Privacy Impact Assessment for the VA IT System called:

WellHive - Enterprise

Veterans Health Administration (VHA)

Office of Integrated Veteran Care (IVC)

eMASS ID #1174

Date PIA submitted for review:

04/15/2025

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Eller Pamintuan	eller.pamintuan@va.gov	303-331-7512
Information System Security Officer (ISSO)	Randall Smith	randall.smith@va.gov	319-631-2120
Information System Owner	Thomas Adams	thomas.adams4@va.gov	817-350-7773

Abstract

The abstract provides the simplest explanation for "what does the system do for VA?".

WellHive -Enterprise (WellHive) is a FedRAMP Authorized Software as a Service (SaaS) hosted on Amazon Web Services (AWS) GovCloud. VA Data resides outside the VA network. The WellHive system has multiple uses at VA. Performance Oversight and Access Reporting (POAR) is used by the Office of Integrated Veteran Care (IVC), Veterans Integrated Service Network (VISNs) and medical centers to integrate community care financial costs to monitor, forecast and control Community Care's medical services costs. The WellHive Scheduling and providers within the VA's Community Care Network. The functionality includes the ability to search Platform solution enables VA staff to directly schedule medical appointments with VHA providers for providers, compare schedules and directly schedule appointments electronically within a singular application. The search for a suitable provider will be guided by choice of specialty, geographic location, and timeliness of availability. This will help maximize the timeliness of care for community care appointments and bring efficiencies when scheduling internally.

WellHive -Enterprise (WellHive) is the combination of Performance Oversight and Access Reporting (POAR) and External Provider Scheduling (EPS).

Overview

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

1 *General Description*

A. *What is the business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?*

There are two primary purposes for this Software as a Service (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 second is 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' Electronic Health Record (EHR) and Practice Management systems. Additionally, WellHive will collect Patient, referral, and referral authorization information 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 phones 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. Patient demographics are received from the integration with VA Master Person Index (MPI-e). Additionally, patient and referral data is already delivered to WellHive from VA's Corporate Data Warehouse (CDW) once per month for the EPS program, and this data will be used as available to reduce the amount of data entry performed by VA schedulers.

B. *Who is the owner or has control of the IT system or project? If the system has an eMASS entry, ensure this information matches with the eMASS entry.*

VA Controlled / non-VA Owned and Operated. Most of the WellHive 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 POAR 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 Secure File Transfer Protocol (SFTP).

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.

2. Information Collection and Sharing

C. *Indicate the expected number of individuals whose information is stored in the system and include a brief description of the typical client or affected individual?*

For the management of costs associated with care provided in the community, primary purpose listed above in 1.B., the expected number of individuals whose information is stored is 2.1 million. For the second purpose listed above in 1.B., to increase the accuracy, visibility, and volume OHI (other health insurance) coverages available to the VA for billing 3rd party insurance carriers, the expected number of individuals whose information is stored is roughly the entire VA patient population, i.e., 9 million. For the third purpose of scheduling community care referrals, the expected number of individuals is the number of individuals eligible for Community Care, approximately 2.1 million.

Check if Applicable	**Demographic of individuals**
☒	Veterans or Dependents
☒	VA Employees
☐	Clinical Trainees
☒	VA Contractors
☒	Members of the Public/Individuals
☐	Volunteers

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

Historical patient data, CC (Community Care) referrals and claims data, and 3rd party insurance and billing data are received from VA CDW via Secure File Transfer Protocol (SFTP), for analyzing and reporting on predicted referral costs, incoming claims allocation to those predicted costs, and correlation with budget; Patient demographics are used for delivering to VA Community Care Network (CCN) providers for the purposes of securing an appointment for an authorized referral. Provider profile data from VA Provider Profile Management System (PPMS) is used to enable VA schedulers to identify potential providers for an appointment. VA employee and contractor email addresses, first names, and last names are used to identify users within the system.

E. *What information sharing is conducted by the IT system? A general description of the modules and components, where relevant, and their functions.*

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. This functionality is part of WellHive's Care Navigation capability, which supports VA External Provider Scheduling (EPS). No information sharing functionality exists for WellHive's Analytics capability, which supports VA POAR.

F. Are the modules/subsystems only applicable if information is shared?

Information sharing is only relevant for the Care Navigation capability, which supports VA EPS.

