Privacy Impact Assessment for the VA IT System called:

WellHive Advanced Medical Cost Management System – enterprise

VHA Office of Community Care (OCC), Chief Health Informatics Officer

Date PIA submitted for review:

January 25, 2021

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Julie Drake	Julie.drake@va.gov	303-331-7823
Information System Security Officer (ISSO)	Richard Alomar-Loubriel	Richard.alomarloubriel@va.gov	787-641-7582 ext. 11411
Information System Owner	Terrill Harrison	Terrill.Harrison@va.gov	202-461-5468

Abstract

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

The Office of Community Care (OCC), Business Operations & Administration (BOA) Chief Health Informatics Office (CHIO) supports management and delivery of care provided to Veterans in the community. As part of that effort, it provides stewardship of financial resources and financial information. The WellHive Advanced Medical Cost Management System – enterprise (AMCMS - e) is part of a managed service contract, with Liberty IT as prime contractor, and WellHive as a subcontractor. The contract is for a commercial off the shelf Software as Service (SaaS) product that resides within the Amazon Web Service Government Cloud and is used by the Office of Community Care (OCC), Veterans Integrated Service Network (VISNs) and medical centers to integrate community care financial costs for the purpose of monitoring, forecasting and controlling Community Care's medical services costs, as well as to increase accuracy, visibility, and volume of insurance coverages available to the VA for billing.

Overview

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

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *If your system is a regional GSS, VistA, or LAN, include a list of the hospitals/medical centers, or other regional offices that fall under your system. Additionally, what region is the system under?*
- *A general description of the information in the IT system.*
- *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?*
- *Does the system use cloud technology? If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517.*

- *Does a contract with Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII?*
- *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 is the magnitude of harm if privacy related data is disclosed, intentionally or unintentionally? Would the reputation of the CSP or its customers (VA) be affected?*

The Software as a Service (SaaS) WellHive AMCMS - e and the name of the program office, Office of Community Care, Chief Health Informatics Office (CHIO) that owns the SaaS. There are two primary purposes for this SaaS.

The first is to improve the management of costs associated with care provided in the community by providing an electronic mechanism to assist in the data analytics necessary to monitor, forecast and control Community Care medical services costs. The typical affected individual is a Veteran who is eligible to receive care from a community provider when Veterans Affairs (VA) cannot provide the care needed. This care is provided on behalf of and paid for by VA. The expected number of individuals whose information is stored is 2.1 million.

The second purpose is to increase accuracy, visibility, and volume OHI (other health insurance) coverages available to the VA for billing 3rd party insurance carriers. The VA has the authority and the legal mandate to bill 3rd party insurance carriers for any healthcare provided that is not associated with a Veteran's service-connected disabilities. The typical affected individual is a Veteran who receives care at a VA facility. The expected number of individuals whose information is stored is roughly the entire VA patient population, i.e. 9 million.

Most of the AMCMS system is hosted within the VA-owned tenant in WellHive's FedRAMP Moderated authorized cloud service and is managed and maintained by WellHive. Additionally, there are a set of components to the AMCMS solution that do live within the VA, specifically, Corporate Data Warehouse (CDW) data, Comma Separated Value (CSV) file extraction, and Lighthouse API Platform, but are not managed or maintained by WellHive. Historical patient data, CC (Community Care) referrals and claims data, and 3rd party insurance and billing data are received from VA CDW via SFTP, for two purposes: (1) for analyzing and reporting on predicted referral costs, incoming claims allocation to those predicted costs, and correlation with budget; (2) for assembling a National Insurance File by retrieving updated and new insurance information from 3rd party insurance carriers. Transactional appointment data, 3rd party insurance data, and updated patient data are communicated in both directions between the VA and WellHive via VA Lighthouse APIs, for the purpose of maintain the National Insurance File by continually retrieving updated and new insurance information from 3rd party insurance carriers, and for writing that information back to the VA to make it available for billing.

