Privacy Impact Assessment for the VA IT System called:

3M RevCycle Health Services Platform (RHSP)

VA Central Offices (VACO)

Electronic Health Record Modernization Integration Office (EHRM-IO)

Date PIA submitted for review:

June 13, 2023

System Contacts:

System Contacts

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

3M RevCycle Health Services Platform (RHSP) is an authorized Federal Risk and Authorization Management Program (FedRAMP) software as a service (SaaS) cloud computing back-end system, owned and controlled by Oracle Health/Cerner and hosted by Amazon Web Service (AWS) GovCloud, supporting key operations offered by the 360 Encompass (360e) front-end residing inside the Federal enclave, including natural language processing (NLP) support for medical coding, clinical documentation integrity, clinician input and medical coding edits, self-service reporting to enable coders gain insights from data without relying on technical skills, evaluation and management.

Overview

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

1 General Description

A. The IT system name and the name of the program office that owns the IT system.
The IT system name is 3M RevCycle Health Service Platform (RHSP). The program office is Electronic Health Record Modernization Integration Office (EHRM-IO)

B. The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.
3M RHSP business purpose is to provide back-end processing for high-quality coding and management of medical care payment activities. This back-end module is not directly accessed by hospitals/medical centers, or regional offices.

C. Indicate the ownership or control of the IT system or project.
The 3M RHSP system is owned by the vendor yet under the control of the VA EHRM-IO. The system operates as one single shared-technology platform serving the organizational users of the Federal EHR.

2. Information Collection and Sharing

D. The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.
3M RHSP stores information for thousands of patients, aligned with front-end 360 Encompass 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.

E. A general description of the information in the IT system and the purpose for collecting this information.

3M 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.

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

3M RHSP operates 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.

G. 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.

3M RHSP is a FedRAMP SaaS, AWS GovCloud-hosted back-end system supporting the front-end 360 Encompass (360e) operation located in the Federal Enclave, a DHA authorized cybersecurity boundary.

3. Legal Authority and SORN

H. A citation of the legal authority to operate the IT system.

The authority for the system to collect, use, and disseminate information about individuals that is maintained in systems of records by federal agencies, in accordance with the code of fair information practices established by the Privacy Act of 1974, as amended, 5 U.S.C. § 552a, are stated in System of Record Notification (SORN) 24VA10A7, Patient Medical Records-VA, dated October 2, 2020, and 114VA10, The Revenue Program-Billing and Collections-VA, dated January 25, 2021. The authority to operate the system is stated in Title 38, United States Code, Sections 501(b) and 304. In compliance with the Federal Information Security Modernization Act of 2014 (FISMA Reform) and VA Directive 6500, VA Cybersecurity Program, published on February 24, 2021, on October 21, 2021, the system was initially authorized to operate (ATO) by the VA Authorization Official (AO) for one year, yet four months later, on February 4, 2022, the VA AO approved a full three-year ATO with authorization termination date (ATD) of February 2, 2025.

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

No amendment or revision of the existing SORN's is needed as part of the system deployment.

D. System Changes

J. Whether the completion of this PIA will result in circumstances that require changes to business processes

No change to business processes is expected once this Privacy Impact Assessment is completed.

K. Whether the completion of this PIA could potentially result in technology changes

No technology change is expected once this Privacy Impact Assessment is completed.

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.

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

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

- ☒ Name
- ☐ Social Security Number
- ☒ Date of Birth
- ☐ Mother's Maiden Name
- ☐ Personal Mailing Address
- ☐ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☐ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☐ Financial Information
- ☐ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers*
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☐ Medications
- ☒ Medical Records
- ☒ Race/Ethnicity
- ☐ Tax Identification Number
- ☒ Medical Record Number
- ☒ Gender
- ☐ Integrated Control Number (ICN)
- ☐ Military History/Service Connection
- ☐ Next of Kin
- ☒ Other Data Elements (list below)

