PIA will not require further changes to either the business processes or technology changes.

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

The completion of this PIA will not require further changes to either the business processes or technology changes.

Section 1. Characterization of the Information

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

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

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

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

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

☒ Name
☒ Social Security Number
☐ Date of Birth
☐ Mother's Maiden Name
☒ Personal Mailing Address
☐ Personal Phone Number(s)
☐ Personal Fax Number
☒ Personal Email Address
☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
☒ Financial Information

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

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

Other PII/PHI data elements:
- VCPL User ID
- Patient Account Number
- Deposit Ticket Number

PII Mapping of Components (Servers/Database)

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

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

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
Patient Table in PostgreSQL RDS MS	Yes	Yes	Acct Number First-Name	Information is needed to research unidentified	Files are Secure File Transfer Protocol

---

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

			Middle-Name Last-Name SSN	payments and to post payments at the VAMC's	(SFTP) to/from the server. Only authorized users have access to the data
Payment Item Table in PostgreSQL RDS MS	Yes	Yes	Acct-Number First-Name Middle-Name Last-Name SSN	Information is needed to research unidentified payments and to post payments at the VAMC's	Files are Secure File Transfer Protocol (SFTP) to/from the server. Only authorized users have access to the data

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

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.2a List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

Data available through VCPL collected electronically from the US Bank- LBX Bank and CCPC system. VCPL does not collect sensitive personal information (SPI) directly from individuals.

1.2b Describe why information from sources other than the individual is required? For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question indicate why the system is using this source of data. 1.2c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?

Data available through VCPL collected electronically from the US Bank- LBX Bank and CCPC system. VCPL does not collect SPI directly from individuals. VCPL transmits payment information to the VAMCs to post payments to the corresponding accounts.

1.3 How is the information collected?

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.3a This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technologies used in the storage or transmission of information in identifiable form?

VCPL receives all data via secure electronic transfer from other systems using various transfer methods such as Secure File Transfer Protocol (SFTP) and Hypertext Transfer Protocol over SSL (Secure Socket Layer)-HTTPS

1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, what is the form's OMB control number and the agency form number?
No information is collected on a form. All information is done electrically.

1.4 How will the information be checked for accuracy? How often will it be checked?
These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

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

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

VCPL checks that information was checked for accuracy when it was first entered into the host system. VCPL is not public-facing application.

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

ORN 114VA10, "The Revenue Program-Billing and Collections Records-VA", https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01541.pdf. **Authority for maintenance of the system can be found in Title 38, United States Code, section 1710 and 1729**
SORN 79VA10, "Veterans Health Information Systems and Technology Architecture (VistA) Records-VA", https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf. **Authority for maintenance of the system can be found in Title 38, United States Code, section 7301(a)**

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete this section)

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

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

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

Principle of Individual Participation: Does the program, to the extent possible and practical, collect information directly from the individual?

Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?
This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:

Privacy Risk:
Because VCPL collects its data from external sources, there is a risk that data could be corrupted during data transfer and/or host system data entry.

Mitigation:
All data is transmitted across encrypted links. The query and report functions are only available on the VA intranet. VCPL has restricted role-based users helping to ensure that all users do not have open access to the system and have restricted access to the information needed to perform their job function applying the principle of least privilege.

Section 2. Uses of the Information

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

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

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

PII/PHI Data Element	Internal Use	External Use
Veteran's Identification	Used to verify Veteran Identity	Not used
Social Security Number	Used to verify Veteran Identity	Not used
Personal Account Information	Used Payment for VA services	Not used
Credit Card Number	Used Payment for VA services	Not used
Deposit Ticket Number	Used Payment for VA services	Not used
VCPL User ID	Used to verify Veteran Identity	Not used
Address	Used to verify Veteran Identity	Not used
Financial Information	Used Payment for VA services	Not used
Personal Email	Used Payment for VA services	Not used

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

2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis?
2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

   The VCPL system itself does not perform any kind of analysis or run analysis tasks.

2.3 How is the information in the system secured?
These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

2.3a What measures are in place to protect data in transit and at rest?
   The VCPL have implemented data Encryption at 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?

   SSN is partially masked.

2.3c How is PII/PHI safeguarded in accordance with OMB Memorandum M-06-15?
   All employees and contractors are required to participate in general and role-based privacy training annually, all appropriate administrative, technical and safeguards have been implemented to protect VCPL, data accessed and displayed by the system and users of the system and these controls are reviewed regularly.

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

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:

<u>Principle of Transparency:</u> Is the PIA and SORN, if applicable, clear about the uses of the information?

<u>Principle of Use Limitation:</u> Is the use of information contained in the system relevant to the mission of the project?
This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

2.4a How is access to the PII determined?

