Privacy Impact Assessment for the VA IT System called:

3M RevCycle Health Service Platform (RHSP)

OEHRM – Office of Community Care Veterans Health Administration

Date PIA submitted for review:

September 7, 2021

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Griffin, Stephania	Stephania.griffin@va.gov	704-245-2492
Information System Security Officer (ISSO)	Estacio, Albert	Albert.Estacio@va.gov	909-583-6309
Information System Owner	Hartzell, Michael	Michael.Hartzell1@va.gov	803-406-0112

Abstract

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

The Department of Veterans Affairs (VA) Office of Electronic Health Record Modernization (OEHRM) RevCycle Health Service Platform (RHSP) utilizes natural language processing and artificial intelligence to provide services, including auto-suggestions of treatment and procedure codes, which are necessary to process, enrich, and enhance medical coder productivity. RHSP is the cloud-hosted back-end supporting the front-end operation of 360e Genesis.

3M plans to deploy RHSP in the Amazon Web Services (AWS) GovCloud environment.

Overview

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

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

The IT system name is 3M RevCycle Health Service Platform, and the program office is the VHA and VA Office of Electronic Health Record Modernization (OEHRM).

The business purpose of the system is to provide high-quality coding and management of medical records. The RHSP system provides back-end processing which supports this mission under the same enabling authority.

RHSP stores information for thousands of patients, aligned with front-end 360e Genesis record processing. The specific number varies and is related to the number of patients whose records are coded within each of the Veterans Integrated Service Networks (VISN). RHSP collects and maintains medical health records, and the system collects data of VA employees, veterans, and dependents.

This is a back-end processing system that is not directly accessed by hospitals/medical centers, or other regional offices.

3M RevCycle Health Service Platform (RHSP), or 3M HSP commercially, is an AWS GovCloud-hosted back-end which supports the 360e Genesis front-end operation located in the Joint Department of Defense (DoD)/VA Federal Enclave. RHSP is not a customer-facing system. RHSP utilizes natural language processing and artificial intelligence to provide services (including auto-suggestions of treatment and procedure codes) which are necessary to process, enrich, and enhance medical coder productivity. RHSP is the required back-end for 360e Genesis and allows 360e Genesis to perform computer-assisted coding. RHSP shall operate as one single shared-technology platform serving both the VA and DoD, but logical separations exist such that no data shall be shared between VA and DoD. 3M is the third-party solution owner. This is a Revenue Cycle solution that falls under Health Information Management, hence the name; RevCycle was added to Health Service Platform (HSP) to form RHSP.

RHSP connects to 360e Genesis in the Joint DoD/VA Federal Enclave via a secure network connection. Specifically, data is securely transmitted via the Joint Security Architecture (JSA), which is the Joint VA/ Defense Health Agency (DHA) Single Security Architecture (SSA), formerly Medical Community of Interest or MedCOI. The service provides authorized VA and DoD mission partners the ability to connect via a Multiprotocol Label Switching (MPLS) layer 3 Virtual Private Network (VPN) incorporated in this Joint Security Architecture (JSA).

RHSP will operate in the AWS GovCloud site and selected controls are relevant for use in that site.

The Secretary of Veterans Affairs established these guidelines pursuant to the authorities in and requirements of Title 38, United States Code, section 81 11 (38 U.S.C. 5811 I), titled "Sharing of Department of Veterans Affairs and Department of Defense Health Care Resources," and the authorities contained under Title 10, United States Code, section 1104 (10 U.S.C.5 1104), titled "Sharing of Resources with the Department of Veterans Affairs," which incorporates Title 31, United States Code, section 1535 (31 U.S.C. 51 535), titled "Agency Agreements," also known as the "Economy Act." These guidelines assist in the implementation of these statutes.

No business or technology changes are required due to completion of the PIA beyond the plans that have been presented. This is because privacy controls are already planned for application to the system.

The information system is not in the process of being modified with regard to the PII or PHI fields processed. Therefore, amendment or revision and approval of a SORN is not required.

RHSP uses AWS GovCloud computing. RHSP is undergoing FedRAMP agency authorization.

RHSP leverages existing contracts and relationships between the VA, Cerner and AWS GovCloud to establish VA ownership rights over data obtained by or entered into RHSP.

The magnitude of harm due to disclosure would be of moderate impact as determined with reference to FIPS-199 and NIST SP-800-60. A corresponding impact might affect the reputation of the CSP or its customers (VA) to the same extent.