G. *Is the system operated in more than one site to include primary and secondary 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?*

This system is Software as a Service (SaaS) and is not operated in more than one site.

3. Legal Authority and System of Record Notices (SORN)

H. What is the citation of the legal authority and SORN to operate the IT system?

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 (7-30-2015);
- 54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files - VA (3-3-2015);
- 155VA10, Customer Relationship Management System (CRMS) - VA (9-15-2023)

Additional 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 › ChapterVII › 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.

H. What is the SORN?

*23VA10NB3, Non-VA Care (Fee) Records - VA (7-30-2015);
https://www.govinfo.gov/content/pkg/FR-2015-07-30/pdf/2015-18646.pdf
54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files - VA (3-3-2015);
https://www.govinfo.gov/content/pkg/FR-2015-03-03/pdf/2015-04312.pdf
155VA10, Customer Relationship Management System (CRMS) - VA (9-15-2023);
https://www.govinfo.gov/content/pkg/FR-2023-09-15/pdf/2023-20044.pdf.*

I. SORN revisions/modification

23VA10NB3 and 54VA10NB3 are in the process of being revised/updated by the SORN POC.

I. If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval.

Yes. Updates needed as stated above, but no modifications required.

4. System Changes

J. Will the business processes change due to the information collection and sharing?

☐ *Yes*

☒ No
if yes, <<ADD ANSWER HERE>>

K. *Will the technology changes impact information collection and sharing?*

☐ Yes

☒ No
if yes, <<ADD ANSWER HERE>>

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 Information collected, used, disseminated, created, or maintained in the system.

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

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

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1. It must also match the information provided in question 3.4 of the PTA.

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
☒ **Full** Social Security Number
☐ **Partial** Social Security Number
☒ Date of Birth
☐ Mother's Maiden Name
☒ Personal Mailing Address
☒ Personal Phone Number(s)
☒ Personal Fax Number
☒ Personal Email Address
☒ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
☐ Financial Information
☒Health Insurance Beneficiary Numbers Account Numbers

☐ Certificate/License numbers[1]
☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☐ Medications
☒ Medical Records
☒ Race/Ethnicity
☒ Tax Identification Number
☒ Medical Record Number
☒ Sex
☒ Integrated Control Number (ICN)
☐ Military History/Service Connection
☐ Next of Kin
☐ Date of Death
☒ Business Email Address
☐ Electronic Data Interchange Personal Identifier (EDIPI)
☒ Other Data Elements (list below)

Other PII/PHI data elements: Individual Patient Demographics, Medical Appointments, Appointment Reason, Claims and Claim Responses, Individual Providers, Provider Organizations, Provider Locations

1.2 List the sources of the information in the system
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

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

Appointments booked through EPS are created by VA schedulers within WellHive, under the VA EPS program. All other data is sourced from various VA systems: SSOi, CDW, MPI-E, and PPMS.

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

All sources used for data are VA-managed systems. The VA aggregates historical data from CDW (Corporate Data Warehouse) for the purpose of analysis, therefore making CDW an appropriate source of the historical claims and financial data. 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. MPI-e is an aggregate of current patient demographics accessible by approved integration with external services making it an appropriate source for patient demographics. No commercial aggregators or other external sources are used.

1.2c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?

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

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. WellHive will create records of healthcare appointments scheduled through the system. WellHive does not otherwise create or make available new or previously unutilized information about an individual.

1.3 Methods of information collection

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

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

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.

Patient demographics are retrieved by WellHive from VA's MPI-e service via HTTPS requests.

VA schedulers will be able to select from this data for sharing with VA Community Care providers and can manually enter add referral data directly into WellHive User Interface.

1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, what is the form's OMB control number and the agency form number?

Information is collected from various VA system. The information is not directly collected from an individual using a form, system is not subject to Paperwork Reduction Act.

1.4 Information checks for accuracy, and how often will it be checked.

These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

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

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. 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 patient demographics received from MPI-e, it is the responsibility of VA processes managing data in MPI-e to ensure accuracy.

For records of appointments scheduled through WellHive, accuracy of the status of the appointment is ensured with recurring automated checks against relevant CC Provider system records until the appointment reaches a terminal state (i.e. completed or cancelled).