VCPL has restricted role-based users helping to ensure that all users do not have open access to the system and have restricted access to the information needed to perform their job function applying the principle of least privilege.

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

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

2.4c Does access require manager approval?

Yes

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

No

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

The SORN 114VA10 The Revenue Program-Billing and Collection Records-VA defines the information collected from Veterans, use of the information, and how the information is accessed and stored. The VCPL application team has implemented the required security controls based on the tailoring guidance of NIST Special Publication 800-53 Rev 4 and VA directives or handbooks.

VA Records Management Policy and VA National Rules of Behavior in Talent Management System govern how Veterans' information is used, stored, and protected. Conditions must be met to be an authorized user of VCPL with specific access privileges. Completed access forms are required when creating accounts and granting appropriate access. Management approval is needed to establish accounts which helps to prevent the use of shared accounts on the VCPL system. System Administrators also manage all VCPL accounts once a completed access form is in place and an appropriate a Service Now ticket is submitted.

Section 3. Retention of Information

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

*Identify and list all information collected from question 1.1 that is **retained** by the system. This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal*

> **Name**
> **Social Security Number**
> **Personal Mailing Address**
> **Financial Account Information**
> **Credit Card Number**
> **Personal Email**
> **Deposit Ticket Number**
> **VCPL User ID**

3.2 How long is information retained?

*In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. **The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.** If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.*

Retention period is six (6) years in accordance with Record Control Schedule (RCS) 10-1, Chapter 4, Financial Records and Reporting Records https://www.va.gov/vhapublications/rcs10/rcs10-1.pd

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)?

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner. Please work with the system Privacy Officer and VA Records Officer to answer these questions.
This question is related to privacy control DM-2, Data Retention and Disposal.

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

Records Control Schedule (RCS) 10-1 Chapter 4 Item 4000.1 a & b approved by NARA
https://www.va.gov/vhapublications/rcs10/rcs10-1.pd

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

Records Control Schedule (RCS) 10-1 Chapter 4 Item 4000.1 a & b approved by NARA. Disposition authority (GRS 1.1, Item 010) (DAA–GRS–2016–0001–0002)
https://www.va.gov/vhapublications/rcs10/rcs10-1.pd

3.4 What are the procedures for the elimination or transfer of SPI?

Explain how records are destroyed, eliminated or transferred to NARA at the end of their mandatory retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc.? This question is related to privacy control DM-2, Data Retention and Disposal.

When the records are authorized for destruction (or upon system decommission), the process will be carried out in accordance with VA 6500.1 HB Electronic Media Sanitization. Disposition of Printed Data: Forms and other types of printed output produced by any computer systems and related peripherals will be evaluated by the responsible staff member for data sensitivity. Printed output containing sensitive data will be stored in locked cabinets or desks and disposed of properly (when the approved records schedule permits destruction) by shredding or similar VA approved methods in accordance with VA Directive 6371 https://www.va.gov/vapubs/search_action.cfm?dType=1**. Program listings and documentation relating to the use of or access to a computer system require special handling if the listings or documentation provide information about a system which processes sensitive data. VA personnel are responsible for retrieving/removing all printed outputs they request from printers.**

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

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

VCPL does not use actual data for research, testing or training.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains

information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

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

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

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

Follow the format below:

Privacy Risk:
There is a risk the information maintained by VCPL could be retained for longer than 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, VCPL adheres to the NARA General Records Schedule. When the retention date is reached for a record, the individual's information is carefully disposed of by the determined method as described in General Records Scheduled.

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?

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*
Office of Information and Technology Consolidated Copayment Processing Center (CCPC) System	To identify exception or excluded items To transmit file to the VAMCs	Account number, Full SSN, Name and address	Electronic transfer/Secure File Transfer.
Data Management Center (DMC)	To transfer files from the mainframe to the VCPL server	Account number, credit card number/check info an SSN	Electronic transfer/SFTP
Office of Information and Technology Data Management Interface (DMI)	To transmit file to the VAMCs	Account number, check info, credit card number	Electronic transfer/SFTP
Office of Management Financial Management System (FMS)	To record unidentified items to FMS)	No SPI: deposit ticket number and dollar amount for unidentified payments.	Electronic transfer/SFTP

4.2 **PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure**

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

Follow the format below:

Privacy Risk:

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:
The principle of need-to-know is strictly adhered to by the VCPL personnel. Only personnel with a clear business purpose are allowed access to the system and the information.

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.