Section 1. Characterization of the Information

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

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

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

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

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

- ☒ Name
- ☐ Social Security Number
- ☒ Date of Birth
- ☐ Mother's Maiden Name
- ☐ Personal Mailing Address
- ☐ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☐ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☐ Financial Account Information
- ☐ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers

☐ Current Medications
☒ Previous Medical Records
☒ Race/Ethnicity
☐ Tax Identification Number
☒ Medical Record Number
☒ Other Unique Identifying Information (list below)

Enterprise Patient Number/Enterprise Patient Identifier (EPN/EPI), Electronic Data Interchange Personnel Identifier (EDIPI), Death Date, Gender, Disability, Living Arrangement, Admit Date, Discharge Date, Disposition, Length of Stay, Patient Type, Account numbers (Medical Account Number), Past Visits, Patient Key, Patient Enterprise Key, Financial Class, Discharge Status Patient Class, Visit Types.

PII Mapping of Components

3M RevCycle Health Service Platform consists of **1** key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **3M RevCycle Health Service Platform** and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

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

PII Mapped to Components

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
360e Genesis VA pillars located in the Joint VA/DOD Federal Enclave	Yes	Yes	Name, Medical Record Number (MRN), Enterprise Patient Number/Enterprise Patient Identifier (EPN/EPI), Electronic Data Interchange Personnel Identifier (EDIPI), Birth Date, Death Date, Gender, Disability,	Natural Language and other data processing	System controls have been established and assessed to safeguard security and privacy. Data at rest is encrypted using AES 256. Data in transit is

			Race/Ethnicity, Living Arrangement, Admit Date, Discharge Date, Disposition, Length of Stay, Patient Type, Account numbers (Medical Account Number), Past Visits, Patient Key, Patient Enterprise Key, Financial Class, Discharge Status Patient Class, Visit Types.		encrypted using TLS v1.2+.

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

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

Describe why information from sources other than the individual is required. For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question 1.3 indicate why the system is using this source of data.

If the system creates information (for example, a score, analysis, or report), list the system as a source of information.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

RHSP collects, processes, and maintains the health-related records identified above sourced from information securely transmitted from the 360e Genesis medical coding system located in the secure Joint DoD/VA Federal Enclave. 360e Genesis obtains the health-related information from the electronic health record.

RHSP is a back-end processing system for the 360e medical coding system.

RHSP generates medical diagnosis and procedure code suggestions based on the information transmitted from the 360e Genesis medical coding system located in the secure Joint DoD/VA

Federal Enclave. These suggested codes may become part of the electronic health records and may constitute information creation.

1.3 How is the information collected?

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

If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form's OMB control number and the agency form number.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

Personally Identifiable Information (PII) and protected health information (PHI) information is securely received from 360e Genesis located in a secure Joint DoD/VA Federal Enclave via electronic transmission over a secure network connection. Specifically, data is securely transmitted via Joint VA/DHA SSA. The service provides authorized VA and DoD mission partners the ability to connect via a Multiprotocol Label Switching (MPLS) layer 3 VPN incorporated in this Joint Security Architecture (JSA).

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

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

If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.
This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

The information is imported from existing VA system and the accuracy is verified by the original source. Accuracy is assured by periodic refreshes from the data source, 360e Genesis. Frequency of update is related to frequency of use by 360e Genesis.

1.5 What specific legal authorities, arrangements, and agreements defined the collection of information?

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders.
This question is related to privacy control AP-1, Authority to Collect

The DoD Electronic Data Interchange Personnel Identifier (EDIPI) is the Unique Identifier for the Veteran. Legal Authority: Title 38 United States Code (U.S.C), Section 501 and Sections 901–905. The Secretary of Veterans Affairs established these guidelines pursuant to the authorities in and requirements of Title 38, United States Code, section 81 11 (38 U.S.C. 5811 I), titled "Sharing of Department of Veterans Affairs and Department of Defense Health Care Resources," and the authorities contained under Title 10, United States Code, section 1104 (10 U.S.C.5 1104), titled "Sharing of Resources with the Department of Veterans Affairs," which incorporates Title 31, United States Code, section 1535 (31 U.S.C. 51 535), titled "Agency Agreements," also known as the "Economy Act." These guidelines assist in the implementation of these statutes.

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.