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

No.

1.5 Identify the specific legal authorities, arrangements, and agreements that 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); 155VA10, Customer Relationship Management System (CRMS) (FR: Tuesday March 3, 2015)

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 <u>PRIVACY IMPACT ASSESSMENT: Characterization of the information</u>

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

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

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

Principle of Minimization: The information is directly relevant and necessary to accomplish the specific purposes of the program.

Principle of Individual Participation: The program, to the extent possible and practical, collects information directly from the individual.

Principle of Data Quality and Integrity: VA policies and procedures must ensure that personally identifiable information is accurate, complete, and current.
This 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, Master Person Index, and PPMS. Risk that may occur is that the data received from those other VA systems is not accurate. Any sharing of PII to VA Community Care providers carries risk to the confidentiality of the PII.

Mitigation: All electronic exchange of information is performed using encrypted protocols, which protects the integrity and confidentiality of the information while in transit. 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 that will be used in support of the program's business purpose.

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

PII/PHI Data Element	Internal Use	External Use
Name	Individual Veteran community care claim identification, 3rd party insurance coverage identification, identifying clinical staff providing care to Veterans in the community for the purpose of forecasting, monitoring, and trending Office of Community Care (OCC)'s medical services and costs	Individual identification of patients for CC Providers.
Social Security Number	Individual Veteran community care claim identification, 3rd party insurance coverage identification	Individual identification of patients for CC Providers.
Date of Birth	Individual Veteran community care claim identification, 3rd party insurance coverage identification	Individual identification of patients for CC Providers.
Personal Mailing Address	Individual Veteran community care claim identification, 3rd party insurance coverage identification	Enable CC Providers to communicate with patients.
Personal Phone Number	Used by VA Medical Support Assistants to contact the veteran for requesting updated insurance coverage information	Enable CC Providers to communicate with patients.
Personal Email Address	Used by VA Medical Support Assistants to contact the veteran for requesting updated insurance coverage information	Enable CC Providers to communicate with patients.
Individual Patient Demographics	Identifying 3rd party insurance coverage for individual Veteran	Individual identification of patients for CC Providers.
Tax Identification Number	Identifying clinical staff providing care to Veterans in the community for the purpose of forecasting, monitoring, and trending IVC's medical services and cost	Not used externally.
Medical Records	Diagnosis Code: Used to identify reason for the patient outpatient encounter or admission for the purpose of forecasting, monitoring and	Not used externally.

	trending IVC 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 IVC 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 IVC medical services and costs	
Medical Records Numbers	Diagnosis Code: Used to identify reason for the patient outpatient encounter or admission for the purpose of forecasting, monitoring and trending IVC 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 IVC 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	Individual identification of referrals for CC Providers.

	forecasting, monitoring and trending IVC medical services and costs	
Insurance Coverages	Forecasting, monitoring and trending medical services and costs	Not used externally.
Insurance Eligibility	Forecasting, monitoring and trending medical services and costs	Not used externally.
Medical Appointments	Forecasting, monitoring and trending medical services and costs	Booking appointments with CC Providers.
Claims and Claim Responses	Forecasting, monitoring and trending medical services and costs	Not used externally.
Individual Providers	Forecasting, monitoring and trending medical services and costs	Not used externally.
Payer Organizations	Forecasting, monitoring and trending medical services and costs	Not used externally.
Provider Organizations	Forecasting, monitoring and trending medical services and costs	Not used externally.
Provider Locations	Forecasting, monitoring and trending medical services and costs	Not used externally.
Personal Fax Number	Individual Veteran community care claim identification, 3rd party insurance coverage identification	Enable CC Providers to communicate with patients.
Emergency Contact Information	Individual Veteran community care claim identification, 3rd party insurance coverage identification	Enable CC Providers to communicate with patient emergency contacts.
Health Insurance Beneficiary Numbers	Individual Veteran community care claim identification, 3rd party insurance coverage identification	Not used externally.
Appointment Reason	Individual Veteran community care claim identification, 3rd party insurance coverage identification	Booking appointments with CC Providers.
Sex	Individual Veteran community care claim identification, 3rd party insurance coverage identification	Individual identification of patients for CC Providers.