Electronic Data Interchange Personnel Identifier (EDIPI), Death Date, Disability, Living Arrangement, Admit Date, Discharge Date, Disposition, Length of Stay, Patient Type, Past Visit, Patient Key, Patient Enterprise Key, Financial Class, Discharge Status Patient Class, Visit Types, Enterprise Patient Number/Enterprise Patient Identifier (EPN/EPI), Integrated Control Number (ICN)

PII Mapping of Components (Servers/Database)

3M RHSP consists of one (1) key component (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by 3M RHSP 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 the server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

Internal Database Connections

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
Millennium (360e)	Yes	Yes	Name, Birth Date, Race/Ethnicity, EDIPI, EPN/EPI, Death Date, Gender, 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	Natural Language and other data processing for auto code suggestion and data warehousing for reporting.	AES 256 for data at rest and TLS 1.2+ for data in transit

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

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

RHSP collects and processes patient information securely from the Millennium database, passing through its front-end 360 Encompass (360e) application located in the same ATO boundary with the production Millennium, hosted by Oracle Health/Cerner, within the Federal enclave and authorized to operate by the DHA AO. RHSP generates medical diagnosis and procedure code suggestions, once

being processed and determined by coders, would likely become part of a patient electronic health record.

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.

RHSP is the back-end processing that uses data collected by the front-end 360 Encompass to generate medical diagnosis and procedure code suggestions, which may become part of a patient electronic health record.

1.2c If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

RHSP generates medical diagnosis and procedure code suggestions, which may become part of a patient electronic health record.

1.3 How is the information collected?

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

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

The front-end system, 360e, collects patient data directly from the Millennium EHR database via electronic transmission. 360e then transfers data to the back-end RHSP using a secure interface between the VA Data Access Service (DAS) Single Point of Entry (SPOE) and the Federal enclave, passing through the Med-COI network, using Multiprotocol Label Switching (MPLS) layer 3 Virtual Private Network (VPN) incorporated in the Joint Security Architecture (JSA).

1.3b 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.

Not applicable – data is collected electronically.

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

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

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your

organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

Patient data in the Millennium EHR is coming from both data migration of existing/legacy VA system and from new episode of cares of those individual patients who have recently been treated at the five VA sites that have deployed Millennium. Data accuracy is verified by the original source, ie. either the legacy VA systems (via VX130) or by the individual patient with assistance, where needed, of VA healthcare administrative professionals, or directly via the patient portal. To ensure accuracy of data processed by the backend RHSP component, certain workflows have been designed and implemented to periodically refresh data ingested by the front-end 360e. Frequency of update is related to frequency of use by 360e.

1.4b 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.

No commercial aggregator is used in 3M RHSP.

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 authority for the system to collect, use, and disseminate information about individuals that is maintained in systems of records by federal agencies, in accordance with the code of fair information practices established by the Privacy Act of 1974, as amended, 5 U.S.C. § 552a, are stated in System of Record Notification (SORN) 24VA10A7, Patient Medical Records-VA, and 114VA10, The Revenue Program-Billing and Collections Records-VA. The authority to operate the system is stated in Title 38, United States Code, Sections 501(b) and 304. In compliance with the Federal Information Security Modernization Act of 2014 (FISMA Reform) and VA Directive 6500, VA Cybersecurity Program, published on February 24, 2021, 3M RHSP has received an initial one-year ATO decision, made by the VA AO, in Oct 2021 and a full three-year ATO in February 2022. The Authorization Termination Date is February 2, 2025

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: A risk may arise should the purpose(s) and relevancy of PII collection are not clearly specified.

Mitigation: RHSP only collects data elements deemed relevant to the system design approved by VA EHRM-IO. RHSP data is transmitted from 360e Genesis, which collects data in a manner approved by the VA. The principles of purpose specification and minimization are followed by the source system, i.e. the front-end 360 Encompass residing in the Federal EHR system. The purposes of PII collection are disclosed and communicated directly to individual patients.
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 to the system.

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 – 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 is 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 – 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?
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 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.

2.2b 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.