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: The purpose for which personal data is collected is not specified in a timely manner. Data collection is not limited. Data is collected in contravention of current privacy laws. PII is not relevant to the purposes for which it is to be used and to the extent necessary for those purposes. PII is obtained by unlawful and unfair means and retained longer than required for unnecessary purpose.
To the extent practicable, not involving individuals in the process of using PII and not seeking individual consent for the collection, use, dissemination, and maintenance of PII.
Personal data is not relevant to the purposes for which it is to be used and, to the extent necessary for those purposes, data is not accurate, not complete, and is not kept up to date.

Mitigation: RHSP defines a constrained set of data fields, and all collection is limited to those essential items. RHSP data is transmitted from 360e Genesis, which collects data in a manner approved by the VA. Data in the source system, 360e Genesis, is collected only via VA approved means, which involve obtaining prior patient consent.
RHSP enforces a data storage system to pull data for review and then, if appropriate, automatically purge that data after the specified retention period has been reached. RHSP limits data field elements to only those that are relevant. RHSP ensures that all distributed reports and products contain only personal information that is relevant.
Principle of Individual Participation is not currently enforced. RHSP is back-end processing system and the service does not interact directly with the individual.
RHSP data is relevant to the purposes for which it is used and, to the extent necessary for those purposes, data is accurate, complete, and is kept up to date.

Section 2. Uses of the Information

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

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

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

Name, Account numbers (Medical Account Number), Enterprise Patient Number (EPN), Medical Record Number and/or Electronic Data Interchange Personnel Identifier (EDIPI) are used to access the system for official use. The purpose of the system is to provide high quality coding and management of medical records. RHSP system provides back-end processing which supports this mission under the same enabling authority.

Name – Patient identification.
Medical Record Number (MRN) – Used to verify patient identity; a file number for patient.
Enterprise Patient Number/Enterprise Patient Identifier (EPN/EPI) – Used to confirm patient's identity.
Electronic Data Interchange Personnel Identifier (EDIPI) - Used to confirm patient's identity.
Birth Date – Used to identify patient.
Death Date – Patient deceased date.
Gender – Identify patient sex.
Disability – Identify patient special accommodation.
Race/Ethnicity –Patient origin.
Living Arrangement – Patient daily living arrangement.
Admit Date – Date patient was admitted as an inpatient to hospital.
Discharge Date – Date patient left the hospital.
Disposition – Refers to where a patient is being discharged.
Length of Stay – Dates patient stays in the hospital.
Patient Type – Patient's first indication of the level of resource needed to provide care.
Account numbers (Medical Account Number) – An account number is a unique identifier of the patient and permits access to patient account.
Past Visits – History of patient visits.
Patient Key – Used to confirm patient's identity.
Patient Enterprise Key – Used to confirm patient's identity.
Financial Class – The patient demographic and ties to the charge.
Discharge Status Patient Class – Date patient was inactive.
Visit Types – Routine care such as physical examinations, well exam, and new patient evaluations.

2.2 What types of tools are used to analyze data and what type of data may be produced?

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

If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.
This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

The system uses Machine Learning (ML) tools and algorithms to analyze existing records, narratives and transcripts to suggest medical coding information. The processing is transactional, and the information is valid for the session and returned when ready, rather than augmented to existing records as derivative information except via the front-end systems. No actions are therefore taken against or for the individual because of the generated codes. No new records are created. Rather these codes may be used to augment and improved records at the front-end by coding specialists.

2.3 How is the information in the system secured?

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

All databases, data volumes and storage buckets are encrypted at rest with a minimum of AES 256 standard. All data in transit is encrypted with a minimum of TLS 1.2.

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

The system does not process Social Security Numbers.

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

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

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

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

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

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

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

Add answer here:

Access to the PII is determined based on the need to manage, optimize, or respond to RHSP requirements or events. Elevated access procedures, controls, and responsibilities into the RHSP SaaS are well-documented. RHSP access is limited to access by personnel who have been trained, vetted, and cleared via the VA personnel security process. Personnel need to be able to

successfully attain a Public Trust clearance, and complete VA training security awareness and HIPAA required for personnel supporting the VA program.

VA onboarding requires multiple checks, management approval, including VA Supervisor and COR.

All access to PII is monitored, tracked, recorded and logging using account authentication and access logs and Security Information Event Management (SIEM) tools like Splunk. The Risk Management Framework (RMF) implementation and assessment teams are responsible for assuring safeguards for the PII. Control responsibility is shared and layered across AWS GovCloud, and the RHSP system implementation.