This system is Software as a Service (SaaS) and is not operated in more than one site. Legal authority to operate the system can be found in U.S. Code Title 38 Veterans' Benefits, Part V, Chapter 73, Subchapter 11, Section 7330C. "Quadrennial Veterans Health Administration Review" (b)(C)(3) which authorized the Department of Veterans Affairs to developing a multi-year budget process that is capable of forecasting future year budget requirements and projecting the cost of delivering health care services under a high-performing integrated health care network. The legal authorities that defined the collection of information include Privacy Act of 1974, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. Systems of Records Notices applicable to this system are 23VA10NB3, Non-VA Care (Fee) Records-VA (FR: Thursday, July 30, 2015); 54VA10NB3, ''Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files—VA'' (FR: Tuesday March 3. 2015); 55VA10NB, Customer Relationship Management System (CRMS). CFR › Title 38 › Chapter I › Part 3 › Subpart A › Section 3.216 - Mandatory disclosure of social security numbers. CFR › Title 38 › Chapter I › Part 1 › 38 CFR 1.575 - Social security numbers in veterans' benefits matters. U.S. Code › Title 38 › Part IV › Chapter 51 › Subchapter I › § 5101 38 U.S. Code § 5101 - Claims and forms CFR › Title 32 › Subtitle A › Chapter VII › Subchapter A › Part 806b › Subpart C › Section 806b.12 32 CFR 806b.12 - Requesting the Social Security Number Health Insurance Portability and Accountability Act of 1996 (HIPAA) Rules. The completion of this PIA will not result in circumstances that require changes to business processes. The completion of this PIA will not result in technology changes. A System of Records Notice (SORN) will not need to be modified. Yes, the system uses cloud technology. AMCMS is obtaining an Agency Authority to Operate (ATO) from the VA, following the Federal Risk and Authorization Management Program (FedRAMP) documentation and VA requirements. The AMCMS system is categorized as a Moderate-risk system that uses FedRAMP-accredited cloud technology that supports Federal Information Processing Standards (FIPS) 140-2 encryption requirements. Yes, the contract establishes VA has ownership rights over data including PII. The contractor is ultimately accountable for the security and privacy of data held by a cloud provider on their behalf. AMCMS connects and stores Protected Health Information (PHI)/Personally Identifiable Information (PII) data. Therefore, there is a risk that, if data were accesses by an unauthorized individual or otherwise breached, or misused, serious personal/professional or financial harm may result for the individuals affected. The compromise of this information would constitute a breach of confidence with the Veterans served by the VA.

Section 1. Characterization of the Information

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

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

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

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

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

☒ Name

☒ Social Security Number

☒ Date of Birth
□ Mother's Maiden Name

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

Gender
Current Medical Records

PII Mapping of Components

AMCMS consists of 2 (two) key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by AMCMS and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

PII Mapped to Components

Components of the information system (servers) 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
VHA Corporate Data Warehouse (CDW) VHACDWDWHSQL52 CC_AMCMS CC_AMCMS_ETL	Yes	Yes	Name, Social Security Number, Date of Birth, Personal Mailing Address, Personal Phone, Personal Email Address, Health Insurance Beneficiary Numbers, Race/Ethnicity, Tax Identification Number, Previous Medical Records	Cost Management, forecasting activities, and insurance capture	FIPS 2.0 Encryption
Commercial Amazon Web Service Gov Cloud (AWS) WellHive Cloud Service instance	Yes	Yes	Name, Social Security Number, Date of Birth, Personal Mailing Address, Personal Phone, Personal Email Address,	For analyzing CC (Community Care) referrals,	Federal Risk and Authorization Management Program

			Health Insurance Beneficiary Numbers, Race/Ethnicity, Tax Identification Number, Previous Medical Records	claims, predicted costs, and budgets; and for improving accuracy, visibility, and volume of OHI insurance coverages available to the VA for billing 3rd party insurance carriers.	(FedRAMP) Compliant (encryption), Two factor authentication; Security Manager configured to limit data access according to role and organizational assignments. Access is limited to only those components required in the performance of work.

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.

The VA aggregates historical data from CDW(Corporate Data Warehouse) for the purpose of analysis, therefore making CDW an appropriate source of the historical data needed by AMCMS.

