Privacy Impact Assessment for the VA IT System called:

Coding & Reimbursement System Plus

Health Information Management
Veterans Health Administration

Date PIA submitted for review:

March 30, 2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Christian D. Loftus	Christian.Loftus@va.gov	859-281-2470
Information System Security Officer (ISSO)	Roland Parten	Roland.Parten@va.gov	205-534-6179
Information System Owner	Gail J. Nemetz	Gail.Nemetz@va.gov	216-849-6020

Abstract

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

Coding & Reimbursement System Plus (CRS+) is an electronic means for Health Information Management (HIMS) Department users and Veterans Health Administration (VHA) coders to look up codes representing diagnosis, procedures or services using standard codes sets, e.g., International Classification of Disease, 10th Edition, Clinical Modification/Procedural Code Ste (ICD10-CM/PCS), Common Procedure Terminology (CPT), Health Common Procedure Code (HCPCS), and Evaluation & Management (E/M) codes. The software will be used to calculate Medical Severity -Diagnosis Related Grouping (MS-DRG) based on the codes assigned for a given inpatient stay and provide national coding edits to ensure correct coding guidelines are applied. CRS+ interface with another coding software, (Veterans Health Information Systems and Technology Architecture) VistA Integration, Revenue, and Reporting (VIRR) that interface with Veterans Health Information Systems and Technology Architecture (VistA) 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?*

3M Health Information System, Inc. Coding & Reimbursement System Plus (CRS+) is a Commercial-Off-the-Shelf (COTS) encoder software, under the Health Information Management Program Office, which enable health record coding to the Health Information Management (HIM) Department and Veterans Health Administration (VHA) coders. CRS+ an Application Programming Interface (API) that provides users to look up codes representing diagnosis, procedures, or services using the standard codes sets, e.g., International Classification of Disease, 10th Edition, Clinical Modification/Procedural Code Set (ICM10-CM/PCS), Common Procedure Terminology (CPT), Health Common Procedure Code (HCPCS), and Evaluation & Management (E/M) codes. The software will be used to calculate Medical Severity-Diagnosis Related Grouping (MS-DRG) based on the codes assigned for a given inpatient stay and provide national coding edits to ensure correct coding guidelines are applied.

CRS+ is a web-based application with a Structured Query Language (SQL) database which interface with the (Veterans Health Information Systems and Technology Architecture) VistA Integration, Revenue, and Reporting (VIRR) software. VistA Integration, Revenue, and Reporting (VIRR) interface with the VistA Health Information System and Technology Architecture (VistA) packages.

CRS+ interface with two of the four VIRR Graphical User Interface (GUI) modules: Veterans In-Patient (VIP) Workplace and Coding Compliance Module (CCM). These modules pass billing and coding data to the VistA packages including Patient Care Encounter, Patient Treatment File, Computerized Patient Record System (CPRS), and Surgery. CRS+ utilizes built-in Authentication and Authorization (A&A) capabilities. When CRS+ is launch from the VIRR VIP Workplace and CCM modules, the CRS+ application display the following Personally Identifiable Information (PII) information: Age, Admission Date and Discharge Date. CRS+ does not store any Protected Health Information (PHI)/ Personally Identifiable Information (PII) data.

CRS+ application is used at all Veterans Health Administration (VHA) sites and the software is hosted on National Data Center/Regional Data Center virtual servers. The VA considers CRS+ to be a COTS product because it could be sold and interfaced with other systems. The completions of the PIA will not change the CRS+ business and technology processes.

Coding & Reimbursement System Plus (CRS+)’s legal authority for operating: Title 38, United States Code, Sections 501(b) and 304. The applicable System of Records Notices (SORN) are 24VA10A7, Patient Medical Record-VA, and 121VA10A7, National Patient Database-VA, and would likely not require 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.

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)

Age, Admission Date, Discharge Date

PII Mapping of Components

Coding & Reimbursement System Plus consists of **one** key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **Coding & Reimbursement System Plus** and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

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

PII Mapped to Components

Database Name of the information system collecting/storing PII	**Does this system collect PII? (Yes/No)**	**Does this system store PII? (Yes/No)**	**Type of PII (SSN, DOB, etc.)**	**Reason for Collection/ Storage of PII**	**Safeguards**
EECF_DB	Yes	Yes	Age, Admission Date, Discharge Date	CRS+ Database does not store PHI/PII. Application **only display** the following information: Age, Admission and Discharge Date	Database is encrypted by Database Management Team. (SQL TDE and is a part of SQL)

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.