Both the RHSP primary and alternate backup data centers provide physical security controls such as: cipher locks, combination locks, key cards, CCTV, safes, and 24/7 security guards. Administrative controls such as backups secured off-site, encryption of backups, methods of ensure only authorized personnel access to PII, periodic security audits, and regular monitoring of user's security practices are in place. Data at rest is encrypted at rest within the GovCloud hosting environment. Data in transit is protected through the use of TLS 1.2. All users for the RHSP project need to be able to successfully attain a Public Trust clearance, and complete VA training security awareness and HIPAA required for personnel supporting the VA program. A data loss prevention (DLP) tool will ensure that sensitive data is not lost, misused, or accessed by unauthorized users.

This PIA is clear about the uses of information, as described in this document. All data in RHSP is covered under the Privacy Act system of records, "Patient Medical Records-VA", 24VA10A7 or "VistA-VA" 79VA10. These SORNs also clearly describes the use of associated information.

RHSP data is not disclosed, made available or used for any purposes other than those specified in section 1.1 of this document. Event monitoring SIEM tools are in place for analyzing inbound and outbound traffic and are directed to VA Cyber Security Operations Centre (CSOC) team. A comprehensive training and awareness strategy aimed at ensuring that personnel understand privacy responsibilities and procedures are conducted for staff. These are targeted, role-based privacy trainings for personnel having responsibility for PII or for activities that involve PII within every three hundred sixty-five days (365).

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

RHSP collects and retains the following information:
Name, Medical Record Number (MRN), Enterprise Patient Number/Enterprise Patient Identifier (EPN/EPI), Electronic Data Interchange Personnel Identifier (EDIPI), Birth Date, Death Date, Gender, Disability, Race/Ethnicity, Living Arrangement, Admit Date, Discharge Date, Disposition, Length of Stay, Patient Type, Account numbers (Medical Account Number), Past Visits, Patient Key, Patient Enterprise Key, Financial Class, Discharge Status Patient Class, Visit Types.

Retention of records will be conducted by 360e Genesis, as the system that stores the full health records for VA patients.

The following information are collected and retained by the RHSP system:
Name – Patient identification.
Medical Record Number (MRN) – Used to verify patient identity; a file number for patient.
Enterprise Patient Number/Enterprise Patient Identifier (EPN/EPI) – Used to confirm patient's identity.
Electronic Data Interchange Personnel Identifier (EDIPI) - Used to confirm patient's identity.
Birth Date – Used to identify patient.
Death Date – Patient deceased date.
Gender – Identify patient sex.
Disability – Identify patient special accommodation.
Race/Ethnicity –Patient origin.
Living Arrangement – Patient daily living arrangement.
Admit Date – Date patient was admitted as an inpatient to hospital.
Discharge Date – Date patient left the hospital.
Disposition – Refers to where a patient is being discharged.
Length of Stay – Dates patient stays in the hospital.
Patient Type – Patient's first indication of the level of resource needed to provide care.
Account numbers (Medical Account Number) – An account number is a unique identifier of the patient and permits access to patient account.
Past Visits – History of patient visits.
Patient Key – Used to confirm patient's identity.
Patient Enterprise Key – Used to confirm patient's identity.
Financial Class – The patient demographic and ties to the charge.
Discharge Status Patient Class – Date patient was inactive.
Visit Types – Routine care such as physical examinations, well exam, and new patient evaluations.

3.2 How long is information retained?

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

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

RHSP retains records for three (3) years or less. The information pulled from health records into RHSP are temporary copies of records covered under the Privacy Act system of records, "Patient Medical Records-VA", 24VA10A7 or "VistA-VA" 79VA10 and may be destroyed when no longer needed.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so please indicate the name of the records retention schedule.

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

VHA Records Control Schedule 10-1, Item 4000.1.b – "Financial Transaction Records Related to Procuring Goods and Services, Paying Bills, Collecting Debts, and Accounting.".

3.4 What are the procedures for the elimination of SPI?

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

As RHSP is a back-end processing system, data is regularly overwritten in service of electronic transmissions from 360e Genesis data storage and overwrite requests. In the case of system decommissioning, data undergoes secure disposal in line with NIST SP 800-88 rev.1 guidelines, and AWS GovCloud data destruction procedures. This typically involves the shredding of hard drives.