The VA Lighthouse API Platform provides interfaces and integrations for external services to interact with internal services, therefore making it an appropriate source for transactional data needed by AMCMS.

AMCMS - e provides both analytics and insurance eligibility capabilities, including capability to retrieve updated and new insurance data from 3rd party insurance carriers.

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.

Historical data is delivered by the VA from CDW to WellHive via SFTP put commands executed on a CDW host. Analysis data is retrieved back by the VA from WellHive to the CDW host via SFTP pull commands. Transactional data is retrieved by WellHive from VA Lighthouse API Platform via HTTPS requests. Transactional data is delivered by WellHive to the VA Lighthouse API Platform via HTTPS requests.

1.4 What is the purpose of the information being collected, used, disseminated, created, or maintained?

Include a statement of why the particular SPI is collected, maintained, used, or disseminated in the system is necessary to the program's or agency's mission. Merely stating the general purpose of the system without explaining why this particular type of information should be collected and stored is not an adequate response to this question.

If the system collects, uses, disseminates, or maintains publicly available or commercial data, include a discussion of why commercial data is relevant and necessary to the system's purpose.
This question is related to privacy control AP-2, Purpose Specification.

Historical patient data, CC (Community Care) referrals and claims data, and 3rd party insurance and billing data are delivered to WellHive from VA CDW via SFTP, for two purposes: (1) for analyzing and reporting on predicted referral costs, incoming claims allocation to those predicted costs, and correlation with budget; (2) for assembling a National Insurance File by retrieving updated and new insurance information from 3rd party insurance carriers. Transactional appointment data, 3rd party insurance data, and updated patient data are communicated in both directions between the VA and WellHive via VA Lighthouse APIs, for the purpose of maintain the National Insurance File by continually retrieving updated and new insurance information from 3rd party insurance carriers, and for writing that information back to the VA to make it available for billing.

1.5 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.

For all use cases, integrity of data in transit from the VA systems to WellHive is protected by the usage of protocols (SFTP and HTTPS) which include checksum mechanisms in AMCMS – e that would cause corrupted data to be retransmitted automatically.

For AMCMS analysis and reporting use cases, accuracy of data prepared for analytics is performed only after full refreshes, which are tentatively planned to occur on a monthly cadence. This is performed manually through comparisons of high-level aggregate values like row counts to ensure the output of ETL pipeline matches expectations based on the inputs of data from VA systems.

For National Insurance File use cases, accuracy of insurance plan data discovered by WellHive on behalf of the VA is performed with a human-assisted, semi-automated process, with configurable tolerances for automated decisions. When WellHive discovers an insurance plan that might be associated with a given patient, an automated process will calculate a "confidence score" that represents the level of certainty that the insurance plan really does match that patient. If that score satisfies the VA-configured tolerance, no further effort is needed, and the insurance plan is associated with the patient within the National Insurance File. If the score does not satisfy the configured tolerance, an insurance verification task is created within WellHive and assigned to (VA-configured) appropriate VA personnel. It then becomes the responsibility of the assignee to make the final decision on accuracy and determine if the insurance plan should be associated with the patient.

1.6 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

Privacy Act of 1974

> Privacy Act of 1974, 5 U.S.C. § 552a, establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies.

Freedom of Information Act (FOIA) 5 USC 552
VA Directive 6500 Managing Information Security Risk: VA Information Security Program
The legal authorities that defined the collection of information include:
U.S. Code Title 38 Veterans' Benefits, Part V, Chapter 73, Subchapter 11, Section 7330C.
"Quadrennial Veterans Health Administration Review" (b)(C)(3)

Systems of Records Notices applicable to this system are:

23VA10NB3, Non-VA Care (Fee) Records-VA (FR: Thursday, July 30, 2015);

54VA10NB3, ‘‘Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files—VA’’ (FR: Tuesday March 3, 2015);

55VA10NB, Customer Relationship Management System (CRMS).

CFR › Title 38 › Chapter I › Part 3 › Subpart A › Section 3.216 - Mandatory disclosure of social security numbers.

CFR › Title 38 › Chapter I › Part 1 › 38 CFR 1.575 - Social security numbers in veterans' benefits matters.

