



Privacy Impact Assessment for the VA IT System called:

**WellHive Scheduling Grid Integration –
Columbia Community Care (CC) Scheduling
Veterans Integrated Service Network (VISN)
7 – Columbia A Medical Center
Veterans Health Administration**

Date PIA submitted for review:

1/28/2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	<i>Selina Bland</i>	<i>Selina.bland@va.gov</i>	<i>(803) 776-4000 x6974</i>
Information System Security Officer	<i>Calvin Dingle</i>	<i>Calvin.dingle@va.gov</i>	<i>(803) 776-4000 x56893</i>

	Name	E-mail	Phone Number
Information System Owner	<i>Fred Tolley</i>	<i>Fred.tolley@va.gov</i>	<i>202-461-9005</i>

Abstract

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

The WellHive Scheduling Grid Integration – Columbia Community Care (CC) Scheduling solution enables Veterans Health Administration (VHA) community care staff to directly schedule into a community care provider’s schedule within the WellHive platform. The WellHive Integrated Outside Network (ION) Platform will provide an appointment management service for the VA’s community care referral process in the form of electronic searching of open slots and booking of appointments. This will help maximize the timeliness of care for community care appointments. Medical Support Assistants (MSAs) in Columbia charged with processing community care referrals will use the WellHive user interface (UI) to search for available providers within Columbia’s Community Care Network (CCN). The search for a suitable provider will be guided by choice of specialty, geographic location, and timeliness of availability.

Overview

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

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *Indicate the ownership or control of the IT system or project.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *A general description of the information in the IT system and the purpose for collecting this information.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.*
- *A citation of the legal authority to operate the IT system.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*

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

The IT system is the WellHive SaaS product and the WellHive tenant licensed by Health Services Program Office, Community Care. The VA refers patients to external Community Care providers for care in some cases, such as when there are no timely appointments at VA facilities near to the patient. This process is difficult and labor intensive, requiring VA schedulers to make many phone calls to find available appointments at external providers. Through WellHive, the VA can connect directly to external providers to retrieve their availability grid, filter to find available slots best for the patient, directly book appointments into available slots, and deliver referral authorizations directly into external providers' EHR and Practice Management systems.

WellHive will collect Patient, referral, and referral authorization information in order to share that information with VA's Community Care providers when booking appointments with those providers. Business processes will change for VA schedulers. For each Community Care referral, instead of making many phone calls out to providers to find available appointments, they will search availability for multiple providers on one screen in WellHive, select the most appropriate appointment slot, enter required patient and referral information, and book the appointment with a click. Additionally, patient and referral data is already delivered to WellHive from CDW once per month for the AMCMS program, and this data will be used as available to reduce the amount of data entry performed by VA schedulers.

While the system will be available to users at multiple VA sites, the system itself is not hosted at those sites since it is a cloud service. The WellHive cloud service has a FedRAMP Moderate provisional authorization sponsored by the VA and is in process for a VA ATO for this use case. VISN 7 has a visiting patient population of roughly 40,000 patients. For any of these patients receiving Community Care, their PII may traverse this system. The contract establishes VA has ownership rights over data including PII. Given the volume of individuals' PII, there is a risk that, if data were accessed by an unauthorized individual or otherwise breached, or misused, serious personal/professional or financial harm may result for the individuals affected, as well harm to the reputation of both WellHive and the VA. Completion of this PIA will not result in technology changes.

Legal Authority to operate stems from 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

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

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://vawww.va.gov/vapubs/>). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

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

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

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

- | | | |
|--|--|---|
| <input checked="" type="checkbox"/> Name | <input checked="" type="checkbox"/> Emergency Contact Information (Name, Phone Number, etc. of a different individual) | <input type="checkbox"/> Internet Protocol (IP) Address Numbers |
| <input checked="" type="checkbox"/> Social Security Number | <input type="checkbox"/> Financial Account Information | <input type="checkbox"/> Current Medications |
| <input checked="" type="checkbox"/> Date of Birth | <input checked="" type="checkbox"/> Health Insurance Beneficiary Numbers | <input type="checkbox"/> Previous Medical Records |
| <input type="checkbox"/> Mother's Maiden Name | <input type="checkbox"/> Certificate/License numbers | <input checked="" type="checkbox"/> Race/Ethnicity |
| <input checked="" type="checkbox"/> Personal Mailing Address | <input type="checkbox"/> Vehicle License Plate Number | <input type="checkbox"/> Tax Identification Number |
| <input checked="" type="checkbox"/> Personal Phone Number(s) | | <input type="checkbox"/> Medical Record Number |
| <input checked="" type="checkbox"/> Personal Fax Number | | <input checked="" type="checkbox"/> Gender |
| <input checked="" type="checkbox"/> Personal Email Address | | <input type="checkbox"/> Integration Control Number (ICN) |