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

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

No. RHSP does not use PII for research, testing, or training.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks.

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

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

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

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

Privacy Risk: The information system retains more than the information necessary for its purpose. The PII retained is extended beyond the data vital to fulfill the specified purposes.
Mitigation: RHSP constrains the information retained to only the information necessary for its purpose. The PII retained is not extended beyond the data vital to fulfill the specified purposes.

Privacy Risk: PII collected is not relevant to the purposes identified for its use. Data is not accurate or complete and is not kept up to date.
Mitigation: RHSP data is accurate, complete, and kept up to date. RHSP PII collected is relevant to the purposes identified for its use.

Privacy Risk: There are no policies and procedures developed to purge irrelevant and unnecessary documents. Data collection is not limited. Data is collected by unlawful means. Data is collected without consent. RHSP does not minimize the collection of PII, data retention, and disposal.
Mitigation: RHSP will enforce and minimize the collection of PII, data retention, and disposal.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA.

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

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

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

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

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

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?
This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are shared/received with the Program Office or IT system***	***Describe the method of transmittal***
360e Genesis VA pillars located in the	RHSP is a back-end processing system	Name, Medical Record Number	Data is securely transmitted via

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are shared/received with the Program Office or IT system*	*Describe the method of transmittal*
Joint VA/DOD Federal Enclave	for 360e Genesis. Information is shared to facilitate this back-end processing. Legal Authority: Title 38 United States Code (U.S.C), Section 501 and Sections 901–905. The Secretary of Veterans Affairs established these guidelines pursuant to the authorities in and requirements of Title 38, United States Code, section 81 11 (38 U.S.C. 5811 I), titled "Sharing of Department of Veterans Affairs and Department of Defense Health Care Resources," and the authorities contained under Title 10, United States Code, section 1104 (10 U.S.C.5 1104), titled "Sharing of Resources with the Department of Veterans Affairs," which incorporates Title 31, United States Code, section 1535 (31 U.S.C. 51 535), titled "Agency	(MRN), Enterprise Patient Number/Enterprise Patient Identifier (EPN/EPI), Electronic Data Interchange Personnel Identifier (EDIPI), Birth Date, Death Date, Gender, Disability, Race/Ethnicity, Living Arrangement, Admit Date, Discharge Date, Disposition, Length of Stay, Patient Type, Account numbers (Medical Account Number), Past Visits, Patient Key, Patient Enterprise Key, Financial Class, Discharge Status Patient Class, Visit Types.	secure network connection. Specifically, data is securely transmitted via Joint VA/DHA SSA. The service provides authorized VA and DoD mission partners the ability to connect to via a Multiprotocol Label Switching (MPLS) layer 3 VPN incorporated in this Joint Security Architecture (JSA).

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are shared/received with the Program Office or IT system*	*Describe the method of transmittal*
	Agreements," also known as the "Economy Act." These guidelines assist in the implementation of these statutes.		

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

Privacy Risk: File sharing can introduce the risk of malware infection, hacking, and loss or exposure of sensitive information. Also, high risk for exposing the sensitive data to new security threats.

Mitigation: RHSP will ensure data-sharing sessions are secure at all times by using end-to-end encryption.

Section 5. External Sharing/Receiving and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to VA, which includes Federal, State, and local governments, and the private sector.

5.1 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

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

NOTE: Question 3.11 on Privacy Threshold Analysis should be used to answer this question.

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

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

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

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

Data Shared with External Organizations

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

If specific measures have been taken to meet the requirements of OMB Memoranda M-06-15 and M-06-16, note them here.

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

Follow the format below:

Privacy Risk: N/A. RHSP Does not share information external to the agency.

Mitigation: N/A. RHSP Does not share information external to the agency.

Section 6. Notice

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

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

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

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

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

Yes, notice is provided to the individual before collection of the original information under the purview of the VA program. The information is gathered as part of Veterans Integrated Services Network (VISN) operations prior to submission to 360e Genesis. RHSP is a back-end processing system, and therefore not involved in the direct collection of PII or PHI.

The Secretary of Veterans Affairs established these guidelines pursuant to the authorities in and requirements of Title 38, United States Code, section 81 11 (38 U.S.C. 5811 I), titled "Sharing of Department of Veterans Affairs and Department of Defense Health Care Resources," and the authorities contained under Title 10, United States Code, section 1104 (10 U.S.C.5 1104), titled "Sharing of Resources with the Department of Veterans Affairs," which incorporates Title 31,

United States Code, section 1535 (31 U.S.C. 51 535), titled "Agency Agreements," also known as the "Economy Act." These guidelines assist in the implementation of these statutes.