Coding & Reimbursement System Plus (CRS+) is an Application Programming Interface (API) that provides users with support for selecting International Classification of Disease, 10th Edition, Clinical Modification/Procedural Code Set (ICM10-CM/PCS), Common Procedure Terminology (CPT), Health Common Procedure Code (HCPCS), and Evaluation & Management (E/M) codes lookup.

CRS+ is an web-application that interface with the (Veterans Health Information Systems and Technology Architecture) VistA Integration, Revenue, and Reporting (VIRR) Veterans In-Patient (VIP) Workplace and Coding Compliance Module (CCM) modules. These modules display the following Personally Identifiable Information (PII) within CRS+: Age, Admission Date and Discharge Date. No Personally Identifiable Information (PII)/Protected Health Information (PHI) data is store in CRS+ database. CRS+ dataset store standard codes sets, e.g., International Classification of Disease, 10th Edition, Clinical Modification/Procedural Code Ste (ICD10-CM/PCS), Common Procedure Terminology (CPT), Health Common Procedure Code (HCPCS), and Evaluation & Management (E/M) codes.

VistA Integration, Revenue, and Reporting (VIRR) interface with the VistA Health Information System and Technology Architecture (VistA) System. VIRR uses RPC Broker technology, which permits the application end users to retrieve and store data within the VistA Health Information System and Technology Architecture System. The VIP Workplace and CCM modules pass billing and coding data to the VistA packages including Patient Care Encounter, Patient Treatment File, Computerized Patient Record System (CPRS), and Surgery.

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.

CRS+ is an web-application that provides standard codes sets, e.g., International Classification of Disease, 10th Edition, Clinical Modification/Procedural Code Ste (ICD10-CM/PCS), Common Procedure Terminology (CPT), Health Common Procedure Code (HCPCS), and Evaluation & Management (E/M) codes. CRS+ interface with the (Veterans Health Information Systems and Technology Architecture) VistA Integration, Revenue, and Reporting (VIRR) application which uses RPC Broker technology. CRS+ passes health care codes to VIRR. VIRR interface with the VistA packages including Patient Care Encounter, Patient Treatment File, Computerized Patient Record System (CPRS), and Surgery. VIRR application end user require a VistA account with VIRR secondary menu option and security keys.

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.

Health Information Management (HIM) Department Chief, Supervisor, and their designee(s) manages and validates the data by querying the Veterans Health Information Systems and Technology Architecture (VistA) System database and VistA Integration, Revenue, and Reporting (VIRR) application. VIRR interface with the VistA packages including Patient Care Encounter, Patient Treatment File, Computerized Patient Record System (CPRS), and Surgery.

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

Title 38 United States Code (U.S.C.) §§1701, 1703, 1710(c), 1712, 3104 and Title 38 Code of Federal Regulation (CFR) Chapter 17 authorizes the provision of Veterans medical, nursing home, and domiciliary care and associated record-keeping. The applicable System of Records Notices (SORN) are 24VA10A7, Patient Medical Record-VA, and 121VA10A7, National Patient Databases-VA, and would likely not require amendment.

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: There are no privacy risks regarding data stored in Coding & Reimbursement System Plus (CRS+). CRS+ only display the following the following Personally Identifiable Information (PII): Age, Admission Date and Discharge Date. CRS+ does not collect/store Personally Identifiable Information (PII), Protected Health Information (PHI) and other highly delicate Sensitive Personal information (SPI). If this information were to be breached or accidently released to inappropriate parties or the public, it could result in financial, personal, and/or emotional harm to the individuals whose information is contained in the system.

Mitigation: The Department of Veterans Affairs is careful to only collect the information necessary to identify the Veteran in crisis, identify the potential issues and concerns, and offer assistance to the Veteran so that they may find the help they need to get through their crisis. By only collecting the minimum necessary information, the VA can better protect the Veterans' information. Users are trained on how to handle sensitive information by taking VA Privacy and Security Awareness Training and reading and attesting they understand the VA Rules of Behavior on an annual basis.

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.

