SPLASH PAGE LANGUAGE

The completion of Veterans Affairs Privacy Impact Assessments (PIAs) is mandated for any rulemaking, program, system, or practice that collects or uses PII under the authority of the E-government Act of 2002 (44 U.S.C. § 208(b)) and VA Directive 6508, Implementation of Privacy Threshold Analysis and Privacy Impact Assessment.

The PIA is designed to identify risk associated with the use of PII by a system, program, project or practice, and to ensure that vital data stewardship issues are addressed for all phases of the System Development Life Cycle (SDLC) of IT systems. It also ensures that privacy protections are built into an IT system during its development cycle. By regularly assessing privacy concerns during the development process, VA ensures that proponents of a program or technology have taken its potential privacy impact into account from the beginning. The PIA also serves to help identify what level of security risk is associated with a program or technology. In turn, this allows the Department to properly manage the security requirements
under the Federal Information Security Management Act (FISMA).

VA HANDBOOK 6508.1: "Implementation of Privacy Threshold Analysis and Privacy Impact Assessment," July 2015, https://www.va.gov/vapubs/viewPublication.asp?Pub_ID=810&FType=2

Please note that the E-government Act of 2002 requires that a PIA be made available to the public. In order to comply with this requirement PIA will be published online for the general public to view. When completing this document please use simple, straight-forward language, avoid overly technical terminology, and write out acronyms the first time you use them to ensure that the document can be read and understood by the general public.

Privacy Impact Assessment for the VA IT System called:

The Diameter Health Clinical Care Document Analyzer

Enterprise Program Management Office (EPMO)
Veterans Health Administration (VHA)

Date PIA submitted for review:

September 15, 2021

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)	Albert Estacio	Albert.Estacio@va.gov	909.583.6309
Information System Owner	Chris Brown	Christopher.Brown1@va.gov	(202) 270-1432

Abstract

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

The Diameter Health Clinical Care Document Analyzer (DH CCDA) (Analyzer) is used to create instant clinical data quality ratings for Clinical Care Documents (CCD) that are part of the Veterans Health Information Exchange (VHIE). Analyzer evaluates health data within CCDs that the non-VA partners provide to VHA via the health exchange and assigns a "score" based on the quality/completeness/quantity of data received. The purpose of this tool is to measure the data VHA is receiving from our non-VA partners, to improve the information received.

Overview

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

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

The VHA VHIE licensed the Analyzer product to create instant clinical data quality ratings for CCDs and Health Level Seven (HL7) Consolidated CDA formatted Continuity of Care Documents that are part of the VHIE. Analyzer evaluates health data (CCDs) that the non-VA partners provide to VHA via the health exchange and assigns a "score" based on the quality/completeness/quantity of data received. The purpose of this tool is to measure the data VHA is receiving from our non-VA partners, to improve the continuity of care information received (VHA typically shares a much higher quality/quantity of data than our partners). According to Meaningful Use Stage 2 criteria, CCD is the designated standard that certified provider Electronic Health Records (EHR) must use to exchange data. CCDs include summary

information from clinical encounters between the Veteran and their health care provider and are designed to support continuity of care when a patient moves from one provider to another. The tool generates document quality ratings, using hundreds of configurable rules addressing dimensions of document completeness, syntax and consistency across key sections of clinical documents. Accuracy is gauged by comparing contents of one section of the CCD to other sections within the same document. For completeness, it checks whether expected sections are included, and whether expected entries are complete. For syntax, Analyzer checks whether the document is structured correctly, and whether the right terminologies are used. Analyzer supports all standardized clinical terminologies.

Analyzer depends on real time connectivity to VA networks for two key business functions:

- Integrated single sign on using VA's DS Login infrastructure
- Secure access to VHIE CCD documents used as input for quality review.