Individuals are provided Privacy Act Statement (PAS) at the time of such collection, prior to data being entered into 360e Genesis.

As the Veterans Integrated Service Network (VISN) medical systems will collect PII directly from individuals, it will be required to provide those individuals a Privacy Act Statement (PAS) at the time of such collection.

This statement serves to inform patients of the purpose for collecting the personal information required by the Veterans Integrated Service Network (VISN) 360e Genesis system, and how it will be used.

Legal Authority: Title 38 United States Code (U.S.C), Section 501 and Sections 901–905. The Secretary of Veterans Affairs established these guidelines pursuant to the authorities in and requirements of Title 38, United States Code, section 81 11 (38 U.S.C. 5811 I), titled "Sharing of Department of Veterans," and the authorities contained under Title 10, United States Code, section 1104 (10 U.S.C.5 1104), titled "Sharing of Resources with the Department of Veterans Affairs," which incorporates Title 31, United States Code, section 1535 (31 U.S.C. 51 535), titled "Agency Agreements," also known as the "Economy Act." These guidelines assist in the implementation of these statutes.

PURPOSE: To collect information to provide and document medical care; determine eligibility for benefits and entitlements; adjudicate claims; determine whether a third party is responsible for the cost of Veterans Integrated Service Network (VISN); provide healthcare and recover that cost; evaluate fitness for duty and medical concerns which may have resulted from an occupational or environmental hazard; evaluate the Veterans Integrated Service Network (VISN) and its programs; and perform administrative tasks related to Veterans Integrated Service Network (VISN); operations and personnel readiness.

Any protected health information (PHI) in your records may be used and disclosed generally as permitted by the HIPAA Privacy Rule (45 CFR Parts 160). Permitted uses and disclosures of PHI include, but are not limited to, treatment, payment, and healthcare operations.

APPLICABLE SORN: RHSP is not a separate or independent system of records and any PII is covered under the Privacy Act system of records, “Patient Medical Records-VA”, 24VA10A7 or “VistA-VA” 79VA10. Therefore, health record disclosure would not typically be satisfied via this system, but more likely from the source Joint VA/DOD Federal Enclave. https://www.oprm.va.gov/docs/Current_SORN_List_08_17_2021.pdf) would apply.

DISCLOSURE: Voluntary. If you choose not to provide the requested information, comprehensive health care services may not be possible, you may experience administrative delays, and you may be rejected for service or an assignment. However, care will not be denied.

Any notice provided would be in accordance with the normal practice of notice provision for the EHRM at the VA service locations. The privacy notice is not applicable here as RHSP is a downstream, non-customer facing service without direct patient interaction.
Legal Authority: Title 38 United States Code (U.S.C), Section 501 and Sections 901–905. The Secretary of Veterans Affairs established these guidelines pursuant to the authorities in and requirements of Title 38, United States Code, section 81 11 (38 U.S.C. 5811 I), titled "Sharing of Department of Veterans Affairs and Department of Defense Health Care Resources," and the authorities contained under Title 10, United States Code, section 1104 (10 U.S.C.5 1104), titled "Sharing of Resources with the Department of Veterans Affairs," which incorporates Title 31, United States Code, section 1535 (31 U.S.C. 51 535), titled "Agency Agreements," also known as the "Economy Act." These guidelines assist in the implementation of these statutes.

PURPOSE: To collect information to provide and document medical care; determine eligibility for benefits and entitlements; adjudicate claims; determine whether a third party is responsible for the cost of Veterans Integrated Service Network (VISN); provide healthcare and recover that cost; evaluate fitness for duty and medical concerns which may have resulted from an occupational or environmental hazard; evaluate the Veterans Integrated Service Network (VISN) and its programs; and perform administrative tasks related to Veterans Integrated Service Network (VISN); operations and personnel readiness.

Any protected health information (PHI) in your records may be used and disclosed generally as permitted by the HIPAA Privacy Rule (45 CFR Parts 160) Permitted uses and disclosures of PHI include, but are not limited to, treatment, payment, and healthcare operations.