Age: End diagnosis code has a specific age range to differentiate between newborn, pediatrics, and adult
Admission Date: Used to report a patient's diagnosis and services based on his duration of stay
Discharge Date: Used to report the time the healthcare providers provided services to a patient

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

Coding & Reimbursement System Plus (CRS+) does not analyze or produce patient data. CRS+ is designed to provide provides standard codes sets, e.g., International Classification of Disease, 10th Edition, Clinical Modification/Procedural Code Ste (ICD10-CM/PCS), Common Procedure Terminology (CPT), Health Common Procedure Code (HCPCS), and Evaluation & Management (E/M) codes to Health Information Management (HIMS) Department users and Veterans Health Administration (VHA) coders.

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

Data is encrypted when it resides in Veterans Health Information Systems and Technology Architecture (VistA) System, and when it is being transmitted on the VA network.

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

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

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

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

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

Add answer here:

Coding & Reimbursement System Plus (CRS+) application is used by the Health Information Management (HIMS) Department users and Veterans Health Administration (VHA) coders; and interface with the VistA Integration, Revenue, and Reporting (VIRR) application which require a VistA account and VIRR secondary menu options and security keys.

Local VHA site Administrative Officer/Supervisor/ADPAC/designee(s) submit an ePAS/NARS request. New user's Veterans Health Information Systems and Technology Architecture (VistA) ePAS/NARS request will include VistA menu options/security keys, Clinical Patient Record System (CPRS) access, VistA Imaging System access, etc. There are application-specific VistA menu option/security keys.

Local VHA site OI&T is responsible to complete the ePAS/NARS request. The following is the Coding & Reimbursement System Plus (CRR+) user's requirements:
VistA Integration, Revenue, and Reporting (VIRR) application VistA secondary menu options
VistA Integration, Revenue, and Reporting (VIRR) application VistA security keys
VistA Default Division

All VHA staff are responsible for assuring safeguards for the Personally Identifiable Information (PII), Protected Health Information (PHI) and other highly delicate Sensitive Personal information (SPI). Organizational and Non-Organizational users are required to take the Talent Management System (TMS) VA Privacy and Information Security Awareness and Rules of Behavior Training yearly. VHA facilities ISSO is responsibility to monitor VistA access and verify the TMS training has been completed and current.

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

Coding & Reimbursement System Plus (CRS+) does not retained Personally Identifiable Information (PII), Protected Health Information (PHI) and other highly delicate Sensitive Personal information (SPI). CRS+ interface with the VistA Integration, Revenue, and Reporting (VIRR) application which interface with the Veterans Health Information Systems and Technology Architecture (VistA) System.

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.

CRS+ interface with the VistA Integration, Revenue, and Reporting (VIRR) application. VIRR interface and store data in the Veterans Health Information Systems and Technology Architecture (VistA) System which is to be maintained indefinitely. Whenever technically feasible, all records are retained indefinitely in the event of additional follow-up actions on behalf of the individual. VA Electronic Health Records (ERM) system permanently retains data as part of ongoing healthcare.

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.

SORN 24VA10A7 states: "In accordance with the records disposition authority approved by the Archivist of the United States, paper records and information stored on electronic storage media are maintained for seventy-five (75) years after the last episode of patient care and then destroyed/or deleted. VHA Records Control Schedule (RCS 10–1), Chapter 6, 6000.1d (N1–15–91–6, Item 1d) and 6000.2b (N1–15–02–3, Item 3).

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

CRS+ interface with the VistA Integration, Revenue, and Reporting (VIRR) application. VIRR interface and store data in the Veterans Health Information Systems and Technology Architecture (VistA) System which is to be maintained indefinitely as long as necessary; the records are all electronic (no paper). No records have ever needed to be destroyed, whenever technically feasible, all records are retained indefinitely in the event of additional follow-up actions on behalf of the individual. VA Electronic Health Records (EHR) system permanently retains data as part of ongoing healthcare.

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

Coding & Reimbursement System Plus (CRS+) new releases are not National installation prior to testing. With an approved MOU (Memorandum of Understanding) from the IOC site(s), the vendor, 3M Health Information Systems, Inc., new releases are installed and tested in the CRS+ Pre-Production Test System. IOC site(s) tester(s) complete the Test Site(s) User's Acceptance CRS+ Pre-Production System document prior to CRS+ Production System installation.