The VHA VHIE systems are to address and comply with Executive Order 13410 "Promoting Quality and Efficient Health Care in Federal Government Administered or Sponsored Health Care Programs". This Executive Order requires federal agencies to use recognized health interoperability standards to promote the direct exchange of health information between federal agencies and with non-federal entities in supporting quality and efficient health care. The system's legal authority for operating the system, specifically the authority to collect the information listed in Question 1.1 is the Data Use and Reciprocal Support Agreement (DURSA) - an agreement between Health Information Exchange (HIE) partners/organizations and VA information systems with the eHealth Exchange/The Sequoia Project, providing for the interoperability "rules of the road" for all participants. The DURSA provides the legal framework governing participation in the exchange of health information by requiring the signatories to abide by a common set of terms and conditions. These commons terms and conditions support the secure, interoperable exchange of health data between and among numerous VHIE partners. The Diameter Health CCD Analyzer does not conduct any information sharing.

As an add-on service connected to the VHA's VHIE, the Analyzer application will process CCDs from Veterans who received care outside the VA health system and opted to have that information shared with their VA primary care team. At the present time, over 1.8 million Veterans have been identified as receiving part of their care with non-VA partners.

Analyzer is an Amazon Web Services (AWS) GovCloud deployed system that is currently under an ATO issued by VA. The applicable SORNs for the Diameter Health CCD Analyzer would be 24VA10A7, Patient Medical Record- VA, and 168VA005, Health Information Exchange- VA, with neither SORN requiring an update or amendment.

Section 1. Characterization of the Information

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

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

Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy- Protected Information. For additional information on these information types and definitions, please see VA Directives and Handbooks in the 6500 series

(https://vaww.va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

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

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

- ☒ Name
- ☒ Social Security Number
- ☒ Date of Birth
- ☐ Mother's Maiden Name
- ☐ Personal Mailing Address
- ☐ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☐ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☐ Financial Account Information
- ☐ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☒ Current Medications
- ☐ Previous Medical Records
- ☐ Race/Ethnicity
- ☐ Tax Identification Number
- ☐ Medical Record Number
- ☒ Other Unique Identifying Information (list below)

CCDs (see Health Level Seven CDA) may contain PII and Protected Health Information (PHI) including: Purpose, Problems, Procedures, Family history, Social history, Payers, Advance directives, Alerts, Medications, Immunizations, Medical equipment, Vital signs, Functional stats, Results, Encounters, Plan of care.

PII Mapping of Components

CCD Analyzer consists of 2 key components. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by CCD Analyzer and the functions that collect it are mapped below.

PII Mapped to Components

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

PII Mapped to Components

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards

		PII? (Yes/No)			
Analyze	**No**	**Yes**	**Please see checkmarks above.**	**Enabling system functionality**	**Database is encrypted, access to the database is limited to user interface and/or the API. Authentication and Identification controls restrict access so that the systems is only available to a limited set of VHA staff.**
Fusion	**No**	**Yes**	**Please see checkmarks above**	**Enabling system functionality**	**Database is encrypted, access to the database is limited to user interface and/or the API. Authentication and Identification controls restrict access so that the systems is only available to a limited set of VHA staff.**

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.

Continuity of Care Documents (CCD) are sent to this system from VHIE for quality assessment and scoring. There are no other sources of data used as input and all inputs are for the assessment and scoring functions related to CCDs. This system aggregates, parses, and scores CCDs to produce assessment reports to reflect quality and completeness of the health records passing through the VA's Health Information Exchange.

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.

The primary mechanism for data input is an application programming interface (API) that will be used by the VHIE to submit CCDs for review. CCDs move from the health information exchange to Analyzer via the API. The system API is secured using HTTPS encryption and API keys issued only to the VHIE application. A secondary manual secure HTTPS interface supports upload of individual Continuity of Care Documents for assessment and scoring. Members of the VHIE Data Quality Team are the only authorized users of the system. CCDs are exported from all compliant Electronic Health Record (EHR) systems. According to Meaningful Use Stage One criteria, CCD is the designated standard that EHRs must use to exchange data.

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.

CCD Analyzer includes hundreds of rules that assess completeness and accuracy of the data within the CCD. CCDs must adhere to strict standards defined by the Center for Medicaid and Medicare Services, Office of the National Coordinator for Health Information Technology as part of the Meaningful Use "final rule" that specifies the required elements and structure and semantics of "clinical documents" (C-CDA) including CCDs used for health information exchange between certified healthcare systems (See outline of standards below, and link to CMS documentation for further information).