Yes. RHSP generates medical code suggestions based on the information transmitted from the front-end 360 Encompass system in supporting of health care billing processing.

2.3 How is the information in the system secured?

These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

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

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.

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

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

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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.

2.4a How is access to the PII determined?

Access to PII is determined based on the need to manage, optimize, or respond to RHSP requirements or events.

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

The criteria, procedures, controls, and responsibilities for access into the AWS GovCloud are well-documented. RHSP access is limited to personnel who have been trained, vetted, and cleared via the Customer Agency personnel security process. Personnel need to be able to successfully attain a Public Trust clearance, and complete training for Security Awareness and HIPAA, as required for personnel supporting the program.

2.4c Does access require manager approval?

AWS GovCloud access is restricted via multiple levels of authentication, secure protocols, and management approval.

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

RHSP monitors, tracks, and records user access and other user activities involved PII. All access to PII is monitored, tracked, recorded, and logged using account authentication, access logs and Security Information Event Management (SIEM) tools such as 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.

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

The System Owner is ultimately responsible for assuring safeguards for the PII collected by and stored in the system. 3M contractors, subjected to binding under Non-Disclosure Agreement. Are responsible for the design and maintenance of the system.

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*

Information with specific elements as listed in 1.1 and 2.1 is collected and processed by RHSP. 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. Retention of records is performed by the front-end 360e system, as a sub-component of Millennium, which retains the full health records of VA patients.

3.2 How long is information retained?

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

The retention period for VA sensitive information processed by and stored in RHSP is 5 years, according to item 4000.1b of the VHA Records Control Schedule (RCS) 10-1 for "Financial Transaction Records Related to Procuring Goods and Services, Paying Bills, Collecting Debts, and Accounting." (https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf)

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

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

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

Yes, all records stored within this Back-end system are identified and categorized using the guidance provided by RCS.10-1 at the following link https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

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

The data processed and retained by RHS is categorized as financial transaction records. Therefore, in accordance with VA/VHA Record Control Schedule RCS 10-1 published in January 2021, chapter 4 – Finance Management, series 4000 - Financial Management and Reporting Records, item 4000.1b, these financial records are retained for five (5) years. The said chapter/series is part of the National

Archives and Records Administration (NARA) General Records Schedules (GRS), which provides disposal authorities for temporary administrative records common to all U.S. Federal agencies. The RCS 10-1 (https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf) is the main authority for the retention and disposition requirements of VHA records, and also provides the NARA disposition authorities or the GRS authorities, whichever is appropriate for the records, in addition to program and service sections.

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.

As RHSP is a back-end processing system, data is regularly overwritten in service of electronic transmissions from 360e data storage and overwrite requests. Routine information disposal is achieved by overwriting data. In the case of system decommissioning, data undergoes secure disposal in line with VA Directive 6500, VA Cybersecurity Program, NIST SP 800-88 rev.1 guidelines, and AWS GovCloud data destruction procedures. This typically involves the shredding of hard drives. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destruction.

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.

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

3.6 <u>PRIVACY IMPACT ASSESSMENT: Retention of information</u>

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

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

PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

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

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

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

Follow the format below:

Privacy Risk: The information system may retain more data than 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

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Office of Information and Technology (OI&T)/ Data Access Services (DAS) Cloud	Revenue cycle solution to process, enrich, and enhance medical coder productivity in health information management	Name, Birth Date, Race/Ethnicity, EDIPI, EPN/EPI, 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	Hypertext transfer protocol secure (HTTPS)/ Transport Layer Security (TLS) 1.2, via Joint Security Architecture (JSA)