APPLICABLE SORN: RHSP is not a separate or independent system of records and any PII is covered under the Privacy Act system of records, “Patient Medical Records-VA”, 24VA10A7 or “VistA-VA” 79VA10. Therefore, health record disclosure would not typically be satisfied via this system, but more likely from the source Federal Enclave.

DISCLOSURE: Voluntary. If you choose not to provide the requested information, comprehensive health care services may not be possible, you may experience administrative delays, and you may be rejected for service or an assignment. However, care will not be denied.

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

Yes. However, if individuals choose not to provide the requested information, comprehensive health care coding services may not be possible, patients may experience administrative delays, and patients may be rejected for service or an assignment. However, care will not be denied.

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

Yes, consent is obtained in accordance with all applicable VA privacy regulations. This consent is carried out as part of VISN operations prior to entering data into 360e Genesis, and thereafter into RHSP.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

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

Privacy Risk: Agencies are not open about developments, practices, and policies with respect to the collection, use, dissemination, and maintenance of PII. Sufficient notice is not provided to the individuals.
Mitigation: RHSP is transparent to individual about developments, practices, and policies with respect to the collection, use, dissemination, and maintenance of PII. Sufficient notice is provided to the individuals prior to data collection.

Privacy Risk: Information is not used for the purpose for which notice has been provided directly to the individual. Procedures are not in place to ensure that information is used only for the purpose articulated in the notice.

Mitigation: RHSP Information is used for the purpose for which notice was provided directly to the individual. RHSP has developed procedures to ensure information is used only for the purpose articulated in the notice.
Section 7. Access, Redress, and

Section 7. Access, Redress, and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

7.1 What are the procedures that allow individuals to gain access to their information?

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

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

If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information.
This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

Individuals are provided Privacy Act Statement (PAS) at the time of such collection, prior to data being entered into 360e Genesis.

As the Veterans Integrated Service Network (VISN) medical system will collect PII directly from individuals, it will be required to provide those individuals a Privacy Act Statement (PAS) at the time of such collection.

This statement serves to inform you of the purpose for collecting the personal information required by the Veterans Integrated Service Network (VISN) 360e GENESIS system, and how it will be used.

Legal Authority: Title 38 United States Code (U.S.C), Section 501 and Sections 901–905. The Secretary of Veterans Affairs established these guidelines pursuant to the authorities in and requirements of Title 38, United States Code, section 81 11 (38 U.S.C. 5811 I), titled "Sharing of Department of Veterans Affairs and Department of Defense Health Care Resources," and the

authorities contained under Title 10, United States Code, section 1104 (10 U.S.C.5 1104), titled "Sharing of Resources with the Department of Veterans Affairs," which incorporates Title 31, United States Code, section 1535 (31 U.S.C. 51 535), titled "Agency Agreements," also known as the "Economy Act." These guidelines assist in the implementation of these statutes.

PURPOSE: To collect information to provide and document medical care; determine eligibility for benefits and entitlements; adjudicate claims; determine whether a third party is responsible for the cost of Veterans Integrated Service Network (VISN); provide healthcare and recover that cost; evaluate fitness for duty and medical concerns which may have resulted from an occupational or environmental hazard; evaluate the Veterans Integrated Service Network (VISN) and its programs; and perform administrative tasks related to Veterans Integrated Service Network (VISN); operations and personnel readiness.

Any protected health information (PHI) in your records may be used and disclosed generally as permitted by the HIPAA Privacy Rule (45 CFR Parts 160) Permitted uses and disclosures of PHI include, but are not limited to, treatment, payment, and healthcare operations.

APPLICABLE SORN: RHSP is not a separate or independent system of records and any PII is covered under the Privacy Act system of records, "Patient Medical Records-VA", 24VA10A7 or "VistA-VA" 79VA10. Therefore, health record disclosure would not typically be satisfied via this system, but more likely from the source Joint VA/DOD Federal Enclave.

DISCLOSURE: Voluntary. If you choose not to provide the requested information, comprehensive health care services may not be possible, you may experience administrative delays, and you may be rejected for service or an assignment. However, care will not be denied.

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.

RHSP is a back-end processing system for 360e Genesis. All procedures for correcting inaccurate information are established for the front-end medical systems.

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.

RHSP is a back-end processing system for 360e Genesis. All procedures for correcting inaccurate information are established for the front-end medical systems.

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.