Analyzer rules are structured either around completeness or syntax/content. The completeness rules check for the existence required data elements, either per the C-CDA2.1 implementation guide or per the best practice. The syntax/content check for the data elements that do exist, whether they are in the right clinical terminology/have reasonable content.

An example of the completeness rule would be that patient gender should be included in the document, because the C-CDA implementation guide says so. If we don't find such information, we will deduct points. An example of syntax rule would be if we do find gender info (i.e., there is some content in the gender field), we then examine whether it is coded in the right way (using the correct clinical terminology, using the defined value set, etc.). If it's not coded or not coded properly, then the relevant rule would be triggered and credit associated with that rule will be deducted.

CMS Standards:

Standards Criteria*	
§170.202(a)	Applicability Statement for Secure Health Transport.
§170.202(b)	XDR and XDM for Direct Messaging Specification.
§170.202(c)	Transport and Security Specification.
§170.205(a)(1) ***Implementation specifications***	HL7 CDA Release 2, CCD.: HITSP Summary Documents Using HL7 CCD Component HITSP/C32.
§170.205(a)(2)	ASTM E2369 Standard Specification for Continuity of Care Record and Adjunct to ASTM E2369.
§170.205(a)(3)	HL7 Implementation Guide for CDA Release 2: IHE Health Story Consolidation. The use of the "unstructured document" document-level template is prohibited.
§170.207(a)(3)	IHTSDO SNOMED CT® International Release, July 2012; and US Extension to SNOMED CT,® March 2012.
§170.207(d)(2)	RxNorm, August 6, 2012 Release.
§170.207(e)(2)	HL7 Standard Code Set CVX Vaccines Administered, updates through July 11, 2012.
§170.207(i)	The code set specified at 45 CFR 162.1002(c)(2) for the indicated conditions.

Link to CMS Standards document: https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/downloads/8_Transition_of_Care_Summary.pdf

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

Executive Order 9397 is the legal authority that allows for the system to operate, however please note that VHIE does not actually "use or collect" the SSN, as the process with DH CCD Analyzer is focused on evaluation of the healthcare data which is viewed anonymously, and VHIE has no control over information in the CCD retrieved from the non-VA partner that may include the Veteran's SSN or ID number. Additional authorities per the applicable System of Records Notices (SORNs) include Title 38, United States Code (U.S.C.) Sections 501(b) and 304.

The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 provides HHS with the authority to establish programs to improve health care quality, safety, and efficiency through the promotion of health IT, including electronic health records and private and secure electronic health information exchange.

HITECH Section 3003 establishes the Health IT Standards Committee to make recommendations to the National Coordinator around standards, implementation specifications, and certification criteria for electronic exchange and use of health information.

The Medicare and Medicaid EHR Incentive Programs provide financial incentives for the "meaningful use" of certified EHR technology. To receive an EHR incentive payment, providers have to show that they are "meaningfully using" their certified EHR technology by meeting certain measurement thresholds that range from recording patient information as structured data to exchanging summary care records. CMS has established these thresholds for eligible professionals, eligible hospitals, and critical access hospitals.

The Medicare and Medicaid EHR Incentive Programs include three stages with increasing requirements for participation. All providers begin participating by meeting the Stage 1 requirements for a 90-day period in their first year of meaningful use and a full year in their second year of meaningful use. After meeting the Stage 1 requirements, providers will then have to meet Stage requirements for two full years. CMS has recently published a proposed rule for Stage 3 of meaningful use which focuses on the advanced use of EHR technology to promote health information exchange and improved outcomes for patients.

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

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

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

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:

The CCD Analyzer receives CCDs from VHIE to assess and ultimately improve the quality of health care data available to VA health care teams and their patients.

Privacy Risk: The CCDs may contain patient identifiers that could be used to relate the health care data to a person in other systems.

Mitigation: Data is protected in transit and at rest through encryption and access control measures designed to prevent unauthorized disclosure and/or use. System audit mechanisms and continuous monitoring protocols are in place to protect against abnormal use of the system.

