Privacy Impact Assessment for the VA IT System called:

Health Information Gateway and Exchange (HINGE)

Veteran's Health Administration (VHA)

National Radiation Oncology Program (NROP)

Date PIA submitted for review:

August 30, 2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Margaret (Peggy) Pugh	Margaret.Pugh@va.gov	(202) 731-6843
Information System Security Officer (ISSO)	John. D. Mills	john.mills4@va.gov	415-221-4810 x25990
Information System Owner	Tony Sines	Tony.Sines@va.gov	(316) 249-8510

Abstract

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

Health Information Gateway and Exchange (HINGE) is a data abstraction, aggregation, storage and analysis platform for the radiation oncology domain. Web based forms allow clinicians to record radiotherapy specific details as well as get access to existing patient history from Vista. HINGE also has a data analysis dashboard that shows Quality Measure data based on delivered treatments.

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.

Health Information Gateway and Exchange (HINGE) - National Radiation Oncology Program (NROP)

B. The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.

High quality patient care is important to any medical discipline but is of particular concern in radiation oncology given the potential for serious harm in the event of a treatment-related error. Radiation treatment planning is a very complicated process with many safety aspects involved and with the increased application of more sophisticated technologies in radiation therapy, concerns have arisen about whether radiation is being used appropriately. Quality-assurance procedures must evolve with complex radiotherapy planning and delivery systems in order to ensure that consistently effective and safe therapy is delivered. The Veterans Health Administration (VHA) concurred with the Office of Inspector General (OIG) Health Inspection report, dated March 10, 2011, that there was a need for a robust physician peer review process related to all VHA radiotherapy programs. To measure quality of care and service rendered to Veterans, the VHA National Radiation Oncology Program (NROP) office established the VA Radiation Oncology Quality Surveillance (VA-ROQS) and Peer Review program.

The purpose of HINGE is to provide a state-of-the-art system for the recording and aggregation of radiotherapy related data. By using web-based forms integrated with Vista, Treatment Management System (TMS) and Treatment Planning Systems (TPS), HINGE provides a single consistent method for accessing radiotherapy treatment information. This platform also includes a dashboard which aids in the Quality Measure (QM) and Quality Assurance (QM) of treatments based on prior treatments.

Using web API calls, HINGE accessing Vista data from the 41 VA facilities that provides radiotherapy services in-house which allows for the end users to receive patient history information and submit completed Text Integration Utilities (TIU) notes back to Vista. The

submission of notes to Vista is performed using a Security Token Service (STS) token generated from the end user's Single Sign-On (SSO) verification using their Personal Identity Verification (PIV) based authentication. Each treating facility has a HINGE-Broker service that allows for the HINGE platform to query for Treatment Management and Treatment Planning Systems technical treatment information that is not available in Vista. The connection from the local HINGE-Broker services to the HINGE platform is point-to-point only and uses Secure Sockets Layer (SSL) encrypted communication.

C. Indicate the ownership or control of the IT system or project.

The Health Information Gateway and Exchange (HINGE) platform was developed and solely owned by the National Radiation Oncology Program office at the Department of Veterans Affairs.

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.

HINGE will be used for the recording and aggregation of radiotherapy related data for the 15,000 estimated veterans treated with radiotherapy at the VA each year. HINGE will also share consult request data with community care providers using the approved Box.com platform as well as receive treatment completion data for up to 25,000 veterans per year. Data from each veteran's treatment will remain with HINGE for the life of the project to allow for practice assessment and to aid in the treatment of a secondary cancer diagnosis in the future. The total number of veterans in HINGE will increase by an estimated 40,000 per year.

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

Patient history information such as labs, problem list, vitals, allergies, and prior TIU notes will be interfaced from the active EMR (Vista or Cerner) to partially complete the web based forms in HINGE. Discrete data elements selected by the physician and their free text narratives will also be stored as well as the final full text note that will be sent back to the EMR.

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

HINGE as a community care dashboard which helps to facilitate the consult request process with outside providers as well as receive treatment completion information from veterans treated outside of the VA. All data transfer uses the VA's approved Box.com platform as defined by their FedRAMP. HINGE also shares radiation treatment information to the VA's VINCI platform as defined by their ATO.

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.

HINGE will be used across all 41 VA facilities that treat radiation in-house. HINGE is deployed on the VAEC AWS so all data is stored on the same cloud based resources. Across the enterprise, access to the HINGE application required a valid PIV card and access permissions and roles are managed by HINGE admin team. Access to the VAEC AWS IT resources used by HINGE require an elevated privileged Non-Mail Enabled Account (NMEA) account and secure key fob.

3. Legal Authority and SORN

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

Title 38, United States Code, Sections 501(b) and 304

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?*

HINGE currently has an active authorization to operate (ATO). A SORN exists for this type of system: Patient Medical Records-VA [24VA10A7/ 85 FR 62406] https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf. There is no modification to this SORN for the HINGE application.

D. System Changes

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

No change in business processes will result from the completion of this PIA

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

No change in technology will result from the completion of this PIA

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)

- Veterans or dependents: Previous medical records:
  - Vitals (BP, weight, height, pulse, etc.)
  - Surgical reports
  - Pathology reports
  - Radiation therapy treatment information (treatment dates, delivered dose, treatment plan details)
  - Lab results
  - List of medication
  - Prior encounter notes
  - DICOM/DICOM-RT (embedded tags can include name, treatment date, treatment facility, physician name, etc.)
- VA Employees and VA Contractors:
  - Name
  - Role
  - Facility ID

PII Mapping of Components (Servers/Database)

HINGE consists of one key component (database). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by HINGE 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
MongoDB	Yes	Yes	• VA employee/Contractor Name • Role • Facility ID • Patient Name, Date of birth, gender, race • Integration Control number, EDIPI	Clinical data required for managing treatments	Encryption, SSO based access tokens

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?

HINGE retrieves information from Vista related to each veteran's cancer treatment which is required for clinical use. Discrete technical treatment information from the facility specific Treatment Management Systems (ARIA/Mosaiq) is also retrieved which is not available through Vista. Imaging and radiotherapy-based information in the Digital Imaging and Communications in Medicine (DICOM) format (DICOM Treatment Plan, Dose, Structure set, Images) is also stored for extracting clinically relevant data elements and Quality Measure analysis. Clinical notes completed in the HINGE web forms are also submitted back to Vista so that they can be used for future care.

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.

In addition to the data collected directly related to the patient, HINGE also collects some information about the community care providers. This information is used by the NROP staff to know which providers are serving veterans and their level of clinical staffing and technical qualifications. The clinical information about the patient's health condition, medication, labs, and treatment protocols, progress is stored in the VISTA system. HINGE collects this information from the VISTA system with the purpose to measure quality of care and service rendered to Veterans.

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

HINGE creates TIU notes that will be submitted to Vista based on the data originally collected from Vista as well as the data directly entered by the physician.

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?

Vista – HINGE uses the existing web Remote Procedure Call (RPC) based API calls using VA's SSOi system for requesting data and submitting notes with Vista.
Treatment Management System (TMS) Data – Using a subscription-based methods, HINGE receives updated TMS data from the local TMS commercial software (ARIA, Mosaiq) through their HINGE-Broker over a secure and encrypted SSL connection.

Treatment Planning System (TPS) Data – Using existing tools in their commercial TPS software, users export DICOM files (images, dose, etc.) through the local HINGE-Broker which then send the data to HINGE over the secure and encrypted SSL connection.

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.

The system does not collect data in a paper form.

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.

All data templates and elements are reviewed and analyzed for completeness and accuracy by VA Radiation Oncology clinicians and staff. If necessary, the Radiation Oncology clinicians and staff can resolve ambiguities in the clinical note templates within the HINGE application.

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.

The system does not check for accuracy by accessing a commercial aggregator of information.

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 HINGE application is run as part of the National Radiation Oncology Program's project called VA-Radiation Oncology Quality Surveillance (VA-ROQS). The Veterans Health Administration (VHA) concurred with the Office of Inspector General (OIG) Health Inspection report, dated March 10, 2011, that there was a need for a robust physician peer review process related to all VHA radiotherapy programs. The VA-ROQS program gives VA centers providing in-house radiation oncology care the capability to seek prospective physician peer reviews online. The capability enables VA radiation oncologists to consider treatment refinements and alternatives prior to radiation delivery for the safety of Veterans. Legal authority from the SORN: Title 38, United States Code, Sections 501(b) and 304 is Patient Medical Records-VA [24VA10A7/ 85 FR 624]

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:

<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: VA radiation oncology physicians and staff will have access to the patient's health information and will be able to add additional clinical notes via the HINGE clinical note templates. Privacy risk would be with improper access and unauthorized access to the HINGE data for users and improper disclosure of the patient's data by staff that have access to HINGE.

Mitigation: Any access to the HINGE application will be via the VA's secure single sign on authentication and authorization services. All access to the HINGE application will be managed from the VA's user provisioning services via Electronic Permissions Access System (EPAS) tickets.

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.

Radiation treatment planning is a very complicated process with many safety aspects involved. With the increased application of more sophisticated technologies in radiation therapy, concerns have arisen about whether radiation is being used appropriately. Peer review of the treatment plans will help ensure high quality treatment and safer practices which will benefit Veterans undergoing cancer treatment. The absence of such a program can result in unwanted complications and poor outcomes for patients.

There is not currently an IT solution in place to conduct prospective peer review and capture quality data remotely or across the enterprise. This proposed solution will consist of an intranet-based peer review and quality surveillance capability accessible to all VA Radiation Oncology clinics that enables VHA radiation oncologists to seek treatment plan peer reviews on demand and capture quality data in the background. This quality surveillance tool will have the capability to interface with the Vista / Computerized Patient Record System (CPRS) VA Electronic Medical Record (EMR) systems.

HINGE application aggregates data from multiple sources (Vista, TMS, TPS) to make the creation of clinical notes easier, consistent, and less error prone. HINGE also uses collected treatment data for performing data analysis to guide practice improvements including name, date of birth, current medication, previous medical records, race/ethnicity, medical record number, gender, Integration Control Number (ICN), military history/service connection, and DICOM based information.

Patient Name, date of birth, Gender. Medical Record Number (Integration Control Number – VistA, EDIPI (Cerner): is being used to identify the correct patient record is opened in the HINGE system for the clinician to perform their clinical data analysis.

Previous Medical Records, Medications, Race: is being used by the clinicians to access the pre-treatment characteristics of the patients and recommend treatment course and perform patient management tasks within the HINGE system.

VA employee and Contractor name, role and facility ID: is being used to create an account in the HINGE system and the software to identify the user, their facility role (clinician, physicist, therapists, etc.) and the facility ID for the HINGE system to link the user's profile with the specific VA facility.

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.

HINGE calculates Quality Measure scores from the collected data elements using physician defined decision trees. Some of these Quality Measures are also based on Dose Volume Histograms (DVH) which are derived from the DICOM dose and structure set files. These Quality Measure scores are then presented to VA physicians and quality managers through the dashboard component of HINGE for further analysis.

The generated Quality Measure and DVH information will be stored on the HINGE platform to help each facility to improve their practice. This data will not be added to the official health record on the EMR but will be presented on the HINGE dashboard component. Each treating facility will have access to the data they created as well as aggregated results across the entire VA system. The NROP will have access to each facility's data for the purpose of oversight and providing guidance with practice improvement.

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.

The HINGE software is not designed to create any new information about an individual the deviates from the workflow defined in the software. All the information created from the HINGE software will be always accessible by Government employees.

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 data in transit is protected via the SSL certificates. Data at rest will be encrypted with the keys stored in the AWS Key Management Service (KMS) and all AWS services used by HINGE are Federal Information Processing Standard FIPS 140-2 compliant (FIPS - Amazon Web Services (AWS)).

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

We do not collect patient SSNs in the HINGE application. Patient identification is instead performed using the Integration Control Number (ICN) with Vista and the Electronic Data Interchange Personal Identifier (EDIPI) with Cerner.

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

Stored and transmitted PII/PHI is safeguarded with encryption and no data leaves VA controlled environments. To protect Veteran personally identifiable information (PII) the following activities occur as part of the overall information assurance activities:
1. The information with each application is categorized in accordance with FIPS 199 and NIST SP 800-60. As part of the categorization any PII is identified.
2. The VA has policies which direct and guide the activities and processes performed by the VA. The policies are periodically reviewed to ensure completeness and applicability.
3. The NIST SP 800-53 controls are selected based on the categorization. The controls provide protection for veteran PII while, used developed or stored by an application or IT system, physically transported, between facilities, least privilege, stored offsite, or transmitted between IT centers.
4. Internal protection is managed by access controls such as user IDs and passwords, two-factor authentication, in addition: awareness and training, encryption, auditing, and internal network controls. Remote protection is provided by remote access control, authenticator management, audit, and encrypted transmission.

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?

PII data will be used in the HINGE software for user account management. Access to HINGE is based on VA approved users via the Active Directory (AD) provisioning system and a successful Single Sign On Internal (SSOi) login via PIV cards. Any employee who has an active VA active directory account can request for an account to be created in HINGE. The HINGE system administrator is responsible to grant access to VA users after verifying the bonified need for accessing the system.

Users attempting to access the HINGE application will first encounter a landing page requiring a PIV based SSOi login. After the user logs in via their PIV card and is authenticated by the SSOi system, the HINGE database will verify that specific user has been granted access to HINGE and their associated user role. For users who have not been onboarded / registered with the HINGE system, the software will reroute them to a web page where they can request access to HINGE. With this request an email is sent to the HINGE system administrator group at the National Radiation Oncology Program (NROP) office who will approve or deny access based on the review of bonified need. If the request is denied, the users will receive an email notification and will not be granted access to access the HINGE software. Approved users will have an entry with their name, Integration Control Number (ICN) and VA email address added in the HINGE database for future verification. The HINGE system administrator can also remove users who no longer should have access to HINGE.

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

Yes, we have a sharepoint site where users can request access to the HINGE software by filling in the access request form. We have a document detailing the procedure, controls, and responsibilities for access control.

2.4c Does access require manager approval?

Yes, access to HINGE requires manager approval.

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

HINGE has internal audit logs of the users who have logged into the software, performed various activities and accessed the templates in the software that include access to the PII data.

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

The system owner, business owner and HINGE system administrator are responsible for assuring safeguards are in place for inappropriate disclosure of PII.

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*

All the below mentioned list of data elements are retained by the HINGE system:

Name, Date of birth, Medications, Medical Records, Race, Next of Kin, Military Service connection, Medical Record number, Gender, Other Data Elements listed below:

- Veterans or dependents: Previous medical records:
  - Vitals (BP, weight, height, pulse, etc.)
  - Surgical reports
  - Pathology reports
  - Radiation therapy treatment information (treatment dates, delivered dose, treatment plan details)
  - Lab results
  - List of medication
  - Prior encounter notes
  - DICOM/DICOM-RT (embedded tags can include name, treatment date, treatment facility, physician name, etc.)
- VA Employees and VA Contractors:
  - Name
  - Role
  - Facility ID

3.2 How long is information retained?

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

These records are retained and disposed of after 75 years after the last episode of patient care in accordance with the National Archives and Records Administration Schedule 10-1, item number 6000.2 - Electronic Health Record (EHR) (Records Control Schedule 10-1 (va.gov))

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?

These records are retained and disposed of after 75 years after the last episode of patient care in accordance with the National Archives and Records Administration Schedule 10-1, item number 6000.2 - Electronic Health Record (EHR) (Records Control Schedule 10-1 (va.gov))

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

These records are retained and disposed of after 75 years after the last episode of patient care in accordance with the National Archives and Records Administration Schedule 10-1, item number 6000.2 - Electronic Health Record (EHR) (Records Control Schedule 10-1 (va.gov))

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.

Electronic copy of the records will be purged from the database and media after 75 years after the last episode of patient care. In accordance to VA directives 6500 and Section 6000.1 (d) and the Records Control Schedule 10-1 (Records Control Schedule 10-1 (va.gov)).

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.

HINGE has a testing/ development infrastructure platform deployed on the VA-Enterprise cloud and this environment does not have any PHI/PII elements.

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. (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: Data could be compromised at rest.

Mitigation: Medical record data must be kept for 75 years after the last treatment as described by the VA's Record Control Schedule 10-1, Section 6000.1 (d). To address potential privacy risks, this data will remain encrypted at rest on a VA controlled cloud drive until its scheduled date of destruction. Data storage and backups will be with the encrypted Elastic File System (EFS) and Simple Storage Service (S3), both FIPS 140-2 compliant (FIPS - Amazon Web Services (AWS)).

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
VA Informatics and Computing Infrastructure (VINCI)	Provide radiation oncology data currently not available in the CDW	Radiotherapy Treatment delivery data – Dose, fraction, DICOM and clinical data elements	Remote SQL insertion in the VINCI staging database
VHA VistA	To abstract clinical information from the patient's medical record and auto-populate the clinical note	Demographics (name, DOB, sex, treatment facility, ICN) • Vitals (BP, weight, height, pulse, etc.) • Surgical reports • Pathology reports	Bi-directional communication with VistA thru Computerized Patient Record System (CPRS) using FHIR API

List the Program Office or IT System information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*	*Describe the method of transmittal*
	templates within HINGE. Interface signed clinical notes from HINGE to VistA.	• Radiation therapy treatment information (treatment dates, delivered dose, treatment plan details) • Lab results • List of medication • Prior encounter not	calls to the Vista database and transmitted via SSL enabled port communication within the VA internal firewall.
Varian Aria / Elekta Mosaiq – These systems are locally deployed within the MDIA for only 41 VA sites with provide Radiation Oncology services.	To complete the radiation record within the clinical domain and VistA's electronic medical record.	Radiotherapy Treatment delivery data – Dose, fraction, Digital Imaging and Communication in Medince (DICOM) data	Electronically pulled from these systems via an interface. These systems are behind the Medical Device Isolation Architecture ((MDIA), this isolates data in a separate secure network for security purposes) at 41 VA sites. The data is transmitted via electronic data communication on SSL enabled port within the VA internal firewall.

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.

Privacy Risk: Data could be compromised at the time of transmission.

Mitigation: HINGE employs standard data communication ports and secure (SSL) based connected to transmit any data with these internally hosted (within the VA network) systems.

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***	***List the method of transmission and the measures in place to secure data***

			more than one)	
Cerner	To abstract clinical information from the patient's medical record and auto-populate the clinical note templates within HINGE. Interface signed clinical notes from HINGE to Cerner.	Demographics (name, DOB, sex, treatment facility, ICN) • Vitals (BP, weight, height, pulse, etc.) • Surgical reports • Pathology reports • Radiation therapy treatment information (treatment dates, delivered dose, treatment plan details) • Lab results • List of medication • Prior encounter not	SORN: Patient Medical Records-VA [24VA10A 7/ 85 FR 624]	Bi-directional communication with Cerner using Fast Healthcare Interoperability Resource (FHIR) API calls via SSL enabled port communication across the VAEC's TIC according to the HINGE-Cerner ATC.
Box.com	To provide consult request information with community care providers delivering radiation therapy services to veterans. The same interface will be used to return treatment information back to the VA.	Demographics (name, DOB, sex, treatment facility) Radiation therapy treatment information (treatment dates, delivered dose, treatment plan details)	SORN: Patient Medical Records-VA [24VA10A 7/ 85 FR 624]	HINGE will use web API calls to the FedRAMP approved version of Box.com. All data will be stored either within HINGE on the VAEC AWS or the Box.com platform.

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

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

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

Follow the format below:

Privacy Risk: Data could be compromised at the time of transmission.

Mitigation: HINGE employs standard data communication ports and secure (SSL) based connected to transmit any data with these internally hosted (within the VA network) systems.

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.

Notice to the individuals before collection of the data is done several ways, the SORN, this document, Notice of Privacy Practices disseminated by VHA when patients sign up for VA healthcare and VHA sends them to patients annually, posted in VA Medical Centers and on VHA Privacy and VA Forms and Publications website.

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

A link to the Notice of Privacy Practice is provided in the Helpful Links section at the end of this document.

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.

HINGE is an extension of the electronic medical record systems used by the VA and falls under the same notice of information collection.

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

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

VHA Handbook 1605.1 'Privacy and Release Information', Paragraph 5 lists the rights of the Veterans to request VHA to restrict the uses and/or disclosures of the individual's individually identifiable health information to carry out treatment, payment, or health care operations. The Veterans have the right to refuse to disclose their SSN to VHA. The individual shall not be denied any right, benefit, or privilege provided by law because of refusal to disclose to VHA an SSN (see 38 CFR 1.575(a))

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

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

The individual has the right to particular use of the information within the frameworks of the electronic medical record system. HINGE interfaces with the electronic medical record and does not have any controls to limit the access of data between the two systems.

6.4 <u>PRIVACY IMPACT ASSESSMENT: Notice</u>

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

<u>Principle of Transparency:</u> Has sufficient notice been provided to the individual?

<u>Principle of Use Limitation:</u> 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:

<u>Privacy Risk:</u> There is a risk that members of the public may not know that the HINGE System exists within the Department of Veterans Affairs.

Mitigation: The VA mitigates this risk by providing the public with two forms of notice that the system exists, as discussed in detail in question 6.1, including the Privacy Impact Assessment and the System of Record 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.***

All the required information for the patient from HINGE is going to be pushed into the VistA electronic health record. Patients who wish to get access to this information are advised to follow the due process indicated by the VA's FOIA office. https://www.va.gov/foia/.

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).

All the data recorded in HINGE is interfaced and submitted to the Electronic Health Record (VistA/Cerner). There is no information in HINGE that is not filed in VistA as a clinical note. Patients who wish to get access to this information are advised to follow the due process indicated by the VA's FOIA office. https://www.va.gov/foia/.

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.

All the data recorded in HINGE is interfaced and submitted to the Electronic Health Record (VistA/Cerner). There is no information in HINGE that is not filed in VistA as a clinical note. Patients who wish to get access to this information are advised to follow the due process indicated by the VA's FOIA office. https://www.va.gov/foia/.

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.

The clinical notes from HINGE are pushed into Vista's electronic health record and the clinicians have the capability to correct for any inaccuracies or erroneous information within the VistA application by contacting the local Health Information Management Service (HIMS) office where the patient received healthcare service.

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.

All data from HINGE is interfaced over as clinical note into the electronic medical record system (Vista). Individuals are not notified if there is missing or inaccurate information in their record contained in the HINGE system. Since all HINGE data is pushed into Vista, an individual who wishes to determine whether a record is being maintained under his or her name in the Vista system or wishes to determine the contents of such records should submit a written request or apply in person to the VA facility where the received healthcare service and the records are located.

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.

Not applicable, individuals will not access or redress or request for amendments of the records within the HINGE software. Once the data is in Vista via the interface, individuals can request the local medical record office for any of the requested amendment procedures listed in the SORN.

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: There is a risk that individuals may seek to access or redress records about them held by the Vista system and become frustrated with the results of their attempt.

Mitigation: By publishing this PIA, and the applicable SORN, the VA makes the public aware of the unique status of applications and evidence files, such as those stored on the Vista platform. Furthermore, this document and the SORN provide the point of contact for members of the public who have questions or concerns about applications and evidence files.

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.

PII data will be used in the HINGE software for user account management. Access to HINGE is based on VA approved users via the Active Directory (AD) provisioning system and a successful SSOi login via PIV cards. Any employee who has an active VA active directory account can request for an account to be created in HINGE. The HINGE system administrator is responsible to grant access to VA users after verifying the bonified need for accessing the system. Users attempting to access the HINGE application will first encounter a landing page requiring a PIV based SSOi login.

After the user logs in via their PIV card and is authenticated by the SSOi system, the HINGE database will verify that specific user has been granted access to HINGE and their associated user role. For users who have not been onboarded / registered with the HINGE system, the software will reroute them to a web page where they can request access to HINGE. With this an email is sent to the HINGE system administrators' group at the National Radiation Oncology Program (NROP) office who will approve or deny access based on the review of bonified need. If the request is denied, the users will receive an email notification and will not be granted access to access the HINGE software. Approved users will have an entry with their name, Integration Control Number (ICN) and VA email address added in the HINGE database for future verification. The HINGE system administrator can also remove users who no longer should have access to HINGE.

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?

Not applicable, HINGE does not give access to users from other agencies.

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.

For VA users with a valid PIV and who have been determined to have a reason to access HINGE, user roles include same-facility access, enterprise access, system admin.

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, contractor will have access to the HINGE application for design and maintenance purposes. A signed Business Associate Agreement (BAA) is in place for these contractors who work on the HINGE application. VA contract employee access is verified through the Contracting Officer's Representative (COR) and other VA supervisory/administrative personnel before access is granted to any VA system. Contractor access is reviewed annually at a minimum. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of Behavior training via the VA Talent Management System (TMS). All contractors are vetted using the VA background investigation process and must obtain the appropriate level background investigation for their role. Contractors with systems administrative access are required to complete additional role-based training prior to gaining system administrator access. Generally, contracts are reviewed at the start of the initiation phase of acquisitions and again during procurement of option years by the Contracting Officer, Information Security Officer, Privacy Officer, COR, Procurement

Requestor/Program Manager and any other stakeholders required for approval of the acquisition. Contracts generally have an average duration of 1-3 years and may have option years stipulated in the original contract.

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 users who will have access to HINGE application must complete the required annual VA training using the Talent Management System (TMS), including:
1. VA Privacy and Information Security training
2. HIPAA focused training
3. Rules of Behavior training.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* Feb 1, 2023
3. *The Authorization Status:* Authorization to Operate (ATO)
4. *The Authorization Date:* Nov 8, 2022
5. *The Authorization Termination Date:* Nov 8, 2023
6. *The Risk Review Completion Date:* Oct 6, 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.***

Not applicable

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)*

HINGE is being developed and deployed on the VAEC Amazon Web Services (AWS) cloud and has been granted an ATO. HINGE is a Software as a Service developed by and for the NROP. The AWS utilized as an infrastructure for HINGE is FedRAMP ATO authorized.

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

NA

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.

NA

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.

NA

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).

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

ID	Privacy Controls
IP-3	Redress
IP-4	Complaint Management
SE	**Security**
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR	**Transparency**
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

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

Margaret L. Pugh 104985

Digitally signed by Margaret L. Pugh 104985
Date: 2023.09.11 07:43:35 -04'00'

Privacy Officer, Margaret (Peggy) Pugh

John D. Mills 497100

Digitally signed by John D. Mills 497100
Date: 2023.09.11 01:31:01 -07'00'

Information System Security Officer, John. D. Mills

Tony L. Sines 167047

Digitally signed by Tony L. Sines 167047
Date: 2023.09.07 15:42:48 -05'00'

Information System Owner, Tony Sines

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).

Notice to the individuals before collection of the data is done several ways, the SORN, this document, Notice of Privacy Practices disseminated by VHA when patients sign up for VA healthcare and VHA sends them to patients annually, posted in VA Medical Centers and on VHA Privacy and VA Forms and Publications website.

HELPFUL LINKS:

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