Race/Ethnicity	Individual Veteran community care claim identification, 3rd party insurance coverage identification	Individual identification of patients for CC Providers.
Integrated Control Number	Individual Veteran community care claim identification, 3rd party insurance coverage identification	Not used externally.

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

2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis?

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 also includes an analytics capability, which will be used to monitor current utilization and other metrics related to appointments scheduled through the SaaS.

2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

POAR does not create or make available new or previously unutilized information about an individual.

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.

EPS creates records of healthcare appointments booked through the system. These appointment records are accessible to VA employees within WellHive.

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

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

All PII within WellHive is FIPS 140-2 encrypted both 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? (refer to PTA question 3.8).

The system is processing SSNs. Through FedRAMP authorization, WellHive is required to implement more than 300 of the very same controls the VA implements for protecting Federally owned data, which includes any SSNs WellHive receives from the VA. WellHive has over 1000 pages of documentation showing how we satisfy these controls, in the form of a System Security Plan (SSP) and an Operations Manual. We are assessed annually by a FedRAMP 3rd Party Assessor (3PAO). Through this assessment, the 3PAO reviews WellHive's SSP and Operations Manual, and WellHive is required to provide evidence of continuous implementation for each control. The 3PAO's resulting Security Assessment Report, WellHive's SSP, and WellHive's Operations Manual are reviewed by VA cloud security each year. Included in the FedRAMP controls is a requirement to perform Continuous Monitoring of the WellHive system and any/all Federally-owned data that traverses through, as well as to provide monthly reports to VA cloud security on our Continuous Monitoring results. WellHive is compliant with "Revision 5" of FedRAMP controls, which incorporates privacy concerns. In addition to FedRAMP, WellHive complies with HIPAA Security and Privacy Rules.

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

All WellHive personnel supporting the system must agree to rules of behavior, which include privacy-related aspects, before working with the system. WellHive's FedRAMP assessments and authorization ensures appropriate administrative, technical, and physical safeguards are in place to protect all federal data within the system, including PII/PHI.

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

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

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

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

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

2.4a How is access to the PII determined?

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.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented? How are the documented, i.e. Policy, SOP, other. And where is this documentation located?

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, application administrators, provision of access. Criteria, procedures, controls and responsibilities regarding determining access are documented in VA policies and procedures. Specifically, these are captured in a VA-Internal Standard Operating Procedure (SOP) document called "Individual User Provisioning SOP".

2.4c Does access require manager approval?

VA supervisors/managers or contracting officer's technical representative (COR) determine and approve access as required based on user role.

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

Audit logs for access to PII are recorded and maintained within WellHive internal infrastructure. Upon request from the VA, WellHive will provide exports of these audit logs for VA review.

WellHive automatically disables unused VA user accounts after 35 days of inactivity, per FedRAMP control AC-2(3). This helps ensure access to PII is removed if it's no longer needed.

2.4e Who is responsible for assuring safeguards for the PII as identified in eMASS?

Safeguarding of VA data within WellHive is a shared responsibility, shared between WellHive and VA. WellHive's FedRAMP Customer Responsibility Matrix (CRM) can be consulted for details on which security and privacy controls involve VA responsibilities.

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, Personal Fax Number, Patient Emergency Contact Information (Name, Phone number, etc. of a different individual), Patient Sex, Health Insurance Beneficiary Number, Race/Ethnicity, Tax Identification Number (TIN)(might be SSN for individual providers), Previous Medical

Records, Type and specialty of booked appointment, 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. ***The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.*** *If the system is using cloud technology, will it be following the NARA approved retention length and schedule https://www.archives.gov/records-mgmt/grs? This question is related to privacy control DM-2, Data Retention and Disposal.*

Reference the following SORN Retention and Disposal:

23VA10NB3, Non-VA Care (Fee) Records,

Paper and electronic documents at the authorizing healthcare facility related to authorizing the Non-VA Care (fee) and the services authorized, billed and paid for are maintained in ‘‘Patient Medical Records—VA’’ (24VA10P2). These records are retained at healthcare facilities for a minimum of three years after the last episode of care. After the third year of inactivity the paper records are transferred to a records facility for seventy-two (72) more years of storage. Automated storage media, imaged Non-VA Care (fee) claims, and other paper documents that are included in this system of records and not maintained in ‘‘Patient Medical Records—VA’’ (24VA10P2) are retained and disposed of in accordance with disposition authority approved by the Archivist of the United States. Paper records that are imaged for viewing electronically are destroyed after they have been scanned, and the electronic copy is determined to be an accurate and complete copy of the paper record imaged.