U.S. Code › Title 38 › Part IV › Chapter 51 › Subchapter I › § 5101 38 U.S.
Code § 5101 - Claims and forms CFR › Title 32 › Subtitle A › Chapter VII › Subchapter A › Part 806b › Subpart C › Section 806b.12 32 CFR 806b.12 - Requesting the Social Security Number Health Insurance Portability and Accountability Act of 1996 (HIPAA) Rules

1.7 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: The VA-owned tenant in WellHive collects personally identifiable information from VA systems CDW and VA Lighthouse API Platform. Risk that may occur is that the data received from CDW and Lighthouse are not accurate.

Mitigation: The SFTP protocol used to deliver data from CDW to WellHive protects against accidental data changes during transfer. The encryption mechanisms ensure that the data will be unencryptable upon receipt if it is corrupted during transit. Additionally, if the extract process on the CDW side mis-formats the data files, WellHive will reject the files. If the data in CDW itself is identified as inaccurate, then the data in CDW is corrected, the extract and transfer process is re-run, and WellHive overwrites the inaccurate data upon receiving the new data files. Data may be identified in CDW as inaccurate by users viewing and using the data.

Section 2. Uses of the Information

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

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

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

- Name
  - Used for individual Veteran community care claim identification and for 3rd party insurance coverage identification. Also, used to identify clinical staff providing care to Veterans in the community for the purpose of forecasting, monitoring and trending OCC's medical services and costs.
- Social Security Number
  - Used for individual Veteran community care claim identification and for 3rd party insurance coverage identification
- Date of Birth
  - Used for individual Veteran community care claim identification and for 3rd party insurance coverage identification
- Personal Mailing Address
  - Used to identify location of Veteran in relationship to location of community care and for 3rd party insurance coverage identification
- Personal Phone
  - Used by VA Medical Support Assistants to contact the veteran for requesting updated insurance coverage information.
- Personal Email Address
  - Used by VA Medical Support Assistants to contact the veteran for requesting updated insurance coverage information.
- Health Insurance Beneficiary Numbers
  - Used to look up latest coverage eligibility information for a Veteran.
- Race/Ethnicity
  - Used for identifying 3rd party insurance coverage for individual Veteran
- Tax Identification Number (TIN)(might be SSN for individual providers)
  - Used to identify clinical staff providing care to Veterans in the community for the purpose of forecasting, monitoring and trending OCC's medical services and cost. The TIN, like other PII and the SSN, is only accessible by users authorized to view PII.
- Previous Medical Records

- Diagnosis Code: Used to identify reason for the patient outpatient encounter or admission for the purpose of forecasting, monitoring and trending OCC's medical services and costs
- Common Medical Procedure Code: Used to identify and report surgical, medical, or diagnostic procedures and services provided to patients for the purpose of forecasting, monitoring and trending OCC's medical services and costs
- Admission & Discharge Dates: Used to identify length of hospitalization stay for the purpose of forecasting, monitoring and trending OCC's medical services and costs
- Outpatient Visit Date: Used to identify date medical care provided for the purpose of forecasting, monitoring and trending OCC's medical services and costs

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 system will produce information to determine VA benchmarking for VA standard episodes of care, calculate to determine balances of expected payment, identify over/under expected payment amounts, model expected payment for community care referrals and claims, trend referral patterns, outliers and anomalies. The system will also retrieve updated and new 3rd party insurance coverage data for each patient, incorporate into the patient's claim record and make that data available to the VA for billing 3rd party insurance carriers.

2.3 <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. <u>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.</u>

Consider the following Fair Information Practice Principles (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.

Add answer here:
Access to the VA-owned tenant in WellHive is granted to VA employees or contractors after the supervisor/manager or contracting officer's technical representative (COR) determines access is required based on user role. For VA employees or contractors, the supervisor/manager or COR will submit a Leaf request requiring the requestor to certify need for access and confirming the user has completed information security awareness and privacy training. Once an access request is approved, AMCMS application administrators' provision of access. Criteria, procedures, controls and responsibilities regarding determining access are documented in OCC policies and procedures. Criteria, procedures, controls and responsibility for provision access are documented by AMCMS.