- Military History/Service Connection
- Next of Kin

Other Unique Identifying Information (list below)

- Type and specialty of booked appointment
- Appointment reason

PII Mapping of Components

WellHive Scheduling Grid Integration – Columbia Community Care (CC) Scheduling consists of 1 key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by WellHive Scheduling Grid Integration – Columbia Community Care (CC) Scheduling and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

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

PII Mapped to Components

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
WellHive SaaS Cloud Service	Yes	Yes	Name, Social Security Number, Date of Birth, Personal Mailing Address, Personal Phone, Personal Email Address, Personal Fax Number, Emergency Contact Information, Health Insurance Beneficiary Numbers,	Required to book appointments with VA’s Community Care providers.	Federal Risk and Authorization Management Program (FedRAMP) Compliant (encryption), Two factor authentication; Security Manager configured to limit data access according to role and organizational assignments. Access is

			Race/Ethnicity, Gender, Type and specialty of booked appointment, appointment reason		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 sources are data entry from VA schedulers and data delivery from CDW.

The following data elements are received via data entry from VA schedulers, data delivery from CDW, data retrieval from the DTC Integration Platform MPI-E API:

- Patient Name
- Patient Social Security Number
- Patient Date of Birth
- Patient Mailing Address
- Patient Phone Number(s)
- Patient Email Address
- Personal Fax Number
- Patient Emergency Contact Information (Name, Phone Number, etc of a different individual)
- Patient Gender
- Patient Race/Ethnicity
- Type and specialty of booked appointment
- Health Insurance Beneficiary Numbers
- Appointment Reason

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.

Patient and referral data is delivered from VA's CDW to WellHive once per month as part of the AMCMS program via SFTP connection initiated by CDW host machines. VA schedulers will be able to select from this data for sharing with VA Community Care providers, or the scheduler will enter patient and referral data directly into WellHive User Interface.

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

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

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

This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

For data received from CDW, it is the responsibility of VA processes managing data in CDW to ensure accuracy. Each month that data is redelivered, any updates for accuracy that occurred at CDW are received and overwrite existing inaccurate data.

For patient and referral data received by manual entry, the data is checked against any data already received from CDW, e.g. when entering patient demographics matching patient data is presented for selection. Still, since data is received only once per month from CDW, VA schedulers will need to book appointments for patient and/or referrals that WellHive has not yet received data for. In these cases, VA schedulers will enter data manually, and there are no source available to check against for accuracy.

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

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) Version Date: February 27, 2020 Page 8 of 23 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

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: Any sharing of PII to VA Community Care providers carries risk to the confidentiality of the PII.

Mitigation: This risk is mitigated in several ways.

Only providers that have already been vetted through the VA's Community Care program are configured for sharing from the VA's tenant in WellHive.

The data shared through WellHive is only a subset of the data already shared with these same providers via secure fax and secure email.

WellHive itself has FedRAMP Moderate ATO which requires FIPS 140-2 encryption of data within the system, both when at rest and in transit.

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.

- Patient Name
 - For registering a new patient at a receiving Community Care provider
- Patient Social Security Number
 - For registering a new patient at a receiving Community Care provider
- Patient Date of Birth
 - For registering a new patient at a receiving Community Care provider
- Patient Mailing Address
 - For registering a new patient at a receiving Community Care provider
- Patient Phone Number(s)
 - For registering a new patient at a receiving Community Care provider
- Patient Email Address

- For registering a new patient at a receiving Community Care provider
- Personal Fax Number
 - For registering a new patient at a receiving Community Care provider
- Patient Emergency Contact Information (Name, Phone Number, etc of a different individual)
 - For registering a new patient at a receiving Community Care provider
- Patient Gender
 - For registering a new patient at a receiving Community Care provider
- Patient Race/Ethnicity
 - For registering a new patient at a receiving Community Care provider
- Type and specialty of booked appointment
 - For registering a new patient at a receiving Community Care provider
- Appointment Reason
 - For registering a new patient at a receiving Community Care provider
- Health Insurance Beneficiary Numbers (i.e. the VA referral authorization ID and third-party insurance subscriber ID)
 - For providing the authorization information to the Community Care provider that they need for submitting claims back to the VA.

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 WellHive SaaS includes an analytics capability, which will be used to help VA stakeholders understand the performance of the Scheduling Grid Integration program of the Health Services Program Office, Community Care.