54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files, SOR Disposition

Record Control Schedule (RCS) 10–1 item XXXVIII Civilian Health and Medical care (CHMC) Records. NARA job number N1–015–3–1Item 1–8b. (Master file) item 3, Destroy 6 years after all individuals in the record become ineligible for program benefits.

155VA10, Customer Relationship Management System (CRMS), SOR Disposition

CRMS records will be maintained and disposed of in accordance with the schedule approved by the Archivist of the United States, Records Control Schedule (RCS) 10–1, 1925.1, Destroy one year after resolved, or when no longer needed for business use, whichever is appropriate.

3.3 The retention schedule approved by the VA records office and the National Archives and Records Administration (NARA).

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

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

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

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

23VA10NB3, Non-VA Care (Fee) Records, SOR Disposition SOR Disposition

6000.2., Electronic Health Record (EHR): Electronic Final Version of Health Record. Final, consolidated, electronic version of a Patient Medical Record. Includes information migrated from interim electronic information systems, electronic medical equipment, or information entered directly into the patient medical record information system. May be stored on optical disks or other magnetic media. **Temporary**. Destroy/delete 75 years after the last episode of patient care. N1-15-02-3, item 3

54VA10NB3, Veterans and Beneficiaries Purchased Care Community Health Care Claims, Correspondence, Eligibility, Inquiry and Payment Files, SOR Disposition

1260.1., Care in Community: Care in the Community, Health and Medical Care Program records include but not limited to: Veteran and beneficiary claim and administrative records related to receiving health care services at VA expense outside VA facilities. A typical record file includes eligibility information, claim forms, medical records in support of claims and data concerning health care providers, services provided, amounts claimed and paid for health care services. Electronic Records. (Master Files) Electronic records produced from scanned documents or records received electronically (optical disk, magnetic tape or other electronic medium). **Temporary**. Destroy 6 years after all individuals in the record become ineligible for program benefits. N1-15-03-1, item.

155VA10, Customer Relationship Management System (CRMS), SOR Disposition

1925.1., Public Customer Service Operations Records. Records from operating a customer call center or service center providing services to the public. Services may address a wide variety of topics such as understanding agency mission-specific functions or how to solve technical difficulties with external-facing systems or programs. Includes: incoming request and responses, trouble tickets and tracking logs, recording of call center phone conversations with customers used for quality control and customer service training, system data, including customer ticket numbers and visit tracking, evaluation and feedback about customer service, information about customer services, such as "Frequently Asked Questions" (FAQs) and user guides, reports generated from customer management data, and complaints and commendation records; feedback and satisfaction surveys, including survey instruments, data, background material, and reports. **Temporary**. Destroy 1 year after resolved, or when no longer needed for business use, whichever is appropriate. GRS 6.5, item 020, DAA-GRS-2017-0002-0001.

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

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

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. 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 to privacy of using PII for research, testing or training. Training for WellHive is completed in a test environment with de-identified and de-sensitized information. 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.

<u>3.6 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. (Work with your System Privacy Officer (PO) to complete all Privacy Risk questions within this section).

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

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

<u>Principle of Minimization:</u> The project retains only the information necessary for its purpose, additionally, the PII is retained only for as long as necessary and relevant to fulfill the specified purposes.

<u>Principle of Data Quality and Integrity:</u> The PIA should describe 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:

<u>Privacy Risk:</u> Unnecessary retention of PII/SPI: There is risk that the information maintained by POAR and/or EPS 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 (RCS) schedules for the financial management 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.

PII Mapping of Components

4.1a **WellHive -Enterprise** consists of **2** key components (servers/databases/instances/applications/software/application programming interfaces (API)). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **WellHive -Enterprise** and the reasons for the collection of the PII are in the table below.

Note: Due to the PIA being a public facing document, please do not include server names in the table. The first table of 3.9a in the PTA should be used to answer this question.