Section 2. Uses of the Information

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

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

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

Ongoing measurement and reporting of clinical data quality is the first step toward sustainable quality improvement.

Analyzer uses high performance parsing and proprietary logic to normalize, classify and enhance clinical data to support better clinical care and population health analytics.

The application instantly generates document quality ratings, using hundreds of configurable rules addressing dimensions of document completeness, syntax and consistency across key sections of clinical documents. These quality ratings will be used by the VHIE Data Quality Team to improve the quality of data in the VA's

electronic health record and to engage external health care organizations in discussions on how to improve the quality of data in their systems.

Name: The DH Analyzer system does not use the "name", as data is evaluated relevant only to the contributing Exchange partner, without identifying the patient whose information was reviewed, to provide de-identified input/quality scoring information for improvement of quality/completeness of the CCD.
Date of Birth: The DH Analyzer system does not use the "Date of Birth", as data is evaluated relevant only to the contributing Exchange partner, to provide de-identified input/quality scoring information for improvement of quality/completeness of the CCD.
SSN: The DH Analyzer system does not actually "use or collect" the SSN, as the process with DH CCD Analyzer is focused on evaluation of the healthcare data which is viewed anonymously, and VHIE has no control over information in the CCD retrieved from the non-VA partner that may include the Veteran's SSN or ID number.
Current Meds: The DH Analyzer evaluates the data provided (current meds) as stated above, to generate quality ratings, dimensions of document completeness, syntax and consistency, to improve the quality of data in the VA EHR and resulting CCD as well as in the external health care organizations EHR and CCD.
CCDs: The CCD data provided is evaluated as stated above, to generate quality ratings, dimensions of document completeness, syntax and consistency, to improve the quality of data in the VA EHR and resulting CCD as well as in the external health care organizations EHR and CCD. CCDs (see Health Level Seven CDA) may contain PII and Protected Health Information (PHI) including:
Purpose, Problems, Procedures, Family history, Social history, Payers, Advance directives, Alerts, Medications, Immunizations, Medical equipment, Vital signs, Functional stats, Results, Encounters, Plan of care.

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

Analyzer creates instant clinical data quality ratings and presents dashboards that monitor data completeness, accuracy, and error severity for one or many CCDs. Analyzer uses high performance parsing and proprietary logic to normalize, classify and enhance clinical data to support better clinical care and population health analytics.

The application instantly generates document quality rating reports, using hundreds of configurable rules addressing dimensions of document completeness, syntax and consistency across key sections of clinical documents.

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?

The PII is encrypted, both in transit and at rest. The VHIE Data Quality Team application administrators determine who has access to the CCD Analyzer system. All users attest to having completed role specific Privacy Act and Security training. All access to the system and its data is continuously monitored and logged. All logs are maintained in accordance with FISMA High Impact requirements described in the National Institute for Standards and Technology (NIST) publication 800.53.

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

The SSNs are encrypted when stored in the database and are masked for outbound transmission. The system does not allow for search by SSN.

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

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

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

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

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

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

The VHIE Data Quality Team application administrators determine who has access to the CCD Analyzer system. All users attest to having completed role specific Privacy Act and Security training. All access to the system and its data is continuously monitored and logged. All logs are maintained in accordance with FISMA High Impact requirements described in the National Institute for Standards and Technology (NIST) publication 800.53. VA SORN 168VA005 includes clear documentation of the uses of the information.

Health Information Exchange-VA

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

CCDs (see Health Level Seven CDA) may contain PII and Protected Health Information (PHI) including: Purpose, Problems, Procedures, Family history, Social history, Payers, Advance directives, Alerts, Medications, Immunizations, Medical equipment, Vital signs, Functional stats, Results, Encounters, Plan of care. All CCDs loaded are retained in the database. Audit logs for clinical data access and user actions are also retained in the database. Web application system logs (access, error) and database logs are retained in encrypted Amazon Cloud repositories.

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.