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:

<u>Principle of Minimization:</u> 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?

<u>Principle of Data Quality and Integrity:</u> 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:
<u>Privacy Risk:</u> Data is not stored in Coding & Reimbursement System Plus (CRS+). The greater risk is that the information could be compromised or breached in the Veterans Health Information Systems and Technology Architecture (VistA) System.

<u>Mitigation:</u> <If the Coding & Reimbursement System Plus (CRS+) information on the Veterans Health Information Systems and Technology Architecture (VistA) System is part of ongoing research or health care support, the information should be retained for as long as necessary to fulfill the requirements.

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 Health Information Systems and Technology Architecture (VistA)	Retrieve and store clinical data within the Veterans Health Information and Technology Architecture (VistA) System. Coding & Reimbursement System Plus (CRS+) is designed to ensure coding accuracy supporting the coding, auditing, and billing functions using industry standard capabilities to ensure data accuracy for these purposes. Application provides users with support for selecting Evaluation & Management (E/M) codes, International Classification of Diseases 10 (ICD10) codes, Clinical Modification/Procedural Code Set (ICD10-CM/PCS) codes, Healthcare Common Procedure Coding System (HCPCS) codes and Common Procedure Terminology (CPT) codes. CRS+ interface with VistA	Age, Admission Date, Discharge Date	RPC Broker Technology which permits the application end users to retrieve and store health coding data within the Veterans Health Information Systems and Technology Architecture (VistA).

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*
	Integration, Revenue, and Reporting (VIRR) s which interface with the VistA packages including Patient Care Encounter, Patient Treatment File, Computerized Patient Record System (CPRS), and Surgery.		

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 maintaining PII/PHI is that sharing data within the Department of Veteran’s Affairs could happen, and that data may be disclosed to individuals who do not require access and heightens the threat of the information being misused.

Mitigation: The principle of need-to-know is strictly adhered to by the population Healthcare and non-Healthcare providers. Only personnel with a clear business purpose are allowed access to the system and the information contained within the system. Users are trained how to handle sensitive information by taking VA Privacy and security awareness training and reading and attesting they understand the VA Rules of Behavior on an annual basis.

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***
N/A	N/A	N/A	N/A	N/A

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

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

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a

Memorandum Of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.
Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.
This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:
Privacy Risk: N/A

Mitigation: N/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.

All data in Coding & Reimbursement System Plus (CRS+) is secondary data, extracted from VistA data. The VistA data is generated as part of routine medical care. Veterans are provided with Privacy Act statements as part of routine medical care. All enrolled Veterans and Veterans who are treated at VA Medical Centers but not required to enroll are provided the VHA Notice of Privacy Practices (NoPP) every three years, or sooner if a change necessitates an updated notice. The NoPP is also prominently posted in every VAMC (posters) and on the VA public-facing website.

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

CRS+ extracts data that exists that was generated in the course of routine medical care. Patients can in general decline to provide information in routine medical care. Individuals should view the PIA for their local facility VistA to see whether they can consent to their information being used or decline it being used.

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

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

The Privacy Act and VA policy require that personally identifiable information only be used for the purpose(s) for which it was collected, unless consent (opt-in) is granted. Individuals must be provided an opportunity to provide consent for any secondary use of information, such as use of collected information for marketing.

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

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

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

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

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

Follow the format below:
<u>Privacy Risk:</u> There are no risks associated with the information since no individual PII, PHI or SPI is collected and maintained in CRS+ and the data is not for individual use or identification.

Mitigation: No PII, PHI, SPI information is collected in CRS+. Application does not allow individuals to enter PII, PHI or SPI data.

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.

VHA Directive 1605.01 Privacy and Release of Information, Paragraph 7(b) states the rights of the Veterans to request access to review their records. VA Form 10-5345a, Individual's Request for a Copy of Their Own Health Information, may be used as the written request requirement. All requests to review must be received by direct 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 concerned VHA system of records, the facility Privacy Officer, or their designee. Each request must be date stamped and reviewed to determine whether the request for access should be granted.

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 Directive 1605.01 Privacy and Release of Information, Paragraph 8 states the rights of the Veterans to amend their records. 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. 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.

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.