Access to the VA-owned tenant in WellHive is monitored, tracked and recorded through audit logging at system, network, and application level. Explicit access for business purpose to PII is tracked and monitored through access control logs and remote access session approvals. All access (including application users and actions such as view, modify, add, or delete) to the VA-owned tenant in WellHive including internal components such as databases, are securely recorded in audit logs and forwarded to a centralized Security Information Event Manager (SIEM) tool for near real-time 24/7/365 security operational monitoring. All information forwarded to the SIEM tool is included in system backups for accountability and after-action review. There are regular reviews of user access to evaluate whether users have accessed the system within the past 35 days. If no access with 35 days user access is disabled.

WellHive is responsible for assuring safeguards for PII by enabling encryption at rest and in transit and utilizing rotation of application encryption keys and session keys well within best practice lifetimes. WellHive protects data utilizing access controls and role-based access. Personnel roles are reviewed monthly per continuous monitoring best practices.

The VA AMCMS application administrators make a risk-based decision on who to invite to the VA-owned tenant in WellHive and subsequently those who can see the PII required for the system.

All WellHive internal protections are maintained and implemented by WellHive System Administrators and Engineers and assured by the WellHive Chief Privacy Officer identified within the FedRAMP Package.

Section 3. Retention of Information

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

3.1 What information is retained?

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

The VA-owned tenant in WellHive will retain the following data:

- Name
- Social Security Number (SSN)
- Date of Birth
- Personal Mailing Address
- Personal Phone
- Personal Email Address
- Health Insurance Beneficiary Numbers
- Race/Ethnicity
- Tax Identification Number (TIN)(might be SSN for individual providers)
- Previous Medical Records

3.2 How long is information retained?

In some cases VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods.

The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.
This question is related to privacy control DM-2, Data Retention and Disposal.

Retained per the RCS and the requirements of the contract.

AMCMS software maintains compliance with Records Control Schedule (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 6 years after final payment or cancellation, but longer retention is authorized if required for business use. General Record Schedule (GRS) 1.1, Item 010) (Disposition Authority (AA)-GRS-2016-0001-0002)
b. All Other Copies Temporary: destroy or delete when 6 years old, but longer retention is authorized if required for business use. (GRS 1.1 item 013) (DAA-GRS-2016-0001-0002)

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.

VHA Records Control Schedule: https://vaww.va.gov/vhapublications/rcs10/rcs10-1.pdf

AMCMS software maintains compliance with Records Control Schedule (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:

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

Records are kept for the term of the contract. The contract incorporates by clause Federal Acquisition Regulations *(FAR) 52.227-14 Rights in Data – General and 52.227.16 Additional Data Requirements. There is also a Business Association Agreement (BAA) in place.-The Government is the owner of the records generated under this contract.* At termination of the contract information will be destroyed. WellHive will purge all VA-owned data. WellHive adheres to FedRAMP's requirements for retention and disposal, which are NIST MP-6 and DM-2(c).

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

Yes, the system does use techniques to minimize the risk of privacy of using PII for research, testing or training. Training for AMCMS is completed in a test environment with de-identified and de-sensitized claim information as possible.

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:

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: Unnecessary retention of PII/SPI: There is risk that the information maintained by AMCMS 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 or exploited for reasons other than what is described in the privacy documentation associated with the information.