CCD records will be retained and disposed of in accordance with the Department's Record Control Schedule (RCS) 10-1. Data retention periods for CCDs are determined by the VHIE and can be deleted via the Application Programming Interface. See VHIE PIA for detailed description of CCD data retention schedules. In VA SORN 168VA005, Health Information Exchange- VA, Policies and Practices for Retention and Disposal notes GRS 4.3 Items 020, 030, 031 and Electronic Health Records schedule, National Archives and Records Administration (NARA) job #N1–15–02–3, item 1a, 1b, 2, 3, 4, 5, 6.

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.

-Per the VHA Records Manager, we use the Records Control Schedule (RCS) 10-1. In VA SORN 168VA005, Health Information Exchange- VA, Policies and Practices for Retention and Disposal notes GRS 4.3 Items 020, 030, 031 and Electronic Health Records schedule, National Archives and Records Administration (NARA) job #N1–15–02–3, item 1a, 1b, 2, 3, 4, 5, 6.

Records Control Schedule 10-1 (va.gov)

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

CCD records are deleted from the database via the CCD Analyzer API. Records are deleted using proprietary MongoDB delete routines.

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

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

No PII including PHI is used in testing of the application. Strict Access Control, Configuration Management, Auditing, Awareness and Training controls are in place to prevent the use of PII during pre-production configuration.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

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

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

Follow the format below:

Privacy Risk: Data received/used includes Personally Identifiable Information (PII) and Protected Health Information (PHI). Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual or otherwise breached, serious personal, professional or financial harm may result for the individuals affected.

.

Mitigation: The VA's risk assessment validates the security control set and determines if any additional controls are needed to protect agency operations. Many of the security controls such as contingency planning controls, incident response controls, security training and awareness controls, personnel security controls, physical and environmental protection controls, and intrusion detection controls are common security controls used throughout the VA. Our overall security controls follow VA 6500 Handbook, and NIST SP800-53 high impact defined set of controls. The system owner is responsible for any system-specific issues associated with the implementation of the common security controls. These issues are identified and described in the system security plans for the individual information systems.
Also, in accordance with RCS10-1 6000.2 c(1), CCD records will be deleted when no longer needed for administrative or clinical operations.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are shared/received with the Program Office or IT system***	***Describe the method of transmittal***
VHIE (formerly VLER)	CCDs are needed as input to the assessment and content scoring algorithms.	CCDs (see HL7 CDA) may contain PII and Protected Health Information (PHI) including: Header, Purpose, Problems, Procedures, Family History, Social history, Payers, Advance directives, Alerts, Medications, Immunizations, Medical equipment, Vital signs, Functional stats, Results, Encounters, Plans of Care.	Electronically pushed from Joint VA DoD Health Information Exchange (JHIE) to Analyzer RestAPI over Site to Site VPN using SSL encryption and Certificate exchange.

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: System provides quality and completeness assessments of CCDs that pass through the VHIE eHealth Exchange, those CCDs may contain PII and PHI that can be viewed by unauthorized system users. Due to the highly sensitive nature of this data, there is a risk that, if the data were accessed by an unauthorized individual

or otherwise breached, serious personal, professional or financial harm may result for the individuals affected.

Mitigation: Access to the system is strictly limited to authorized members of the VHIE Data Quality Team. The VHIE data quality team administers user accounts. Data is encrypted as it passes into the system and while stored in the application database. Access Control measures are in place to prevent inadvertent access to or exposure of data by systems administrators responsible for maintaining the system infrastructure. Participants of the system must also complete annual VA Privacy and Security Awareness training. They further acknowledge their responsibilities in protecting Veterans' information in the VA Rules of Behavior documents.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.

This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

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

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

Not Applicable

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: Not applicable. This system does not share or expose information outside the department.

Mitigation: This system does not share or expose information outside the department.

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.

This application does not collect information from the public. Analyzer receives data from the VHIE. Please refer to the PIA for VHIE.