RHSP is a back-end processing system for 360e Genesis. All procedures for correcting inaccurate information are established for the front-end medical systems.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Privacy Risk: Individuals have no right to obtain confirmation from a data controller on whether or not the data controller has any data relating to them.
Mitigation: RHSP individuals are given the right to obtain confirmation from a data controller confirmation on whether or not the data controller has any data relating to them.

Privacy Risk: Data relating to individual is not communicated within a reasonable time. Individuals do not have the right of notice as to why the denial was made and how to challenge such a denial.
Mitigation: RHSP individuals have the right of notice as to why a denial was made and how to challenge such a denial.

Privacy Risk: Systems do not have mechanisms in place through which individuals are able to prevent PII obtained for one purpose from being used for other purposes.
Mitigation: RHSP has mechanisms in place by which individuals are able to prevent PII from being used for other purposes.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 What procedures are in place to determine which users may access the system, and are they documented?

Describe the process by which an individual receives access to the system.

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

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

This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.

Individuals are granted access on a need-to-know basis. Access is granted to the RHSP system after individuals have been vetted according to their roles. Neither customer-facing nor patient access is available for RHSP.

No other agencies have access to RHSP information.

Title	Access Type
RHSP Application Specialists	Read/Write
Linguists	Read/Write

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

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

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

Yes, contractors are given access to the RHSP system after they have been vetted. Contractors are involved in remediation, testing, and patch management. A Non-Disclosure Agreement (NDA) is signed by contractors prior to access to the RHSP system.

Contracts are reviewed according to the specific schedule associated with each contract, by the appropriate VA stakeholders. Contractor access is necessary for configuration and remediation activities. All contractors are subject to background checks and must possess a minimum of Public Trust. No privacy differentiation has been established between different users due to similarities of administrative roles in a production system. VA contractor access to PII is required for system tuning, problem investigation and incident response.

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.

VA annual privacy training is required. Role-based privacy training is required for personnel having access to PII or for activities that involve PII.

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

If Yes, provide:

1. *The Security Plan Status,*
2. *The Security Plan Status Date,*

3. *The Authorization Status,*
4. *The Authorization Date,*
5. *The Authorization Termination Date, .*
6. *The Risk Review Completion Date*
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH).*

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

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

In Process.

OEHRM is working on a FedRAMP ATO (in progress) for RHSP, with target IOC date of early May 2022. The system is not currently in production.

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, 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.

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

The system does not have a FedRAMP authorization but is undergoing assessment at this time. To comply with VA Handbook 6517, RHSP was assessed by a 3PAO. The processes used included FedRAMP and RMF. The documents used included System Security Plan (SSP), FIPS199, CIS/CRM workbook, Information Security Policies (ISP), Rules of Behavior (ROB), IT Contingency Plan (ITCP), Configuration Management Plan (CMP), Incident Response Plan (IRP), E-Authentication Workbook, Privacy Threshold Analysis (PTA), Privacy Impact Assessment (PIA)

9.2 Identify the cloud model being utilized.

Example: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS).

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

The cloud model being utilized is Software as a Service (SaaS).

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

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

RHSP leverages existing contracts and relationships between the VA, Cerner and AWS GovCloud to establish VA ownership rights over data.

9.4 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.

This question is related to privacy control DI-1, Data Quality.

N/A – The system is a back-end processing system, which does not collect ancillary data about users, because users do not directly interact with RHSP.

9.5 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.

CSP uses AWS GovCloud as its cloud provider. Security controls for AWS GovCloud have been independently assessed by the VA for suitability, and this same provider is used by VAEC and other VA services.

9.6 If the system is utilizing Robotics Process Automation (RPA), please describe the role of the bots.

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

N/A. RHSP does not use Robotic Process Automation.

Section 9. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

ID	Privacy Controls
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

Stephania H. Griffin 229066

Digitally signed by Stephania H. Griffin 229066
Date: 2021.10.04 13:58:46 -04'00'

Privacy Officer, Griffin, Stephania

Albertino M. Estacio 119921

Digitally signed by Albertino M. Estacio 119921
Date: 2021.10.07 05:57:05 -07'00'

Information Systems Security Officer, Estacio, Albert

Michael J. Hartzell 3487012

Digitally signed by Michael J. Hartzell 3487012
Date: 2021.10.04 13:50:22 -04'00'

System Owner, Hartzell, Michael

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).

https://www.oprm.va.gov/docs/Current_SORN_List_08_17_2021.pdf