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
VHA Corporate Data Warehouse (CDW) Workgroup Database for POAR	**Yes**	**Yes**	**Name, SSN, DOB, Personal Mailing Address, Personal Phone Number,**	**Cost Management, forecasting activities**	**FIPS 140 Encryption**

			Personal Email Address, Medical Records, Medical Records Numbers, Individual Patient Demographics, Insurance Coverages, Insurance Eligibility, Medical Appointments, Claims and Claim Responses, Individual Providers, Payer Organizations, Provider Organizations, Provider Locations, Health Insurance Beneficiary Numbers, Race/Ethnicity, Tax Identification Number, Personal Fax Number, Emergency Contact Information, Health Insurance Beneficiary Numbers, Sex, Appointment Reason		

WellHive SaaS Cloud Service	**Yes**	**Yes**	**Name, SSN, DOB, Personal Mailing Address, Personal Phone Number, Personal Email Address, Medical Records, Medical Records Numbers, Individual Patient Demographics, Insurance Coverages, Insurance Eligibility, Medical Appointments, Claims and Claim Responses, Individual Providers, Payer Organizations, Provider Organizations, Provider Locations, Health Insurance Beneficiary Numbers, Race/Ethnicity, Tax Identification Number, Personal Fax Number, Emergency Contact Information, Health**	**For analyzing CC (Community Care) referrals, claims, predicted costs, and budgets. 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 limited to only those components required in the performance of work.**

			Insurance Beneficiary Numbers, Sex, Appointment Reason		

4.1b List internal organizations information is shared/received/transmitted, the information shared/received/transmitted, and the purpose, and how the information is transmitted.

NOTE: Question 3.9b (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

IT system and/or Program office. Information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List PII/PHI data elements shared/received/transmitted.***	***Describe the method of transmittal***
VA Master Person Index (MPI-e)	Required to book appointments with VA's Community Care providers.	Name, SSN, DOB, Personal Mailing Address, Personal Phone Number, Personal Email Address, Medical Records Numbers, Individual Patient Demographics, Race/Ethnicity, Personal Fax Number, Emergency Contact Information, Sex	API over HTTPS

IT system and/or Program office. Information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List PII/PHI data elements shared/received/transmitted.*	*Describe the method of transmittal*
VHA Corporate Data Warehouse (CDW)	Cost Management, forecasting activities, and insurance capture	Name, SSN, DOB, Personal Mailing Address, Personal Phone Number, Personal Email Address, Medical Records, Medical Records Numbers, Individual Patient Demographics, Insurance Coverages, Insurance Eligibility, Medical Appointments, Claims and Claim Responses, Individual Providers, Payer Organizations, Provider Organizations, Provider Locations, Health Insurance Beneficiary Numbers, Race/Ethnicity, Tax Identification Number, Personal Fax Number, Emergency Contact Information, Health Insurance Beneficiary Numbers, Sex, Appointment Reason	SFTP over SSH
VA Digital Integration Platform (DIP) Provider Profile Management System (PPMS) Proxy	Required to book appointments with VA's Community Care providers.	Details of individual Community Care Providers (healthcare practitioners): Name, type of healthcare provider, provider address, provider phone number, care sites (locations where care is provided), provider services and specialties.	API over HTTPS

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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 WellHive staff members 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 List the external organizations (outside VA) that information shared/received. and information shared/received, and the purpose, and how the information transmitted and what measures are taken to ensure it is secure.

The sharing of information outside the agency must be compatible with the original collection. The sharing must be covered by an appropriate routine use in a SORN. If not covered, please describe under what legal mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.

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

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

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

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

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.
This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

List IT System or External Program Office information is shared/received with	***List the purpose of information being shared / received / transmitted***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)***	***List agreements such as: Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
CC Providers	Required to book appointments with VA's Community Care providers	Name, SSN, DOB, Personal Mailing Address, Personal Phone Number, Personal Email Address, Emergency Contract Information, Health Insurance, Beneficiary Numbers, Race/Ethnicity, Sex, Medical Records (appointment type/specialty, Appointment Reason	Business Associate Agreement (BAA)	The WellHive SaaS and the systems of CC Providers will connect with various protocols, and with connections occurring in either direction. All connections between the WellHive SaaS and CC Providers will be encrypted with TLS 1.1 or TLS 1.2 This usage of TLS 1.1 is permitted by the following clause from NIST SP 800-52 rev 2:

				"When interoperability with non-government system is required, TLS 1.1 and TLS 1.0 may be supported."
Azure Maps	Required to find CC Providers located nearest to a patient	Mailing Address	There is a subscription agreement in place between WellHive and Azure for this service. No BAA or other agreement is required, because only mailing address is shared, with no other identifying information	The WellHive SaaS connects to Azure maps over HTTPS, with TLS version 1.2

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.