With this intended purpose:

- Information about individual patients may be used for analysis, but the results of analysis are expected to be in aggregate form, which means no new or previously unutilized information about individual patients is expected to be created or made available.

- Some new or previously underutilized information about the performance of individual VA personnel (schedulers) may be created or made available.

2.3 How is the information in the system secured?

2.3a What measures are in place to protect data in transit and at rest?

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

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

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

All PII within WellHive is FIPS 140-2 encrypted both in transit and at rest. Extra protection is provided for SSNs, such that users don't have access to SSNs unless explicitly requested and all such requests are logged for auditing.

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

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

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

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

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?

This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

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, WellHive Scheduling Grid application administrators provision access.

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 realtime 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 within 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.

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

- Patient Name
- Patient Social Security Number
- Patient Date of Birth
- Patient Mailing Address
- Patient Phone Number(s)
- Patient Email Address
- Personal Fax Number
- Patient Emergency Contact Information (Name, Phone Number, etc of a different individual

- Patient Gender
- Patient Race/Ethnicity
- Type and specialty of booked appointment
- Appointment Reason
- Health Insurance Beneficiary Numbers (i.e. the VA referral authorization ID and third-party insurance subscriber 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. If the system is using cloud technology, will it be following the NARA approved retention length and schedule?

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

The WellHive SaaS retains information in scope for this PIA for the term of the program which is currently contracted through 9/15/2023.

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 RCS 10-1 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

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)

3.4 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

WellHive will use sampled data for pre-release testing, in an environment that falls within WellHive's FedRAMP Authorization Boundary, and which has all the same protections in place as the production environment used to support VA end users.

Other than the above exception, no PII will be used 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.

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, the system adheres to the VA Records Control Schedule (RSC) schedules for the data it maintains. At the end of the period of contract performance the COR will coordinate with WellHive 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.

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

NOTE: Question 3.9 (second table) on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system within VA with which information is shared.

State the purpose for the internal sharing. If you have specific authority to share the information, provide a citation to the authority.

For each interface with a system outside your program office, state what specific data elements (PII/PHI) are shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?

This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	List the purpose of the information being shared /received with the specified program office or IT system	List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system	Describe the method of transmittal
VA Lighthouse	Required to book appointments with VA's Community Care providers.	•Patient Name•Patient Social Security Number•Patient Date of Birth•Patient Mailing Address•Patient Phone Number(s)• Personal Fax Number(s) •Patient Email Address•Patient Emergency Contact Information•Patient Gender•Patient Race/Ethnicity•Health Insurance Beneficiary Numbers	API over HTTPS
VA Digital Integration Platform (DIP)	Required to book appointments with VA's Community Care providers.	•Patient Name•Patient Social Security Number•Patient Date of Birth•Patient Mailing Address•Patient Phone Number(s)• Personal Fax Number(s) •Patient Email Address•Patient Emergency Contact Information•Patient Gender•Patient Race/Ethnicity•Health Insurance Beneficiary Numbers	API over HTTPS

<i>List the Program Office or IT System information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</i>	<i>Describe the method of transmittal</i>
VA Corporate Data Warehouse (CDW)	Required to book appointments with VA's Community Care providers.	•Patient Name•Patient Social Security Number•Patient Date of Birth•Patient Mailing Address•Patient Phone Number(s)• Personal Fax Number(s) •Patient Email Address•Patient Emergency Contact Information•Patient Gender•Patient Race/Ethnicity•Health Insurance Beneficiary Numbers	Secure File Transfer Protocol (SFTP) over SSH.

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

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

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

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

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.

This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

<i>List External Program Office or IT System information is shared/received with</i>	<i>List the purpose of information being shared / received / transmitted with the specified program office or IT system</i>	<i>List the specific PII/PHI data elements that are processed (shared/received/transmitted) within the Program or IT system</i>	<i>List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)</i>	<i>List the method of transmission and the measures in place to secure data</i>

<p>CC Providers</p>	<p>Required to book appointments with VA's Community Care providers.</p>	<p>Name, Social Security Number, Date of Birth, Personal Mailing Address, Personal Phone, Personal Fax Number(s), Personal Email Address, Emergency Contact Information, Health Insurance Beneficiary Numbers, Race/Ethnicity, Gender , Type and Specialty of Booked Appointment, Appointment Reason</p>	<p>Business Associate Agreement (BAA)</p>	<p>The WellHive SaaS and the systems of CC Providers will connect with various protocols, and with connections occurring in either direction.</p> <p>All connections between the WellHive SaaS and CC Providers will be encrypted with TLS 1.1 or TLS 1.2.</p> <p>This usage of TLS 1.1 is permitted by the following clause from NIST SP 800-52 rev. 2: "When interoperability with non-government systems is required, TLS 1.1 and TLS 1.0 may be supported."</p>
<p>Azure Maps</p>	<p>Required to find CC Providers located nearest to a patient.</p>	<p>Mailing Address</p>	<p>There is a subscription agreement in place between WellHive and Azure</p>	<p>The WellHive SaaS connects to Azure Maps over HTTPS, with TLS version 1.2.</p>

			<p>for this service.</p> <p>No BAA or other agreement is required, because only mailing address is shared, with no other identifying information</p>	
--	--	--	--	--

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum Of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.

Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.

This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:

Privacy Risk:

Any sharing of PII to VA Community Care providers carries risk to the confidentiality of the PII.

Mitigation:

This risk is mitigated in several ways.

1. Only providers that have already been vetted through the VA’s Community Care program are configured for sharing from the VA’s tenant in WellHive.
2. The data shared through WellHive is only a subset of the data already shared with these same providers via secure fax and secure email.
3. WellHive itself has FedRAMP Moderate ATO which requires FIPS 140-2 encryption of data within the system, both when at rest and in transit.

It should also be noted that the VA's CC Scheduling processes already result in sharing the same information with CC Providers, prior to the existence of the WellHive Scheduling Grid Integration. Therefore, sharing this data through WellHive introduces no new risk from an external sharing and disclosure perspective.

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 Version Date: February 27, 2020 Page 20 of 23 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 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks.

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

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

Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?

This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use

Follow the format below:

Privacy Risk: There is risk that individuals who provide information to VA will not know how their information is being shared 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 in WellHive. Information within WellHive comes from the 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 Version Date: February 27, 2020 Page 22 of 23 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 ensure 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 WellHive is inaccurate and decisions are made (outside of WellHive) 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.

Mitigation:

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) from which care was scheduled.

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, 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.

VA contractors have access to the VA's WellHive SaaS tenant for configuration and 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).

WellHive and VA VISN 7 executed a BAA on 2/1/2022.

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.

Community providers are contacted VIA Optum and complete training requirements through Optum. VA staff meet this requirement through annual VA Privacy training.

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

If Yes, provide:

1. *The Security Plan Status, Approved*
2. *The Security Plan Status Date, 7/6/2021*
3. *The Authorization Status, Approved*
4. *The Authorization Date, 10/21/2021*
5. *The Authorization Termination Date, 4/16/2023*
6. *The Risk Review Completion Date N/A*
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.

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

Section 9 – Technology Usage

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

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

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

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

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1.

The system does use cloud computing under the SaaS model in Microsoft Azure and is FedRAMP authorized.

9.2 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract)

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

Per contract 36C10A20F0304 between the VA and WellHive, the VA retains ownership rights over data including PII. From the contract:

Adequate security controls for collecting, processing, transmitting, and storing of Personally Identifiable Information (PII), as determined by the VA Privacy Service, must be in place, tested, and approved by VA prior to hosting, operation, maintenance, or use of the information system, or systems by or on behalf of VA. These security controls are to be assessed and stated within the PIA and if these controls are determined not to be in place, or inadequate, a Plan of Action and Milestones (POA&M) must be submitted and approved prior to the collection of PII.

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.

WellHive collects ancillary data and maintains ownership of this data. Ancillary data includes telemetry data and application logs required for operating the system and for maintaining appropriate system resource availability. Ancillary data also includes audit logs as required by WellHive's FedRAMP authorization. Copies of FedRAMP-required audit logs are available to the VA upon request.

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.

Per contract 36C10A20F0304 between the VA and WellHive:

For information systems that are hosted, operated, maintained, or used on behalf of VA at non-VA facilities, Contractors/Subcontractors are fully responsible and accountable for ensuring compliance with all HIPAA, Privacy Act, FISMA, NIST, FIPS, and VA security and privacy directives and handbooks.

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).

The scheduling capability of the WellHive SaaS includes RPA for orchestrating the movement of patient data between the VA and CC Providers. When a VA scheduler schedules an appointment for a given patient with a given CC Provider, WellHive’s RPA will retrieve data for that patient from a cache of CDW-sourced VA data stored within WellHive, transform it to satisfy the interface of the CC Provider’s system(s), then write that transformed data to the CC Provider’s system(s).

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

ID	Privacy Controls
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, Selina Bland

Information System Security Officer, Calvin Dingle

Information System Owner, Fred Tolley

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).

From Section 6)

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 Version Date: February 27, 2020 Page 20 of 23 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