The Share My Health Records page on the VA's VHIE site (https://www.va.gov/VHIE) provides an explanation of how Veterans can "connect their docs" through the Veterans Health Information Exchange. Veterans may opt-out or opt-back-in at any time, and per the 2019 Notice of Privacy Practices (NoPP), Veterans were advised that they would be automatically opted in for sharing through VHIE ("informed opt-out" model), but could opt-out or opt-back-in at any time. The VHIE Participate in Sharing PHI (Opt-Back-In) Form, VA Form 10-10163 is provided on that site, and contains the Privacy Act Notice.
Form Link: VA Form 10-10163

SORNs 24VA10A7 "Patient Medical Record -VA", and 168VA005 "Health Information Exchange-VA apply:

*Patient Medical Records-VA
24VA10A7: https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf

Health Information Exchange-VA
168VA005: https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01516.pdf

Notice of Privacy Practices

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

Participation in the Veterans Health Information Exchange is optional, thus if they do not wish to participate in electronically sharing their health information, they would choose to opt out. Veterans that wish to stop sharing their health information are instructed to complete the "opt-out" form (VA Form 10-10164, "OPT-OUT OF SHARING PROTECTED HEALTH INFORMATION THROUGH HEALTH INFORMATION EXCHANGES"). Veterans may opt-in by completing Form 10-10163, "REQUEST FOR AND PERMISSION TO PARTICIPATE IN SHARING PROTECTED HEALTH INFORMATION THROUGH HEALTH INFORMATION EXCHANGES". VA Form 10-10163 includes the following language with regard to the Veteran's ability to decline to provide information:

"Your disclosure of the personal information requested on this form is voluntary. However, if the information containing the Social Security Number (SSN) (the SSN will be used to locate records) is not furnished completely and accurately, the Veterans Health Administration (VHA) will be unable to comply with your request. By completing this form, you will be opted-in to the electronic exchange of health information for treatment purposes. Failure to furnish the personal information will not have any effect on any other benefits to which you may be entitled; however, you will not be opted-in to health information exchange. Consistent with the VA Notice of Privacy Practices, VA may also use the information on this form for purposes other than your treatment as authorized or required by law."

VA Form 10-10164
VA Form 10-10163

Notice of Privacy Practices

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

Currently, the Veteran is **only** consenting to the purpose of use "treatment", which is stated on the form, and the only other permissible purpose of use for the Veterans Health Information Exchange may be for treatment in an "emergent" situation.
VA Form 10-10163 provides a description of how the data is intended to be used. VA Form 10-10163 references

SORNs 24VA10A7 "Patient Medical Record -VA", and 168VA005 “Health Information Exchange- VA”. VHA VHIE does participate with the Social Security Administration (SSA) in exchanging Veteran health data for “benefits” or “coverage” purpose of use, utilizing the SSA-827 authorization form, but this is not pertinent to the DH CCD Analyzer project, as that data will not be reviewed in the scope of this project. At the present time, the eHealth Exchange DURSA does permit other purposes of use, however VHIE does not have the technical ability to accommodate other purposes of use at this time.

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 an individual may not receive notice that their information is being collected, maintained, processed, or disseminated by VHIE.

Mitigation: The VHIE VA Form (VA Form 10-10163) provides a description of how information will be used and indicates that the sharing agreement will be in effect until the Veteran opts-out of sharing their health information by completing VA Form 10-10164), and the form also references SORNs 24VA10A7 "Patient Medical Record –VA” and 168VA005 “Health Information Exchange- VA”. Additional mitigation is provided by making the System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) available for review online as well as the Notice of Privacy Practices (NoPP), which is available for review both online and is posted in the VA Medical Centers nationwide and was mailed to all enrolled Veterans prior to September 30, 2019.

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.

This application does not collect information from the public. This system provides quality and accuracy assessments for data collected by the VHIE.

Veterans who receive care from VA can access their VA medical records and their VA Health Summary:

A Continuity of Care Document (CCD) that provides a summary of their health information that can be used to review their medical record and to share essential information with their health care providers.

Veterans can get their VA Health Summary information in two file formats: An easy to read and print PDF and an XML format that can be read by computer systems.