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

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

Follow the format below:

Privacy Risk: 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 EPS. 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 The notice provided to the individual before collection of the information. Please provide a copy and/or screen shot of a web notice of the notice as an Appendix-A 6.1 on the last page of the document. (A notice may include a posted privacy policy, a Privacy Act notice on forms, notice given to individuals by the sources system, or a system of records notice published in the Federal Register.) If notice was not provided, explain why.

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

6.1a Provide the Privacy Notice provided to the public by this system or any source systems. Include a copy of the notice in Appendix A of the PIA, the Federal Register citation, or Privacy Statement from collection of information such as forms or surveys.

This is received by CDW and MPI 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 at https://www.va.gov/find-forms/about-form-10-10ez/ . 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.

6.1b If notice was not provided, explain why.

Notice is provided: https://www.va.gov/find-forms/about-form-10-10sh/.

6.1c Provide how the notice provided at the time of collection meets the purpose of use for this system.

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 at https://www.va.gov/find-forms/about-form-10-10ez/.

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. (Work with your Privacy Officer (PO) to complete all Privacy Risk questions inside the document this section).

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

Principle of Transparency: This is referring to sufficient notice provided to the individual.

Principle of Use Limitation: *The information used only for the purpose for which notice was provided either directly to the individual or through a public notice. The procedures in place must 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 WellHive 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 The procedures that allow individuals to gain access to their information.

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

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

There are no procedures for individuals to gain access to their information on WellHive. Information on WellHive comes from VA itself.

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

There are no procedures for individuals to gain access to their information on WellHive. Information on WellHive comes from VA itself.

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

Individuals 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 Veterans Benefits Administration (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. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

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.*** *(Work with your Privacy Officer (PO) to complete all Privacy Risk questions in this section).*

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: The individual must be provided with the ability to find out whether a project maintains a record relating to them.

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

Principle of Individual Participation: The mechanism by which an individual is able to prevent information about them obtained for one purpose from being used for other purposes without their 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) where care was rendered.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures. (Work with your ISSO to complete this section).

8.1 The procedures in place to determine which users may access the system, must be documented.

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

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

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.

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

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 TMS courses TMS 10176 – VA Privacy and Information Security Awareness and Rule of Behavior and TMS 10203 – Privacy and Health Insurance Portability and Accountability Act 1996 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.

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

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.

8.2a. Will VA contractors have access to the system and the PII?

VA contractors will have access to the software for development, business and maintenance purposes only. VA Contractors must take and pass TMS courses TMS 10176 – VA Privacy and Information Security Awareness and Rule of Behavior and TMS 10203 – Privacy and Health Insurance Portability and Accountability Act 1996 based on support role to the system. VA Contractors must have signed the Non-Disclosure Agreement (NDA) and VA Information Security Rules of Behavior (RoB).

8.2b. What involvement will contractors have with the design and maintenance of the system?

Contractors will have access to system software solely for development, business and maintenance of the system.

8.2c. Does the contractor have a signed confidentiality agreement?

Contractors must have signed the Non-Disclosure Agreement (NDA) and VA Information Security Rules of Behavior (RoB).

8.2d. Does the contractor have an implemented Business Associate Agreement for applicable PHI?

There is not an implemented BAA for VA contractors working on the system. However, contractors must take and pass TMS courses TMS 10176 – VA Privacy and Information Security Awareness and Rule of Behavior and TMS 10203 – Privacy and Health Insurance Portability and Accountability Act 1996 based on support role to the system.

8.2e. Does the contractor have a signed non-Disclosure Agreement in place?

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII. This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.

Contractors 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:

● TMS 10176 – VA Privacy and Information Security Awareness and Rule of Behavior

● TMS 10203 – Privacy and Health Insurance Portability and Accountability Act 1996 based on support role to the system.