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: 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 ensures 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 3.10 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 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 processed (shared/received/transmitted) 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***
Defense Healthcare Management System Modernization (DHMSM) EHR Core/Federal	Revenue cycle solution to process, enrich, and enhance medical coder	Name, Birth Date, Race/Ethnicity, EDIPI, EPN/EPI, Death Date, Gender, Disability, Living Arrangement, Admit Date, Discharge Date, Disposition, Length of Stay, Patient Type, Account Numbers (Medical	a) MOU/ISA between Oracle Cerner and VA OI&T DAS Cloud 4/2023- b) DoD/VA MOA for Implementation	HTTPS/TLS 1.2 via JSA

enclave/ 360 Encompass	productivity in health information management	Account Number), Past Visits, Patient Key, Patient Enterprise Key, Financial Class, Discharge Status, Patient Class, Visit Types	of the Medical Community of Interest (Med-COI) network, 11/2019	

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: VA patient data is now collected and retained in a shared database as part of the Federal EHR may expose to certain privacy/security risks such as unauthorized access or being used for purposes other than the stated purpose and use of the original collection.

Mitigation: Beside the 2014 MOU signed between the then-Secretaries of DoD and VA, the two agencies have entered into several inter-agency MOA, MOU/ISA, in line with the RMF and applicable OMB Memoranda, CNSSI, DoD and VA policies and procedures to ensure data safeguarding and information privacy controls are implemented as having designed to prevent and/or detect violation or compromise situations, maintaining an acceptable risk level for the operating systems, both in Prod and Pre-Prod environments.

Section 6. Notice

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

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

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

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

RHSP is a back-end system, which does not collect information directly from individuals. The source of VA data fed in RHSP is coming from the Millennium database residing in the Federal enclave. With reference to the "Notice" requirements, beside the publication of SORN 24VA10A7, Patient Medical Records-VA, (https://www.oprm.va.gov/docs/SORN/Current_SORN_List_07_06_2023.pdf) in the Federal Register as having mentioned in 1.5 as well as the Helpful Links section following Appendix A, the current publication of the VHA Notice of Privacy Practices (NOPP) can be found in the VHA webpage, http://www.va.gov/health/, under the "Resources" section. A copy of the NOPP must be provided to a patient/Veteran in person when they present for services. Alternatively, a copy of the revised/latest NOPP will be mailed to eligible veterans every 3 years by the VHA.

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

The latest publication of the VHA Notice of Privacy Practices (NOPP) can be found in the VHA webpage, http://www.va.gov/health/, under the "Resources" section. All users of the MyHealtheVet patient portal can also access the same NOPP publication when logging in their account in the portal. A copy of the NOPP must be provided to a patient/Veteran in person when they present for services. Alternatively, a copy of the revised/latest NOPP will be mailed to eligible veterans every 3 years by the VHA.

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

VHA is required by law to maintain the privacy of Veterans/patients protected health information and to provide the Veterans/patients with notice of VHA legal duties and privacy practices. Beside the publication of the System of Record Notice in the Federal Register, the VHA Notice of Privacy Practice outlines the ways in which VHA may use and disclose Veterans/patients health information without their permission as required or permitted by law. For VHA to use or disclose Veterans/patients health information for any other purposes, VHA is required to get the Veteran's/patient's permission in the form of a signed, written authorization. The latest NOPP digital publication can be found in the Resources section of the VHA webpage (http://www.va.gov/health/) A copy of the NOPP must be provided to a patient/Veteran in person at the time they are admitted for services at a VHA health care facility. Alternatively, a copy of the revised/latest NOPP will be mailed to eligible veterans every 3 years by the VHA.

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.

To apply for enrollment in the VA health care system, all Veterans are required to fill out VA Form 10-10EZ. The information provided on this form will be used by VA to determine eligibility for medical benefits. The applicant is not required to disclose their financial information; however, VA is not currently enrolling new applicants who decline to provide their financial information unless they have other qualifying eligibility factors. If a financial assessment is not used to determine the applicant's eligibility for cost-free medication, travel assistance or waiver of the travel deductible, and the applicant chooses not to disclose personal financial information, the applicant will not be eligible for these benefits. More details and instruction for VA Form 10-10EZ can be found through the Resources section of the VHA webpage at va.gov/health/ or at this link https://www.va.gov/vaforms/medical/pdf/VA_Form_10-10EZ.pdf. Veterans/patients have the opportunity to decline the use or disclosure of their health information by "opting-out" of listing in the Patient Directory at the time being admitted to a VHA health care facility. Veterans/patients can revoke, in writing, at any time, the authorization to use or disclose of their health information, unless the use or disclosure falls under one of the exceptions described in the said NOPP or as otherwise permitted by other laws.