Notification for correcting the information must be accomplished by informing the individual to whom the record pertains. The individual requesting the amendment must be advised in writing that the record has been amended and provided with a copy of the amended record. The System Manager for the concerned VHA system of records, the facility Privacy Officer, or their designee, must notify the relevant persons or organizations who had previously received the record about the amendment. If 38 U.S.C. 7332- protected information was amended, the individual must provide written authorization to allow the sharing of the amendment with relevant persons or organizations. Request to amend a record must be acknowledged in writing within 10 workdays of receipt. If a determination has not been made within this time period, the System Manager for the concerned VHA system of records or designee, and/or the facility Privacy Officer, or designee, must advise the individual when the facility expects to notify the individual of the action taken on the request. The review must be completed as soon as possible, in most cases within 30 workdays from receipt of the request. If the anticipated completion date indicated in the acknowledgment cannot be met, the individual must be advised, in writing, of the reasons for the delay and the date action is expected to be completed. The delay may not exceed 90 calendar days from receipt of the request.

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.

No individual PII, PHI or SPI is collected or maintained in CRS+ and therefore this control is not applicable to individuals.

7.5 <u>PRIVACY IMPACT ASSESSMENT: Access, redress, and correction</u>

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

<u>Principle of Individual Participation:</u> 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?

<u>Principle of Individual Participation:</u> 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:
<u>Privacy Risk:</u> N/A

<u>Mitigation:</u> N/A

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.

Local VHA site Administrative Officer/Supervisor/ADPAC/designee(s) submit an ePAS request for new application user's Veterans Health Information Systems and Technology Architecture (VistA) System account and the new application users have completed the Talent Management System (TMS) VA Privacy and Information Security Awareness and Rules of Behavior Training.
Local VHA site OI&T is responsible to complete the ePAS request.

OI& Technical staff complete the ePAS approval for System Administrator (grant server access), Application Administrator (manage application), VistA Management (manage VistA System related tasks). Talent Management System (TMS) Inform Security for IT Specialist, Information Security for System Admin, Elevated Privileges for System Access, and VA Privacy and Information Security Awareness and Rules of Behavior Training, Information Security and Privacy Role-Based Training for System Administrators (WBT), and Contingency Planning – Role Based Training.
Non-Mail enabled account (NMEA) and associated token (USB/OTP) to access the servers.
Note: Organizational and Non-Organizational users are required to take the Talent Management System (TMS) VA Privacy and Information Security Awareness and Rules of Behavior Training yearly.

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 Contractors do not have access to CRS+ and do not have input into the design and maintenance of the system.

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately.
This question is related to privacy control AR-5, Privacy Awareness and Training.

Personnel that will be accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB (for AITC technicians) prior to gaining access to any VA information system or sensitive information. The rules are included as part of the 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 security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system. All VA employees must complete annual HIPAA, Privacy and Security training. Users agree to comply with all terms and conditions of the National Rules of Behavior, by signing a certificate of training at the end of the training session.

Organizational and Non-Organizational users are required to take the Talent Management System (TMS) VA Privacy and Information Security Awareness and Rules of Behavior Training yearly.

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

If Yes, provide:

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

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

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

Coding & Reimbursement System Plus (CRS+) Full ATO package was reviewed and granted a 180-Day ATO on December 2, 2021with High FIPS 199 classification. ATO termination date is May 30, 2022. The Security Plan status is approved, and status date is March 14, 2022.
Security Plan Status Date: March 14, 2022. Risk Review was completed on September 22, 2021, and FIPS 199 classification is High. Artifacts have been added to eMASS.

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.

N/A

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.

N/A

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.

N/A

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.

N/A

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).

N/A

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.

CHRISTIAN LOFTUS

Digitally signed by CHRISTIAN LOFTUS
Date: 2022.04.08 14:04:20 -04'00'

Privacy Officer, Christian D. Loftus

Roland B Parten 596219

Digitally signed by Roland B Parten 596219
Date: 2022.04.08 12:22:10 -05'00'

Information System Security Officer, Roland Parten

Gail J. Nemetz 117486

Digitally signed by Gail J. Nemetz 117486
Date: 2022.04.08 11:58:57 -04'00'

Information System Owner, Gail J. Nemetz

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).

VHA Handbook 1605.04, VHA Notice of Privacy Practices:

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