Mitigation: To mitigate the risk posed by information retention, AMCMS adheres to the VA Records Control Schedule (RSC) schedules for the financial management data it maintains. At the end of the period of contract performance the COR will coordinate with AMCMS for destruction of the records.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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 data element types such as PII/PHI that are shared/received with the Program Office or IT system***	***Describe the method of transmittal***
VA Corporate Data Center Operations, Austin Information Technology Center (AITC)	Fulfill forecasting, monitoring and trending of OCC's medical services and costs	Name, Social Security Number, Date of Birth, Personal Mailing Address, Personal Phone, Personal Email Address, Health Insurance Beneficiary Numbers, Race/Ethnicity, Tax Identification Number, Previous Medical Records	Secure File Transfer Protocol (SFTP) for transfer from CDW to WellHive. HTTPS for transfer from WellHive to VA users' browsers (when viewing analysis dashboards and reports).
VA Lighthouse API Platform	Insurance discovery, verification, and capture	Name, Social Security Number, Date of Birth, Personal Mailing Address, Personal Phone, Personal Email Address, Health Insurance Beneficiary Numbers, Race/Ethnicity, Tax Identification Number, Previous Medical Records	Application Programming Interface (API)
VHA VistA	Insurance discovery, verification, and capture	Name, Social Security Number, Date of Birth, Personal Mailing Address, Personal Phone, Personal Email	VA Lighthouse Application Programming Interface (API)

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 data element types such as PII/PHI that are shared/received with the Program Office or IT system*	*Describe the method of transmittal*
		Address, Health Insurance Beneficiary Numbers, Race/Ethnicity, Tax Identification Number, Previous Medical Records	

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks.
This question is related to privacy control UL-1, Internal Use.

Follow the format below:
Privacy Risk: There is a risk that an access by an unauthorized person could result in a serious personal, professional or financial harm to the individual to whom the information pertains. This is not an internal VA system.

Mitigation: Mitigations include the system being encrypted at rest and in transit, with encryption of the databases, backups encrypted, and the implementation of VA SSO, integrated, or other acceptable authentication methods with multifactor authentication. Access to PII is limited to only those applications and users deemed necessary for staff to perform their job for business purposes, as determined by their management team and their job description. User access is provided following receipt of request from appropriate individuals by defined processes and workflows. Business Associate Agreements are utilized where appropriate and necessary. Explicit access controls via role based access controls and extensive training on PHI/PII handling, use, misuse, and requirements are assigned to individuals who have business purposes to access the system. Well defined incident response and breach notification procedures are centrally published and accessible by all members of AMCMS as necessary.

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: This question is #7 in the Privacy Threshold Analysis.

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 data element types such as PII/PHI that are shared/received 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***
Change Healthcare (CHC)	Patient demographics and insurance subscriber IDs are shared by WellHive to Change Healthcare so that Change Healthcare can respond with the updated insurance	Patient's First Name, Middle Name, Last Name, Date of Birth, Address, Social Security Number, Gender, Insurance Subscriber ID,	Business Associate Agreement (BAA)	There are two methods of transmission between WellHive and CHC. HTTPS requests are used for requesting and retrieving the latest data for known insurance coverages. SFTP is used for requesting and retrieving new, previously unknown insurance coverages. For both, the patient's

	coverage information as well as new, previously unknown insurance coverage information.			data is delivered in the request to CHC. For both connections, WellHive uses the BoringCrypto crypto module, which is FIPS 140-2 validated. BoringCrypto's FIPS 140-2 certificate number is 2964. WellHive configures and runs BoringCrypto in compliance with the Security Policy attached to its FIPS 140-2 validation/certificate. This means the WellHive side of the connections to Change Healthcare services will always negotiate FIPS compliant algorithms and cipher suites, and will terminate connections before any sensitive data is transmitted if a Change Healthcare service fails to offer any compliant protocols or cipher suites during the handshake.

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

WellHive implements the privacy control requirements specified by NIST SP 800-53, Appendix J. Change Healthcare maintains a HITRUST CSF certification, ensuring their compliance to the HIPAA Security and Privacy rules.

5.2 <u>PRIVACY IMPACT ASSESSMENT: External sharing and disclosure</u>

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

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a

Memorandum Of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.
Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.
This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:
Privacy Risk: There is a risk to the data when it is in transit from WellHive to CHC, that an unauthorized person could access the data.

Mitigation: To mitigate this risk WellHive encrypts and scans the connections to CHC and data transferred across those connections. This means the WellHive side of the connections to Change Healthcare services will always negotiate FIPS compliant algorithms and cipher suites, and will terminate connections before any sensitive data is transmitted if a Change Healthcare service fails to offer any compliant protocols or cipher suites during the handshake. It should also be noted that as a medical insurance clearinghouse, Change Healthcare (CHC) already has the identified patients' demographics data in conducting it's business independent of the VA. Therefore, by sharing this data to CHC there is no increased risk to the data once it resides within CHC.

Section 6. Notice

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

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

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

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

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

This is received by CDW prior to ingestion. Notice is provided by the Department of Veterans Affairs provides notice of information collection in several additional ways. The initial method of notification is in writing via the Privacy Act statement on forms and applications completed by the Veteran. Notice is provided to Veterans at the time of enrollment on VA Form 10-10EZ dated April 2017: A copy of VA Form 10-10EZ can be found online https://www.va.gov/vaforms/form_detail.asp?FormNo=10EZ The VA policy is not to disclose any personal information to third parties outside VA without their consent, except to facilitate the transaction, to act on caller's behalf at their request, or as authorized by law. Any questions or concerns regarding VA privacy policy can be made by contacting via email at Contact VA Privacy Service, or by mailing questions or concerns at Department of Veterans Affairs, Privacy Service, 810 Vermont Avenue, N.W. (005R1A) Washington, DC 20420. This Privacy Impact Assessment will be available online as required by the E-Government Act of 2002, Pub.L. 107–347§208(b)(1)(B)(iii). More detail on privacy policy that OCC FM is required to follow can be found at VA Privacy Policy.

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

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

VHA Handbook 1605.1 'Privacy and Release Information' lists the rights of beneficiaries to request the VHA to restrict the use and/or disclosures of individually identifiable health information to carry out treatment, payment, or health care operations. Beneficiaries have the right to refuse to disclose their SSNs to the VHA. The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VHA a SSN (please refer to the 38 Code of Federal Regulations CFR 1.575(a)).

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

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

VHA Handbook 1605.1 'Privacy and Release Information' lists the rights of beneficiaries to request the VHA to restrict the use and/or disclosures of individually identifiable health information to carry out treatment, payment, or health care operations. Beneficiaries have the right to refuse to disclose their SSNs to the VHA. The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VHA a SSN (please refer to the 38 Code of Federal Regulations CFR 1.575(a)).

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:

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 risk that individuals who provide information to VA will not know how their information is being shared and with a contractor for health care operations.

Mitigation: This PIA serves to notify individuals of the AMCMS software and includes information about the sharing of information from VA sources.

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.
There are no procedures for individuals to gain access to their information on AMCMS. Information on AMCSM comes from VA itself. Individuals should seek their information through the usual VA channels. VHA Handbook 1605.1: Privacy and Release Information states the rights of Beneficiaries to request access to review their records. VA Form 10-5345a, Individual's Request for a Copy of Their Own Health Information, may be used as the written request requirement. All requests to review must be received by direct mail, fax, in person, or by mail referral from another agency or VA office. All requests for access to data must be delivered to, and reviewed by, the System Manager for the concerned VHA system of records, the facility Privacy Officer, or their designee. Each request

must be date stamped and reviewed to determine whether the request for access should be granted. Individuals can submit a request for information through the Privacy Office or the Release of information Office at the VA Medical Center where they are receiving 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.

If a correction is requested by a Veteran, then such a request must be in writing and it must adequately describe the specific information that 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 or insurance company that maintains the record or to the VBA. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned system of records, and the facility Privacy Officer, or designee, and needs to be date stamped; and filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579. VHA Handbook 1605.1, Appendix D: Privacy and Release Information, Section 5 lists the rights of Beneficiaries to request that the VHA restrict the uses and/or disclosures of individually identifiable health information to carry out treatment, payment, or health care operations.

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.

VHA Handbook 1605.1, Appendix D: Privacy and Release Information, Section 8 states the rights of Beneficiaries to amend their records by submitting VA Form 10-5345a, Individual's Request for a Copy of Their Own Health Information that may be used as the written request requirement. This includes designated record sets, as provided in 38 CFR 1.579 and 45 CFR 164.526. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the facility Privacy Officer, or designee, to be date stamped; and be filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579.