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.

Right to Request Restriction: Veterans/patients do have the right to request that VHA not use or disclose all or part of their health information to carry out treatment, payment or health care operations, or that VHA not use or disclose all or part of their health information with individuals such as their relatives or friends involved in their care, including use or disclosure for a particular purpose or to a particular person. Reference the NOPP on how to submit a request for restriction. VHA, however, as a "Covered Entity" under the law, is not required to agree to such restriction, except in the case of a disclosure restricted under 45 CFR § 164.522(a)(1) (vi). This provision applies only if the disclosure of the Veteran's or patient's health information is to a health plan for the purpose of payment or health care operations and the Veteran's health information pertains solely to a health care service or visit which is paid out of pocket in full by the Veteran/patient. However, VHA is not legally able to accept an out-of-pocket payment from a Veteran for the full cost of a health care service or visit. The Administration can only accept payment from a Veteran for co-payments. Therefore, this provision does not apply to VHA and VHA is not required or able to agree to a restriction on the disclosure of a Veteran's/patient's health information to a health plan for the purpose of receiving payment for health care services provided by VHA. Additionally, VHA is not

able to honor requests to remove all or part of a patient health information from the electronic database of health information that is shared between VHA and DoD, or to restrict access to the patient health information by DoD providers with whom the patient has a treatment relationship.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

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

Privacy Risk: A risk may arise due to notice of data collection and privacy practice is not provided timely and/or sufficiently to the individuals of whom PII is collected. There may also be a risk to individuals of the entity collecting PII does not have relevant controls or procedures in place to ensure the purpose(s) of use are strictly followed.

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. RHSP has developed procedures to ensure information is used only for the purpose articulated in the notice.

Section 7. Access, Redress, and Correction

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

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

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

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

As having stated in the VHA NOPP, Veterans/patients have the right to review and obtain a copy of their health information by means of completing VA Form 10-5345a – Individuals' Request for a Copy of their Own Health Information, to the facility Privacy Officer of the VHA facility that provided or paid for their care. Form 10-5345a can be obtained from the facility webpage or the VA online repository at the link https://www.va.gov/find-forms/about-form-10-5345a. Additionally, Veterans/patients can gain access to their health record by enrolling in the VA patient portal, myHealtheVet, at https://www.myhealth.va.gov/index.html

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).

This system is not exempt from the access provisions of the Privacy Act.

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.

Not applicable. This is a Privacy Act system.

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.

Right to Request Amendment of Health Information: Veterans/patients have the right to request an amendment (correction) of their health information in Federal EHR records if they believe it is incomplete, inaccurate, untimely, or unrelated to their care. A request in writing must be submitted to the facility Privacy Officer, specifying the information to be corrected, including a reason to support the request for amendment. Reference the VHA NOPP, which can be found in the Resources section of the VHA webpage (http://www.va.gov/health/). Alternatively, a copy of the revised/latest NOPP will be mailed to eligible veterans every 3 years by the VHA.

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.

The NOPP, outlining the procedure for Veterans/patients request amendment (correction) of their health information, is provided to the Veteran/patient at the time their information being

collected and subsequently each time they are admitted for care service. If they enroll in the patient portal, a digital version of the NOPP is also available for their awareness. Alternatively, a copy of the latest NOPP will be mailed to all eligible veterans every 3 years by the VHA. Veterans/patients are expected to review and understand the said procedures as well as the NOPP in its completeness, so that they can properly exercise their rights. Particularly, the procedures also address the situation when a request for amendment is denied - Veterans/patients will be notified of such decision in writing and given information about their right to appeal the decision. In response, the Veterans/patients may do any of the following: file an appeal, file a "Statement of Disagreement" which will be included in their health record, or ask that their initial request for amendment accompany all future disclosures of the disputed health information. Reference the VHA NOPP, which can be found in the Resources section of the VHA webpage (http://www.va.gov/health/).