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

8.4 The Authorization and Accreditation (A&A) completed for the system.

8.4a If Yes, provide:

1. *The Security Plan Status: Finalized, v6.4.0*
2. *The System Security Plan Status Date: 10.31.2024*
3. *The Authorization Status: Authorized*
4. *The Authorization Date:* 04.16.2020
5. *The Authorization Termination Date:* 11.08.2025
6. *The Risk Review Completion Date:* 04.30.2024
7. *The FIPS 199 classification of the system MODERATE (In Process for HIGH)*

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

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

The WellHive system was initially authorized at Moderate Impact in 11/01/2025. The system is currently In Process with DTC to receive A&A at the High Impact. The High use case documented in this PIA has an expected IOC of 09/16/2025.

Section 9 – Technology Usage

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

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

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related *to privacy control UL-1, Information Sharing with Third Parties.* ***(Refer to question 1.8 of the PTA)***

The system does use cloud computing, AWS GovCloud and Microsoft Azure, and uses the Software as a Service (SaaS) model. The system is FedRAMP authorized.

9.2 Does the contract with the Hosting Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract). (*Refer to question 3.3.1 of the PTA)* *This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

Per contract NNG15SD27B 36C10B23F0127 the VA retains ownership rights over data including PII. From the contract: PHI is and remains the property of Covered Entity as long as Business Associate creates, receives, maintains, or transmits PHI, regardless of whether a compliant Business Associate agreement is in place. In addition, 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 VA118-16-D-1015, Order No. 36C10B19N10150046 between the VA and Liberty IT Solutions:

1.The information system solution selected by the Contractor shall comply with the Federal Information Security Management Act (FISMA).

2.The Contractor shall comply with FedRAMP requirements as mandated by Federal laws and policies, including making available any documentation, physical access, and logical access needed to support this requirement. The Contractor shall provide the FedRAMP package in accordance with FedRAMP requirements 60 days after award and update as required.

3.Following guidance from the Federal CIO, VA will utilize existing JAB ATO or agency ATO issued by another agency as a starting point for FedRAMP requirements. If neither of those exist, VA will sponsor FedRAMP ATO. VA will be using the FedRAMP baselines as a starting point, since they are specifically tailored for cloud services.

4.The Contractor shall, where applicable, assist with the VA Authority to Operate (ATO)Process to help achieve agency authorization of the cloud service or migrated application including security scans.

5.The Contractor shall be responsible for generating and updating the Assessment and Authorization (A&A) ATO Package that includes the following documents:

a. System Security Plan (SSP)
b. Risk Assessment (RA)
c. Incident Response Plan (IRP)
d. Information Security Contingency Plan (ISCP)
e. Disaster Recovery Plan (DRP)
f. Configuration Management Plan (CMP)
g. Interconnection Security Agreement/Memorandum of Understanding (ISA/MOU)
h. Additional system description/and diagrams required by VA to gain access to VA network and receive an Authority to Operate (ATO).

6.The Contractor shall afford VA access to the Contractor’s and Cloud Service Provider’s facilities, installations, technical capabilities, operations, documentation, records, and databases.

7.If new or unanticipated threats or hazards are discovered by either VA or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party in accordance with the security appendix B.

8.The Contractor shall not release any data without the consent of VA in writing. All requests for release must be submitted in writing to the COR/CO.

Additionally, 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).*

No RPA is utilized for POAR. 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
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.

ELLER PAMINTUAN

Digitally signed by ELLER PAMINTUAN
Date: 2025.05.13 15:35:16 -06'00'

Privacy Officer, Eller Pamintuan

RANDALL SMITH

Digitally signed by RANDALL SMITH
Date: 2025.05.14 08:24:20 -05'00'

Information System Security Officer, Randall Smith

THOMAS ADAMS

Digitally signed by THOMAS ADAMS
Date: 2025.05.14 08:35:48 -05'00'

Information System Owner, Thomas Adams

APPENDIX A-6.1

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

https://www.va.gov/find-forms/about-form-10-10ez/

HELPFUL LINKS:

Records Control Schedule 10-1 (va.gov)

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

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

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

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

Notice of Privacy Practice (NOPP):
VHA Directive 1605.04
IB 10-163p (va.gov)