To use the VA Blue Button feature and access the VA Health Summary, Veterans must be registered on My HealtheVet as a VA Patient and have a Premium account. A Premium account can be obtained by a My HealtheVet member who has an Advanced account, with instructions on the My HealtheVet website at: Home - My HealtheVet (va.gov)

Per VHA Directive 1605.01, Section 7, Individuals Right of Access, and Section 7(b) Right of Access and/or Review of Records, Veterans may request to view or receive copies of their health information through their local VA Medical Center's Release of Information Office (ROI), according to the following VHA Policy:

Requests for access to look at or review copies of individually-identifiable information must be processed in accordance with all Federal laws, including 38 U.S.C. 5701 and 7332, FOIA, Privacy Act, and HIPAA Privacy Rule. Except as otherwise provided by law or regulation, individuals, upon signed written request, may gain access to, or obtain copies of, their individually-identifiable information or any other information pertaining to them that is contained in any system of records or designated record set maintained by VHA. Individuals do not have to state a reason or provide justification for wanting to see or to obtain a copy of their requested information. ***NOTE:*** *VA Form 10-5345a, Individuals' Request for a Copy of Their Own Health Information, may be used, but is not required, to fulfill the signed written request requirement.*

(2) All written requests to review must be received by mail, fax, in person, or by mail referral from another agency or VA office. All requests for access must be delivered to and reviewed by the System Manager for the VHA system of records in which the records are maintained, the facility Privacy Officer or the designee of either of those positions.

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.

See Record Access Procedures in Health Information Exchange- VA SORN 168VA005. Per VHA Directive 1605.01, Privacy and Release of Information, an individual has the right to request an amendment to any information or records retrieved by the individual's name or other individually-identifiable information contained in a VA system of records, as provided in 38 CFR 1.579 and 45 CFR 164.526. The right to seek an amendment of this information or records is a personal right of the individual to whom the record pertains. The personal representative of a deceased individual has a right to request an amendment of the decedent's records.

An amendment request must be in writing, signed, and must adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written amendment request must be routed to the VA facility Privacy Officer or Chief, Health Information Management (HIM).

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.

See Record Access Procedures in Health Information Exchange-VA SORN 168VA005.
In addition, all Veterans receive a copy of the VA Notice of Privacy Practices (NoPP), and it is available online and posted in VA Medical Centers. The NoPP advises Veterans of their privacy rights, including the right to request an amendment of their information, and provides information regarding the amendment process (IB 10-163, please see link below).

Notice of Privacy Practices

Notice of Privacy Practices IB 10-163 (sharepoint.com)

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 processes are available and provided to Veterans, and are outlined in the above sections 7.1 (access), 7.2 (corrections), and 7.3 (notification of procedures for corrections). In addition, information is provided in the Health Information Exchange-VA, SORN 168VA005, and in Patient Medical Record-VA, VHA SORN 24VA10A7; redress information is provided above.

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 the Veteran may request an amendment that cannot be made due to numerous reasons, or with which the VA facility disagrees, and thus the request for amendment/correction is denied.

Mitigation: Per VHA Directive 1605.01, when a request to amend a record is denied, the Chief of HIM, or designee, or the facility Privacy Officer, or designee, must promptly notify the individual making the request of the decision. The written notification must:

(a) State the reasons for the denial. VHA may deny a request to amend a record if VHA finds that the individually-identifiable information or record requested to be amended:

(1) Was not created by VHA and the originator of the individually-identifiable information is another Federal agency available to act on the request. In this instance, the individual will be informed that the individual needs to request that the originating Federal agency of the individually-identifiable information amend the record. If, however, the originating Federal

agency of the individually- identifiable information is no longer available to act on the request, or authorizes VA to decide whether to amend the record, then VHA must do so.

(2) Is accurate, relevant, complete, or timely in its current form.

(3) Is not part of a VHA system of records or designated record set.

(b) Advise the individual that the denial may be appealed to Office of the General Counsel (OGC) and include the procedures for such an appeal as noted below in paragraph 9.b.
(c) Advise the individual that if an appeal is not filed and a statement of disagreement is not submitted, the individual may still request that the VHA health care facility provide the individual's request for amendment and the denial with all future disclosures of the information. This request needs to be submitted in writing to the Chief of HIM or designee, or the facility Privacy Officer, or designee.

(d) Describe how the individual may file a complaint with VHA or the Secretary, HHS. The description must include the name or title and telephone number of the contact person or office.