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems. ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

The processes outlined in 7.2 and 7.3 are considered formal redress process. To ensure data accuracy and maintain quality of care, patients are encouraged to actively review and verify information included in their health records.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

Privacy Risk: Individuals whose records contain incorrect or out-of-date information may be exposed to the risk of not receiving prescription medications, notification of appointments, or test results timely. Certain incorrect information in a patient medical record could result in improper diagnosis and treatments.

Mitigation: Various accuracy checks are designed and implemented in different workflows of Millennium and EHR Core, where the front-end 360e system resides and considered a component of. VHA built-in procedure requires staff verify information in patient medical records and correct information identified as incorrect during each patient's medical appointments. Staff are informed of the importance of maintaining compliance with VA Request of Information policies and procedures and the importance of remaining alert to information correction requests.
Individual patients have the right to request an amendment (correction) to their health information in VHA records if they believe it is incomplete, inaccurate, untimely, or unrelated to your care. The individuals must submit request in writing, specify the information that they want corrected, and provide a reason to support their request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains the patient's information or health records. Reference "Right to Request Amendment of Health Information" under VHA Notice of Privacy Practices (NOPP) (https://www.va.gov/health/)

Section 8. Technical Access and Security

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

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

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

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

The criteria, procedures, controls, and responsibilities for access into the AWS GovCloud are well-documented. RHSP access is limited to personnel who have been trained, vetted, and cleared via the VA EHRM-IO personnel security process. Personnel need to be able to successfully attain a Public Trust clearance, and complete VA Security & Privacy Awareness and HIPAA, as mandated by VA Directive 6500, for personnel supporting the program.

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?

For the back-end RHSP system, no users from other (U.S. Federal) agencies can access the system. AWS GovCloud access is restricted via multiple levels of authentication, secure protocols, and management approval. The front-end 360e application is indeed considered a DHA system hence certain system admin functions maybe accessed by DHA/DHMSM personnel, including LPDH personnel, other than Oracle Cerner personnel.

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.

Application specialists, linguists, or users performing administrative tasks related to Veterans Integrated Service, are example of user roles with access to data in the back-end system.

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.

As a back-end system owned and operated by Oracle Health/Cerner, in partnership with 3M, all functions of the system are run by personnel of these sub-contractors. 3M specialists are responsible for the design and maintenance of the system. All contractor and sub-contractor personnel have to complete a Non-Disclosure Agreement (NDA), pass a Public Trust clearance, and complete VA mandate Security & Privacy Awareness Training, including HIPAA Compliance course, before receiving approval to access VA data in the system.

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.

All RHSP users must read and acknowledge the VA general Rules of Behavior (ROB) pertaining to everyday behavior expected of Organizational Users, prior to gaining access to any information system processing VA sensitive information. The rules are included as part of the annual VA Privacy and Information Security Awareness and Rules of Behavior (WBT) course, ID# 10176, which all VA network authorized users must complete via the VA's Talent Management System (TMS). After the user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the renew/refreshing privacy and security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system. The 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. System administrators are required to

complete additional role-based training. Additionally, these users also need to complete course ID# 10203, HIPAA and Privacy training annually since they will heavily access to PHI in the Millennium system in particular, and the Federal EHR system in general. The curriculum of TMS courses identified and assigned to a user by the URA process is to address different purposes other than privacy awareness & training.

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

Yes, A&A has been completed for the system.