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*	*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*	*List the method of transmission and the measures in place to secure data*

	specified program office or IT system		*permit external sharing (can be more than one)*	
U.S. Bank Accounts Receivable LBX Bank	U.S Bank (LBX Bank)- Payment	Account Number (includes first 5 characters of the last name), Financial account(partial) Integration Control number	National ISA/MOU	SFTP
Collections Information Repository CIR/Pay.gov Treasury	Treasury	Account Number (includes first 5 characters of the last name), Financial account(partial) Integration Control number	National ISA/MOU	SFTP

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.
Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.
This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

Privacy Risk:
The privacy risk associated with maintaining SPI is that sharing data outside of the Department of Veterans 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:
The principle of need-to-know is strictly adhered to by VCPL personnel. Only personnel with a clear business purpose are allowed access to the system and the information contained within the system. There is also an agreement in place in the form of an ISA/MOU

Section 6. Notice

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

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

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

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

The Department of Veterans Affairs provides notice prior to the collection of PII. This notice is provided in 2 ways as listed below in section 6.1b:

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

The System of Record Notice (SORN) 114VA10 - The Revenue Program Billings and Collection Records-VA https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01541.pdf
and 79VA10 - Veterans Health Information Systems and Technology Architecture (VistA) Records-VA https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf.

Please provide response here
6.1c Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.

This Privacy Impact Assessment (PIA) also serves as notice of the VCPL 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 VCPL, 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.

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 uses of the information would be handled by the source systems that collect the information from the Veteran.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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

Principle of Transparency: Has sufficient notice been provided to the individual?

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

Privacy Risk:
There is a risk that an individual may not know their information is being collected, maintained, processed, or disseminated by VCPL.

Mitigation:
Mitigation is provided by making the System of Record Notices (SORN) 114VA10 The Revenue Program-Billing and Collection Records-VA https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01541.pdf 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?

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

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

7.1b If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR)?

7.1c If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information?

Individuals seeking information regarding access to and contesting of records in this system may write, call or visit the VA facility location where they were treated.

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.

There are no provisions for correcting inaccurate or erroneous information in VCPL. The information in VCPL is obtained electronically from other VA systems. Requests to correct information should be directed to the VA facility where the individual receives care.

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

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Individuals seeking information regarding access to and contesting of records in this system may write, call or visit the VA facility location where they were treated.

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and

*Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. **Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

The information in VCPL is obtained electronically from other VA systems. Requests for copies of records or to correct information should be directed to the VA facility where the individual receives care.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

*Discuss what risks there currently are related to the Department's access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those risks. **For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals involved might change their behavior.** (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).*

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

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

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

Follow the format below:

Privacy Risk:
There is a risk that erroneous information is placed into VCPL via the feed from other VA systems.

Mitigation:
The information in VCPL is obtained via other VA systems. If there is erroneous or inaccurate information, it should be addressed in the other systems. Any validation performed would 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?

These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.

8.1a Describe the process by which an individual receives access to the system?

Users must submit an Electronic Permission Access System (ePAS) request that requires manager approval.

8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

There are no users from other agencies.

8.1c Describe the different roles in general terms that have been created to provide access to the system? For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

Access to VCPL is granted by submitting a VA Access Form with appropriate functional task codes to Program staff, who grant system access.

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.

Contractors can be granted access to VCPL if their VA manager and local Information Security Officer approve. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of behavior training via TMS. All contractors are cleared using the VA background investigation process and must obtain the appropriate background investigation for their role. Contractors with systems administrative access are required to complete additional role-based training prior to gaining system administrator access and yes contractors who access the system are require to sign NDA.

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.

Personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training which all personnel must complete via the VA's Talent Management System (TMS). After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the privacy and security awareness training. Acceptance is.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 04/08/2024
3. *The Authorization Status:* Authorization to Operate (ATO)
4. *The Authorization Date:* 08/18/2023
5. *The Authorization Termination Date:* 08/17/2024
6. *The Risk Review Completion Date:* 08/08/2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* **Moderate**

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

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

Section 9 – Technology Usage

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

9.1 Does the system use cloud technology? If so, what cloud model is being utilized?
If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.
Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1. (Refer to question 3.3.1 of the PTA)

VAEC AWS- Platform as a Service (PaaS)

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

   N/A

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.

   N/A

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.

   N/A

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

   N/A

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

_____

Privacy Officer, Akeel Omari

_____

Information System Security Officer, Amine Messaoudi

_____

Information System Owner, Jeffrey Rabinowitz

APPENDIX A-6.1

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

HELPFUL LINKS:

General Records Schedule
https://www.archives.gov/records-mgmt/grs.html

National Archives (Federal Records Management):
https://www.archives.gov/records-mgmt/grs

VA Publications:
https://www.va.gov/vapubs/

VA Privacy Service Privacy Hub:
https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):
VHA Notice of Privacy Practices
VHA Handbook 1605.04: Notice of Privacy Practices