(e) Be signed by the VHA health care facility Director or official designee.
(10) If requested by the individual, the Chief of HIM, or designee, or the facility Privacy Officer, or designee, must identify the individually-identifiable information that is the subject of the disputed amendment and append or otherwise link the individual's request for an amendment and the facility's denial of the request to the individual's record.
(11) If the amendment does not pertain to the Veteran's health record, the facility Privacy Officer will work with the appropriate System Manager for the VHA system of records in which the information is maintained following the same amendment process as above.

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.

VHIE system administrators manage access to the DH CCD Analyzer. Only VA employees and authorized contractors may have access to the system. No external agencies or external users have access to this system. All access is brokered through the VA's Single Sign On infrastructure to enforce multi-factor authentication controls.

The system has two primary roles, Administrator and normal user. Administrators have the right to manage (create, update and delete) user accounts. All users can inspect individual CCD files that include PII. All users must complete VHA Privacy and Security Training and VA Rules of Behavior annually.

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.

CCD Analyzer is a Diameter Health COTS application purchased through Four Points Technology, LLC (4Points) and hosted in the 4Points GovCloud environment specifically to meet VA technical and administrative safeguards. All members of the 4Points team, a VA contractor, that have access to the environment have completed VA Privacy and Security Training, have undergone background checks, signed the Contractor Rules of Behavior, a NDA and are operating under BAA. Contracts are reviewed at least annually by the Author prior to submitting the Task Order, and also reviewed by the Contracting Officer, and Technology Acquisition Center (TAC).

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.

Everyone that has access to the environment has completed VA Privacy and Security Training offered by the VA. 4Points team members that do not have direct access to the VA systems complete company specific Privacy Act and HIPAA 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,*
   September 17, 2020
3. *The Authorization Status,*
   Active ATO
4. *The Authorization Date,*
   November 24, 2020
5. *The Authorization Termination Date*
   November 24, 2021, .
6. *The Risk Review Completion Date*
   November 13, 2020
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH).*
   confidentiality Moderate integrity high availability low Impact 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.***

Section 9 – Technology Usage

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

9.1 Does the system use cloud technology?

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517.

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

The Diameter Health system does not have a FedRAMP provisional authorization. The system inherits applicable IaaS security controls from the CSP, AWS GovCloud. The system has an agency authorization (details in Section 8). A FedRAMP P-ATO has been issued for AWS GovCloud (US), a FedRAMP P-ATO does not exist for the Diameter Health system itself.

9.2 Identify the cloud model being utilized.

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

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

The system is a Commercial Off The Shelf (COTS) offering utilizing Amazon Web Services GovCloud as Infrastructure as a Service (IaaS).

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

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

Data is owned by the Department of Veterans Affairs. The contractor does not assert any data ownership rights.

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

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

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

Ancillary data collected by the CSP via its native services (e.g. CloudWatch) is owned by the Department of Veterans Affairs.

9.5 NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met?

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

The NIST provision is incorporated into the contract. The contractor is responsible for providing documentation and artifacts necessary to obtain and maintain the Authority to Operate. The Department of Veterans Affairs remains responsible for reviewing the documentation and artifacts and issuing the Authority to Operate.

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

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

The system does not utilize RPA.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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

Signature of Responsible Officials

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

Margaret L. Pugh 104985

Digitally signed by Margaret L. Pugh 104985
Date: 2021.09.20 15:57:26 -04'00'

Privacy Officer, Margaret Pugh

Albertino M. Estacio 119921

Digitally signed by Albertino M. Estacio 119921
Date: 2021.09.21 06:49:21 -07'00'

Information System Security Officer, Albert Estacio

Christopher Brown 101386

Digitally signed by Christopher Brown 101386
Date: 2021.09.21 15:17:21 -05'00'

Information System Owner, Chris 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).

Notice of Privacy Practices IB 10-163 (sharepoint.com)

VA Form 10-10164
VA Form 10-10163

168VA005 HIE 2021-01516_FEDERAL REGISTER.pdf (sharepoint.com)

24VA10A7_Patient Medical Records Nov022020.pdf (sharepoint.com)