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

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

If the Beneficiary discovers that incorrect information was provided during intake, they simply follow the same contact procedures in section 7-3 (also re-stated below), and state that the documentation they are now providing supersedes those previously provided. If a Beneficiary discovers that incorrect information was provided during the intake process, the request must be in writing and adequately describe the specific information the Beneficiary 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 be filed appropriately. In reviewing requests to amend or correct records, the System Manager must be guided by the criteria set forth in VA regulation 38 CFR 1.579.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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 small risk that the information provided to AMCMS is inaccurate and decisions are made (outside of AMCMS) for correction. There is a risk that incorrect information is accidentally recorded in a Beneficiary's record. A Beneficiary may want to review the content of their record to check for data accuracy. The magnitude of harm associated with this risk to the VA would be low.

<u>Mitigation:</u> A Beneficiary who wishes to determine whether a record is being maintained in this system under his or her name or other personal identifier, or who wants to review the contents of such a record, should submit a written request or apply in person to the VA health care facility (or directly to the VHA) where care was rendered.

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 supervisor/manager or COR documents and monitors individual information system security training activities, including basic security awareness training and specific information system security training. This documentation and monitoring is performed using the Talent Management System (TMS). Access to the software is granted to VA employees and contractors for the application after the supervisor/COR authorizes this access once requirements have been met. Only the authorized software administrators will have the ability to modify the software. No users from other agencies have access to the system. Only certain users (implementers and administrators) will have direct access to the software either maintaining or additional development within the authorized boundaries. There are regular reviews of user access to evaluate whether users are active in the environment. If a user is not active, the account will be terminated. All application users must have at least a Public-level clearance plus a Personal Identification Verification (PIV) card for multifactor authentication.

Contractor and VA employees are required to take Privacy, HIPAA, Rules of Behavior, and information security training annually. In addition, this PIA, which will be available online as required by the eGovernment Act of 2002, Pub.L. 107–347§208(b)(1)(B)(iii), serves to notify Veterans about the collection and storage of personal information.

8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII.

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

VA contractors have access to the software for development and business purposes. Contractors also have access to the software for maintenance activities. The following steps are required before contractors can gain access to the system:

- Contractors must take and pass training on privacy, HIPAA, information security, ethics and role-based training based on support role to the system.
- Contractors must have signed the Non-Disclosure Agreement (NDA) and VA Information Security Rules of Behavior (RoB).

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 who will be accessing the software must read and acknowledge their receipt and acceptance of the VA Information Security Rules of Behavior (RoB) prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training that all personnel must complete via the VA's TMS. After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training. Acceptance obtained through electronic acknowledgment is tracked through the TMS system. All VA employees and contractors must complete annual Privacy and Security training. This training includes, but is not limited to, the following TMS Courses:

- Privacy and Info Security Awareness
- Rules of Behavior
- Privacy and HIPAA Training

Liberty IT Solutions and its subcontractors (WellHive, Federal Advisory Partners, Milliman) have mutual non-disclosure agreements that bind their employees.

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

If Yes, provide:

1. *The date the Authority to Operate (ATO) was granted,*
   a *4/16/2020*
2. *Whether it was a full ATO or ATO with Conditions,*

a Full, 3 year at moderate

3. *The amount of time the ATO was granted for, and*
   a 3 Year
4. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH).*
   a Moderate

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

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

Section 9. 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 Privacy Officers

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

JULIE C. DRAKE 969177 Digitally signed by JULIE C. DRAKE 969177
Date: 2021.02.03 15:12:33 -07'00'

Privacy Officer

Signature of Information Security Systems Officers

The Information Security Systems Officers below attest that the information provided in this Privacy Impact Assessment is true and accurate.

RICHARD ALOMAR-LOUBRIEL 139039

Digitally signed by RICHARD ALOMAR-LOUBRIEL 139039
Date: 2021.02.03 16:43:29 -05'00'

Information Security Systems Officer

Signature of Area Manager

The Area Manager below attests that the information provided in this Privacy Impact Assessment is true and accurate.

Terrill N. Harrison
1079525

Digitally signed by Terrill N. Harrison
1079525
Date: 2021.02.03 16:16:36 -05'00'

System Owner

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).