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* Jan 27, 2022
3. *The Authorization Status:* Authorized
4. *The Authorization Date:* Feb 2, 2022
5. *The Authorization Termination Date:* Feb 2, 2025
6. *The Risk Review Completion Date:* Feb 1, 2022
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* MODERATE

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

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

N/A

Section 9 – Technology Usage

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

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

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

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1*. (Refer to question 3.3.1 of the PTA)*

Under VA EHRM-IO sponsorship, RHSP received FedRAMP authorization on May 12, 2022, as a Moderate risk - Software as a Service (SaaS) cloud model and can be deployed in Government Community Cloud environments. The 3M SaaS instance is deployed in AWS GovCloud IaaS.

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

A Memorandum of Understanding and Interconnection Security Agreement (MOU/ISA) signed on April 25, 2023, between the VA DAS Single Point of Entry Enterprise Cloud (DAS SPOE VAEC), owned or leased by VA, and the 3M RevCycle Health Service Platform/3M 360 Encompass (RHSP/360e), owned or leased by Oracle Cerner Corporation utilizing a subcontracting relationship with 3M Corporation, and encompassed within a Department of Defense/Department of Health Administration (DOD/DHA) certification boundary. 3M Corporation, the Cloud Service Provider (CSP) owning RHSP the FedRAMP-authorized SaaS cloud solution, is not a party of this MOU/ISA. Even though the said MOU/ISA does not explicitly include a provision to address VHA ownership of the VA sensitive information, including PII/PHI that RHSP collects, processes, and retains, HIPAA Privacy Rule, 45 Code of Federal Regulations (C.F.R.) Part 164, Standards for Privacy of Individually Identifiable Health Information, was listed in the Authority section of the said MOU/ISA. As a result, this means the scope and provisions of the Subcontractor Business Associate Agreement (BAA) between EHRM-IO and Oracle Cerner, signed on March 13, 2018, are applicable in this system interconnection. Furthermore, as Cerner Oracle indicates "a subcontracting relationship with 3M Corporation" has been established, 3M Corp, implicitly, a sub-contractor to Oracle Cerner, must fully comply with the flown down provisions of the said March 2018 Sub-Contractor BAA.

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.

No ancillary data is collected by either the CSP or RHSP since this is a back-end module without direct interaction with patients/individuals.

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.

As Sub-Contractors and Business Associates of the VA EHRM-IO (Business Associate) and VHA (Covered Entity, data owner), both Oracle Health/Cerner and 3M Corporation must meet the same cybersecurity standards applied to VA/VHA to ensure adequate safeguarding mechanisms, particularly the set of NIST SP 800-53 Rev.4 (soon will be Rev.5) security and privacy controls are in place, to protect VA sensitive information held by their systems. This principle has been described in Contracts, Performance Work Statements (PWS's), Task Orders, Business Associate Agreements (BAA's), and Memorandum of Understanding/Interconnection Security Agreements (MOU/ISA's), etc.

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

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

The system does not utilize Robotics Process Automation (RPA).

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**

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: 2023.08.01 15:35:05 -04'00'

Privacy Officer, Stephania Griffin

Albertino M. Estacio 119921

Digitally signed by Albertino M. Estacio 119921
Date: 2023.07.26 09:26:49 -07'00'

Information Systems Security Officer, Albert Estacio

MICHAEL HARTZELL

Digitally signed by MICHAEL HARTZELL
Date: 2023.07.21 16:10:43 -04'00'

Information Systems Owner, Michael Hartzell

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).

The current version of the VHA Notice of Privacy Practices (NOPP) can be found in the VHA webpage, http://www.va.gov/health/, under the "Resources" section. The link to the FR publication of SORN 24VA10A7, Patient Medical Records – VA, https://www.oprm.va.gov/docs/SORN/Current_SORN_List_07_06_2023.pdf , can also be found in the Helpful Link section in the next page.

HELPFUL LINKS:

SORN 24VA10A7, Patient Medical Records-VA:

https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

Record Control Schedules:

https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

General Records Schedule 1.1: Financial Management and Reporting Records (FSC):

https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

National Archives (Federal Records Management):

https://www.archives.gov/records-mgmt/grs

VHA Publications:

https://www.va.gov/vhapublications/publications.cfm?Pub=2

VA Privacy Service Privacy Hub:

https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices