Privacy Impact Assessment for the VA IT System called:

Community Viewer

Veterans Heath Administration (VHA)
Community Care Program Office

Date PIA submitted for review:

19 January 2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Rita Grewal	Rita.Grewal@va.gov	202-870-1284
Information System Security Officer (ISSO)	Andre Davis	Andre.Davis2@va.gov	512-326-7422
Information System Owner	Christopher Brown	Christopher.Brown1@va.gov	512-326-6645

Abstract

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

Community Viewer (CV) is a web application that provides authorized users (Non-VA health care providers) with the ability to view read-only clinical data (patient's medical records) stored in any electronic medical record system that belongs to the VA's Veterans Health Information System.

Overview

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

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

Community Viewer (CV) is owned by the Veterans Heath Administration (VHA) Community Care Program Office and located/hosted at the VA Austin Information Technology Center (ATIC).

The Veterans Access, Choice, and Accountability Act of 2014 (VACAA) (Public Law 113-146) Section 101 requires the VA to establish a temporary program ("the Choice Program") to improve Veterans' access to health care by allowing eligible Veterans to use eligible health care providers outside of the VA system (non-VA care). Regular growth of Non-VA Medical Care (NVC) over the last ten years, coupled with VACAA's expansion in Veteran eligibility for non-VA care, demands seamless communication between all parties rendering care for our nation's Veterans, irrespective of whether care was rendered internal or external to VA's provider network. In order to meet the demands of the Choice Program, solutions such as CV are needed to provide non-VA providers the ability to access Veteran Electronic Health Record (EHR), in order to improve the availability of medical services provided to Veterans. CV

is the application that meets this demand.

CV is a web application that provides authorized users (currently around 200) (Non-VA health care providers) with the ability to view read-only clinical data (VA's patient's medical records) stored in any electronic medical record system that belongs to the VA's Veterans Health Information System and specifically assigned to that non-VA health care provider. It provides a common view of patient and clinical information from Veterans Health Information Systemsand Technology Architecture (VistA). The Veteran EHR data will be made available to authorized non-VA Providers through controlled access using a secure internet protocol via their current web browsers. NonVA providers will be granted access to Veteran EHR, as authorized by the patient and on a "need to know" basis. This authorized access will allow non-VA providers the ability to review and print existingconsults/referrals, orders and/or progress reports, or other relevant health record data in order to improvemedical services provided to Veterans. Agreements between non-VA providers and the VA are done electronically via the CV web page. These agreements are updated annually as well as archived for historical purposes.

To protect patient privacy, a VA referral Administrative Graphical User Interface (GUI) known as the Community Care Provider Management (CCPM) module will be used to manage non-VA provider activity on the application. Only authorized non-VA providers cleared and approved by the assigned VHA personnel, will be able to access the CV system. This access is managed by assigned VHA personnel through the use of CCPM. Assigned VHA personnel will be able to approve access, assign ID's/passwords, configure access levels, and define the date range of medical history from the Veteran EHR that non-VA providers will be authorized to view for a limited time period. That time limit will also be set using CCPM.

Due to the fact that the CV is a read-only viewer that will be used to disseminate electronic health information, it does not create any Personally Identifiable Information (PII) or Protected Health Information (PHI). CV does not store individual PHI information; however, CV does store specific elements of PII data in a secured database for security/auditing only by authorized VA personnel Potentially affected individuals, in a case of inadvertent disclosure of information, are the Veterans who are referred by the VA to non-VA healthcare providers for medical treatment. Therefore, approximately user's data (approximately 1000 users) will be kept for six years in the audit logs then deleted unless marked for litigation hold.

The Health Insurance Portability and Accountability Act (HIPAA Public Law (Pub. L.) 104-191) implemented by 45 CFR Parts 160 and 164 provides for the improvement of the efficiency and

effectiveness of health care systems by encouraging the development of health information systems through the establishment of standards and requirements for the electronic transmission, privacy, andsecurity of certain health information.

A new function has been added to the viewer which allows the non-VA medical care provider to print therelevant portions of a veteran's electronic health record in support of treatment. The VHA Notice of Privacy Practices is provided to newly enrolled Veterans upon enrollment and to all enrolled Veterans every three years per VHA Handbook 1605.04.

The authority to operate the system is stated in System of Record Notification (SORN) 24VA10A7, VAPatient Medical Records, Title 38, United States Code, Sections 501(b) and 304.

For the user audit log portion of this system, SORN 79VA10, VistA - VA is being updated by VHA privacy to include systems with that functionality. Collection of that data and maintaining the system are authorized by Title 38, UnitedStates Code, Section 501.

CV has assets operating at the VA's, privately owned, Infrastructure Operation's (IO's), internal cloud offering as well as VA's VMWare farm. Management of CV's assets are shared between the contractorand Office of lnformation and Technology's (OI&T) Information Technology Operations and Services (ITOPS). CV's security controls are constantly reviewed during its A&A process and is validated on anannual basis by the Information Owner and the facility formation System Security Officer (ISSO).

Completion of this PIA will not require changes to the business process.

CV is a Federal Information Processing Standard (FIPS) 199 HIGH system. The magnitude of harm would be an Irreparable Impact on Major Application or General Support (GSS) functions, image or reputation, such that the catastrophic result would not be able to be repaired or set right again or couldresult in Loss of Major Tangible assets or resources, including posing a threat to human life.

CV is hosted at AITC. The servers listed in the ComponentDetails tab are included for informational purposes only. These servers fall under the authorization boundary of the Infrastructure Operations (IO) UNIX and Windows Service Lines.

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 Account Information
- ☒ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers
- ☐ Vehicle License Plate Number
- ☒ Internet Protocol (IP) Address Numbers
- ☒ Current Medications
- ☐ Previous Medical Records
- ☒ Race/Ethnicity
- ☐ Tax Identification Number
- ☐ Medical Record Number
- ☐ Gender
- ☐ Integration Control Number (ICN)
- ☐ Military History/Service Connection
- ☐ Next of Kin
- ☒ Other Unique Identifying Information (list below)

CV is a viewer that only disseminates the information, indicated above, which is pulled from VistA and Master Person's Index (MPI). CV does not collect, create, or maintain any of the above identified information with the exception of the IP address of the user accessing the system which is captured in a user audit log. The user audit log is used as part of routine auditing activities as outlined in question 3.1.

The following information is collected and retained in the user audit log: Users login identifier, User ID,Name of User, Patient's Identifier - (EDIPI), Query Action, Start and End Timestamps, Date of Audit, IPAddress of Machine.

PII Mapping of Components

CV consists of 14 key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by CV and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

PII Mapped to Components

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
AITC CV DB server 1	Yes	No	User's Name-ID/PIV/CAC/Patient SSN/Workstation IP address	Used for audit logging	Stored in an encrypted database controlled by IO
AITC CV DB server	Yes	No	User's Name-ID/PIV/CAC/Patient SSN/Workstation IP address	Used for audit logging	Stored in an encrypted database controlled by IO
PITC CV DB server 1	Yes	No	User's Name-ID/PIV/CAC/Patient SSN/Workstation IP address	Used for audit logging	Stored in an encrypted database controlled by IO
PITC CV DB server 2	Yes	No	User's Name-ID/PIV/CAC/Patient SSN/Workstation IP address	Used for audit logging	Stored in an encrypted database controlled by IO

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

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

Describe why information from sources other than the individual is required. For example, if a program's system is using data from a commercial aggregator of information or data taken from

public Web sites, state the fact that this is where the information is coming from and then in question 1.3 indicate why the system is using this source of data.

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

CV is a viewer which displays patient data contained in VistA and MPI. Information within VistA isprovided by the Veteran as well as VA healthcare providers who provide treatment for the veteran. Additional data is extracted and displayed from the Master Veterans Index (MPI) system.
VistA and MPI PIAs can be found on the VA website:
http://www.oprm.va.gov/privacy/pia.aspx User audit log information listed in section 1.1 is collected/maintained via CV's encrypted database.

1.3 How is the information collected?

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

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

CV disseminates a patients' medical information retrieved from VistA/MPI, e.g. name, social securitynumber (SSN), medical conditions, physician's notes, etc.

User audit log information listed in section 1.1 is collected from IO infrastructure/systems that CV connects to.

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

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

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

CV utilizes a one-way data service, which pulls the information directly from the VistA and MPI systems. CV has no way to alter or validate the accuracy of the data it utilizes and therefore accuracy of data is done at the discretion of the owning system (VistA/MPI).

User audit log information User's Name ID/PIV/CAC/Workstation IP address via CV's encrypted database via a one-way data service and therefore is unable to validate accuracy of data, please see statement above.

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

Presidential Review Directive 5, A National Obligation - Planning for Health Preparedness for and Readjustment of the Military, Veterans, and Their Families after Future Deployments, August 1998

- Per SORN 24VA10A7 Patient Medical Records Title 38, United States Code, Section 501(b) and 304.

For the audit log portion of this system, SORN 79VA10, Veterans Health Information Systems and Technology Architecture (VistA) Records-VA is being updated by VHA privacy to include systems with that functionality. Collection of that data and maintaining the system are authorized by Title 38, United States Code, Section 501.

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

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: CV does not create or maintain any PHI or PII; CV only disseminates a read-only view of a patient's medical information. CV uses a data service to assemble a read-only real-time view of electronic health information and then presents that information to VA authorized HIPAA regulated non-VA medical care providers. The non-VA Provider has the ability to print information from an EHR authorized and assigned to them by the VA. If this information is breached or accidentally released to inappropriate parties or the public, it could result in financial, personal, and/or emotional harm to the individuals whose information is presented by the system.

Mitigation: Session security is ensured by the use of secured unique session tokens generated using a 128-bit hash from a secure random number generator for each authenticated user, the system ensures prevention of communication session hijacking. Once the user logs out of the system, the session is immediately destroyed, and the session hash can no longer be used. Also, if in some instance the Session ID were to be obtained, the user cannot paste it as part of a URL string to gain access. Data encryption uses SSL with TLS 1.1, ensuring that all server communication is encrypted, which limits the ability to perform Man in the Middle (MITM) attacks. The web services used in CV employ Schema Validation. This helps prevent Denial of Service (DoS) attacks by preventing the invocation of XML bombs. The non-VA Providers are either under contract through the Choice Program, or are required to sign Provider Agreements, both of which outline and stress the responsibility of the receiving healthcare provider to follow all relevant HIPAA and Privacy Act law and regulatory guidance in the care, control, and retention of the presented or printed information.

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.

CV does not create or maintain any PHI or PII. It is a viewer that disseminates a patient's medical record which is used by community medical professionals to provide better and faster diagnosis of Veterans' health issues. The information below is viewed and can be printed by the clinician in order to provide care to a Veteran. It is not retained and/or maintained on the system.

- Name: To identify the Veteran -internal/external
- Social Security Number: To identify the Veteran-internal/external
- Date of Birth: To identify the Veteran's age-internal/external
- Mailing Address: For communication with the Veteran-internal/external
- Zip Code: Part of mailing address -internal/external
- Phone Number: For communication with the Veteran-internal/external
- Health Insurance Beneficiary Numbers: To identify the Veteran's health insurance for proper coverage of the provided healthcare-internal/external
- Electronic Health information: To facilitate the proper medical treatment of the Veteran-internal/external
    - Internet Protocol (IP) Address Numbers: To meet the requirements of for the accounting for disclosure provisions of the Privacy Act, the HIPAA Privacy Rule, and Freedom of Information Act, outlined in VA Handbook 1605.1, Privacy and Release of Information-internal
- Security audit logs retains the following information for security and law enforcement purposes in CV's encrypted database:
    - Users login identifier - identify user
    - Name of User- to identify user
    - Patient's Identifier - (EDIPI) - to identify correct patient
    - Workstation IP address - to identify the user's location/workstation

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

Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex

analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis.

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

CV is a viewer that disseminates electronic health information pulled from VistA and MPI via a one-way data service and has no ability to analyze any data. Data analysis is done at the discretion of owning VA system (VistA/MPI).

2.3 How is the information in the system secured?

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

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

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

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

CV is a read only system and does not collect, process, or retain data. All data is sent via TLS encrypt tunnels to the user via HTTPS or over RSA encryption within the VA.

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

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. <u>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.</u>

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

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

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

Add answer here:

CV follows VA System of Record Notice (SORN) 24VA10A7, Patient Medical Records for the use of PII and PHI. All authorized non-VA health providers must authenticate using an assigned user ID and password credential. User roles and access privileges are managed by the assigned VHA personnel through the CCPM module, which allows those personnel the ability to approve user access, assign user ID's/passwords, configure access levels, define the timeframe of medical history from the Veteran EHR to be authorized for viewing, and a date range or time limit that information will be available to the specific user. Only authorized users cleared and approved by assigned VHA personnel will be able to access the CV system and can then only gain access to read only patient clinical data for the patient(s) that were assigned to that user by the assigned VHA personnel.

The SORN for the CV system is 24VA10A7 and is located at the following website: https://www.gpo.gov/fdsys/pkg/FR-2012-10-31/pdf/2012-26801.pdf

Amended SORN: https://www.gpo.gov/fdsys/pkg/FR-2013-03-22/pdf/2013-06664.pdf Amended SORN: https://www.gpo.gov/fdsys/pkg/FR-2014-02-11/pdf/2014-02890.pdf Amended SORN: https://www.gpo.gov/fdsys/pkg/FR-2014-08-14/pdf/2014-19283.pdf
Please refer to Section 8. Technical Access and Security for the process to authorize users access to data and/or the system.
79VA10 is located at: https://www.oprm.va.gov/docs/sorn/SORN79VA10.docx

Section 3. Retention of Information

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 What information is retained?

Identify and list all information collected from question 1.1 that is retained by the system.
This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal

The only information identified in question 1.1 retained by the system are the fields captured in the user audit log. CV captures specific flagged information in the system log for auditing purposes only and maintains the data on CV's encrypted database. This information is retained in order to meet the requirements for the accounting for disclosure provisions of the Privacy Act,

the HIPAA Privacy Rule, and Freedom of Information Act, which is outlined in VA Handbook 1605.1, Privacy and Release of Information. The information captured in the system log is:

- Users login identifier
- User ID
- Name of User
- Patient's Identifier - (EDIPI)
- IP Address of Machine Where User is Logged In

3.2 How long is information retained?

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

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

ITOPS is responsible for maintaining CV's operating system the audit logs. Audit logs are retained within QRadar Security Information and Event Management (SIEM), which consolidates log source event data from thousands of devices, endpoints and applications distributed throughout a network, in a live state for six months. Audit logs older than six months are archived and can be reimported back into QRadar SIEM for discovery and compliance. The archives are kept for six years as required by paragraph 35c (4) of VA Handbook 1605.1. In cases of litigation hold, audit logs may be retained until legal proceedings have been completed.

CV user audit logs, information maintained from section 1.1, is maintained in CV's encrypted database for security or legal audits if/when necessary.

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

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

The Record Control Schedule (RCS) 10-1 contains retention and disposition requirements for VHA records which have been authorized by NARA or have been assigned a General Record Schedule (GRS) disposal authority. The VHA RCS 10-1 is the main authority for the retention and disposition requirements of VHA records. It provides a brief description of the records, states the retention period and disposition requirements. The actual defined period will be different depending on the specific record type. VHA Health care facilities do not set record retention periods or disposition authority for PII, nor do they set policy for data destruction. VHA health care facilities are to comply with the VHA RCS 10-1.

3.4 What are the procedures for the elimination of SPI?

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

Audit logs and/or reports containing VA sensitive information pertaining to the system (described insection 3.1) such as IP addresses and other operational data will be destroyed in accordance with VA6500.1 Handbook and any paper records will be destroyed in accordance with VA Directive 6371.

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

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

The CV system does not use PII/PHI/SPI or production data for any testing or development purposes.

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.

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:

There is minimal to no privacy risk, the information captured in the user audit log is information that captures which users (non-VA providers) accessed patient information using CV. System logs are securely maintained in the QRadar event management system under IO management.

The non-VA Provider has the ability to print information from an EHR authorized and assigned to them by the VA, creating a hard copy of the read-only information for their records. Therefore, there is a risk the printed PII/PHI will be exposed/unintentionally released to unauthorized persons increasing the risk of data misuse.

Mitigation:

Per VA Directive and Handbook 6500 which can be accessed in the VA library located at http://wwwl.va.gov/vapubs/, only those with security related duties have access to the system/application logs.

The transfer of information caused by the non-VA Provider's ability to print from authorized and assigned EHR is between one HIPAA regulated healthcare provider to another HIPAA regulated healthcare provider for the specific purpose of providing healthcare to our Veterans. As such, any transfer of data also transfers responsibility and liability for the protection of that data to the receiving HIPAA regulated healthcare provider. The non-VA Providers are either under contract through the Choice Program, or are required to sign Provider Agreements, both of which outline and stress the responsibility of the receiving healthcare provider to follow all relevant HIPAA and Privacy Act law and regulatory guidance in the care, control and retention of the printed records.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
Veterans Benefits Administration (VBA)	Review records needed for VA ratings and compensation claims.	Name Social Security Number Date of Birth Mailing Address Zip Code Phone Number(s) Email Address Emergency Contact Information Current Medications Previous Medical Records	Compensation and Pension Record Interchange (CAPRI) electronic software package

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*
		Race/Ethnicity Information (III).	
Veterans Health Administration VISTA	CV uses VISTA data to display patient's medical records as well as create reports at user's request	Name Social Security Number Date of Birth Mailing Address Zip Code Phone Number(s) Email Address Emergency Contact Information Current Medications Previous Medical Records Race/Ethnicity Patient ICN/EIN	Secure electronic transmission via Transmission Control Protocol (TCP) Hypertext Transfer Protocol Secure (HTTPS). Storage of report uses AES-256 encryption.
Veterans Health Administration VISTA Imaging	CV uses VISTA Imaging data to display patient's medical imaging history.	Name Social Security Number Date of Birth Mailing Address Zip Code Phone Number(s) Email Address Emergency Contact Information Previous Medical Records Race/Ethnicity Patient ICN/IEN Clinical Images – to include scanned documents	Secure electronic transmission via Transmission Control Protocol (TCP) Hypertext Transfer Protocol Secure (HTTPS). Storage of report uses AES-256 encryption.
Veterans Health Administration (VHA) Health Care Providers	Provides health record information to CV to support treatment of veteran. This allows the VA to refer patients/Veterans to local community care providers in times of long wait times/specialty services needed/distance	Name Social Security Number Date of Birth Mailing Address Zip Code Phone Number(s) Email Address Emergency Contact Information Current Medications Previous Medical Records Race/Ethnicity Information	Electronically pulled from VistA thru Computerized Patient Record System (CPRS)

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*
	limitation of the patient/Veteran.		
VA IT Operations and Services (ITOPS) IO Technical Security Office	To meet the requirements for the accounting for disclosure provisions of the Privacy Act, the HIPAA Privacy Rule, and Freedom of Information Act outlined in VA Handbook 1605.1, Privacy and Release of Information.	Users login identifier, User ID, Name of User, Patient's Identifier (EDIPI), Query Action, Start and End Timestamps, Date of Audit, IP Address of Machine	QRadar Data sent from servers to QRadar through QRadar agent from IO Monitoring package.
Veterans Health Administration (VHA) Master Person Index (MPI)	Provides identification information to CV to support treatment of veteran	Name Social Security Number Date of Birth Mailing Address Zip Code Phone Number(s) Email Address Emergency Contact Information Current Medications Previous Medical Records Race/Ethnicity Patient ICN/EIN	Secure electronic transmission via Transmission Control Protocol (TCP) Hypertext Transfer Protocol Secure (HTTPS).

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

Follow the format below:

Privacy Risk:

The privacy risk associated with disclosing PII internally only within the Department of Veterans' is minimal and will follow all established security protocols in the treatment of VA

patients in VA facilities. Veterans Affairs policy is that the data will NOT be disclosed to individuals who do not require access or have a need to know. Inappropriate/unauthorized disclosure heightens the threat of the information being misuse

Mitigation:

There are minimal to no privacy risks to the data captured in the user logs. The system logs are securely maintained in CV's encrypted database. Access to these audit logs are limited to personnel with a security related job function and auditors.

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***
Non-VA Healthcare Providers	Authorized Community Care Providers need Veteran's medical records for effective treatment	Patient identifier; patient demographics; and patient medical records CV disseminates PII, PHI, and Individually Identifiable Information (III) appropriate to the agreement for viewing/printing to external providers. CV receives Pertinent PII and III appropriate to the agreement from external providers for the audit log.	The Privacy Act, 5 U.S.C. 552a, HIPAA (Public Law (Pub. L.) 104-191), VA Handbook 1080.01 VA System of Record 24VA10A7, Title 38, United States Code, Sections 50l(b) and 304. MOU between VA and Albany Medical Center dated 6/15/16.	Secure Hypertext Transfer Protocol (HTTPS)/Single Socket Layer (SSL)/ Transport Layer Security (TLS) a standard security technology for establishing an encrypted link between a web server and a browser.

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:

The possibility exists that PHI data protected under 38 U.S. Code § 7332 can be accessed through the system without the prior written consent of the patient required by statute.
The non-VA Provider has the ability to print information from an EHR authorized and assigned to them by the VA, creating a hard copy of the read only information for their records. Therefore, there is a risk the printed PIVPHI will be exposed/unintentionally released to unauthorized persons increasing the risk of data misuse.

Mitigation:

7332 Protected Data:
Currently no mechanism exists in VistA to identify/flag patient records with 7332 data. CV is dependent upon manual intervention by VHA Community Care Coordinators. Prior to assigning any patient record to a Community Provider, the Coordinator will:

1. Determine if 7332 protected data exist in the patient EHR
2. For any patient found to have 7332 data in their EHR, determine if the patient has signed a release authorization.
    a. If it is determined that the patient does not have a signed release authorization, they will be asked to sign one.
    b. If the patient does not want to sign a release authorization or one cannot be obtained for any other reason, then the currently established manual process for providing patient data to the Community Provider will be followed. The Community Provider will not be authorized access to the EHR for that patient in the Community Viewer.
3. A copy of the authorization of release of 7332 data is shown in Appendix A.

Section 6. Notice

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

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

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

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

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

The Department of Veterans Affairs does provide public notice that the system does exist. This notice is provided in 2 ways:

1. SORN 24VA10A7 - Patient Medical Records and 79VA10, VistA - VAhttps://www.oprm.va.gov/docs/Current_SORN_List_1_7_2022.pdf

2. This Privacy Impact Assessment (PIA) also serves as notice of the CV System. As required by the eGovernment Act of 2002, Pub.L. 107-347 §208(b)(l)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means."

VHA provides effective notice regarding collection, use, sharing, safeguarding, maintenance and disposal of PII, authority for collecting PII and the ability to access or amended PII through its Privacy Act SORNs. In addition, the VHA Notice of Privacy Practices (NOPP) provides notice on privacy practices including collection, use and disclosure of PII and PHI and privacy rights such as the ability to access and amendment.

The VHA NOPP(https://vaww.va.gov/vhapublications/ViewPublication.asp?pub_ID=1090) is provided to newly enrolled Veterans at the time of enrollment and currently enrolled Veterans annually. VHA also provides notice on the authority for collecting PII and choices regarding the PII at the point of collection. VHA permits individuals to agree to the collection of their PII through the use of paper and electronic

forms that include Privacy Act Statements outlining why the information is being collected, how it will be used and what system of records the information will be stored.

The Privacy Act Statements on the paper and electronic forms explain whether data collection is mandatory or voluntary and explains the consequences of not providing the information when data collection is voluntary. In addition, information is collected verbally from individuals. These individuals are made aware of why data is collected through the VHA NOPP and conversations with VHA employees.

VA Forms are reviewed by Veterans Health Administration Central Office (VHACO) periodically to ensure compliance with various requirements including that Privacy Act Statements are on forms collecting personal information from Veterans or individuals. Lastly, VHA provides such notice in its PIAs which are published for public consumption

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 Appendix D 'Privacy and Release Information', section 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)).

The use of CV is an opt-in type technology and must have the Veteran's permission for non-VA health care providers to access the Veteran's records. Veterans can decline however the use of CV would not be authorized.

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

Not applicable. All the data within CV comes from another VA system. CV is not involved in the PII collection process to receive consent concerning the information. For the audit log the user agrees to use and collection as a form of monitoring when agreeing to the terms on the login page.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

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

Follow the format below:
Privacy Risk:

There is a risk that members of the public may not know that the CV application 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 identified in question 6.1, including this Privacy Impact Assessment (PIA) and a System of Record Notice.

The VHA Notice of Privacy Practices is provided to newly enrolled Veterans upon enrollment and to all enrolled Veterans every three years per VHA Handbook 1605.04.

Section 7. Access, Redress, and Correction

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

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

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

http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.

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

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

Individuals (patients) are not given access to their information in CV. CV system data is for use by medical service providers only.

Individuals seeking information regarding access to and contesting of VA medical records may write, call, or visit the last VA facility where medical care was provided as directed in the SORN 24VA10A7 - Patient Medical Records which can be found online at the links noted is section 2.3 above.

When SORN 79VA10 is updated information about access, redress and record correction the audit log data will communicated.

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.

Under the jurisdiction of VHA, VHA Handbook 1605.1 Appendix D 'Privacy and Release Information', section 8 states the rights of the Veterans to amend to their records via submitted VA Form 10-5345a, Individual's Request For a Copy of Their Own Health Information, may be used as the written request requirement, which includes designated record sets, as provided in 38 CFR 1.579 and 45 CFR 164.526.

The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record. A request for amendment of information contained in a system of records must be delivered to the System Manager, or designee, for the concerned VHA system of records, and the facility Privacy Officer, or designee, to be date stamped; and filed appropriately.
See record access procedure from SORN: Individuals seeking information regarding access to and contesting of records in this system may write, call, or visit the VA facility location where they are or were employed or made contact.

When SORN 79VA10 is updated information about access, redress and record correction the audit log data will communicated.

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.

As directed in the System of Record Notice (SORN) 24VA10A7 - Patient Medical Records which can be found online at the links noted is section 2.3 above. "Individuals seeking information regarding access to and contesting of VA medical records may write, call, or visit the last VA facility where medical care was provided."

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

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

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

Formal redress procedures are provided in SORN 24VA10A7. Current link to complete document: https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

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

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

Follow the format below:
Privacy Risk:

There is a risk that individuals may seek to access or redress records about them held by the VA Office 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 this application. The SORN provides the point of contact for members of the public who have questions or concerns about the CV application.

Alternatively, individuals who wish to determine whether this system of records contain information about them should contact the VA facility location at which they are or were employed or made contact. Inquiries should include the person's full name, social security number, dates of employment, date(s) of contact, and return address.

Section 8. Technical Access and Security

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

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

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

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

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

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

All authorized users must authenticate using an assigned user ID and password credential. User roles and access privileges are managed by the assigned VHA personnel through CCPM which allows those

personnel the ability to approve user access, assign user ID's/passwords, configure access levels, configure which portions or data elements from the Veteran EHR will be authorized for viewing and a date range or time limit that information will be available to the specific user.

Only authorized users cleared and approved by the Chief Business Office Purchased Care (CBOPC) will be able to access the CV system and can then only gain access to read only patient clinical data for the patient(s) that were assigned to that user by the assigned VHA personnel. CV retains logging information for auditing purposes only. The information retained is user's login identifier, user ID, name of user, patient's identifier, query action, start and end timestamps, date of audit, and IP address of machine where user is logged in.

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

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

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

VA contract employee access is verified through the Contracting Officer's Representative (COR) and other VA supervISSOry/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.

Personnel that will be accessing VA information or information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB prior

to gaining access to any VA information system or sensitive information. The rules are included as part of the VA Privacy and Security Awareness training which all personnel must complete via the VA's TMS. After the user's initial acceptance of the Rules, the user must re- affirm their acceptance annually as part of the privacy and security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system. 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. System administrators are required to complete additional role-based training. Users with access to PHI are required to complete HIPAA privacy training annually.

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

If Yes, provide:

1. *The Security Plan Status, Approved*
2. *The Security Plan Status Date, 07-12-2021*
3. *The Authorization Status, ATO*
4. *The Authorization Date, 10-03-2021*
5. *The Authorization Termination Date, 10-03-2022*
6. *The Risk Review Completion Date, 07/19/2021*
7. *The FIPS 199 classification of the system is High*

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

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

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).

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.

System is not in a cloud environment

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

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

System is not in a cloud environment

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.

System is not in a cloud environment

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.

System is not in a cloud environment

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).

This is not applicable to this application

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.

RITA K GREWAL 114938

Digitally signed by RITA K GREWAL 114938
Date: 2022.01.31 15:45:17 -05'00'

Privacy Officer, Rita Grewal

Andre L. Davis 1130018

Digitally signed by Andre L. Davis 1130018
Date: 2022.01.31 14:50:01 -06'00'

Information Systems Security Officer, Andre Davis

Christopher Brown 101386

Digitally signed by Christopher Brown 101386
Date: 2022.01.31 15:34:19 -06'00'

Information Systems Owner, Christopher Brown

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).

Link to VA Privacy Website: https://www.va.gov/privacy/. https://www.oprm.va.gov/privacy/pia.aspx

Link to SORN 24VA10A7 Patient Medical Records-

VA: https://www.govinfo.gov/content/pkg/FR-2020-

10-02/pdf/2020-21426.pdf

Link to VHA Notice of Privacy Practices:

https://vaww.va.gov/vhapublications/ViewPublication.asp?pub_ID=1090