Privacy Impact Assessment for the VA IT System called:

Cooperative Studies Program (CSP)
Office of Research and Development
Veteran’s Healthcare Administration (VHA)

eMASS ID: 103

Date PIA submitted for review:

May 24, 2024

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Michelle Christiano	Michelle.Christiano@va.gov	706-399-7980
Information System Security Officer (ISSO)	Erick Davis	Erick.Davis@va.gov	512-326-6178
Information System Owner	Temperance Leister	Temperance.Leister@va.gov	484-432-6161

Abstract

The abstract provides the simplest explanation for "what does the system do?".

The CSP-Cooperative Studies Program is a division within the Office of Research & Development within the Department of Veterans Affairs (VA), Veterans Health Administration (VHA). Using its expertise in clinical research, CSP conducts multi-site clinical trials and epidemiological research on key diseases that impact our nation's Veterans. The system hosted at the Austin Information Technology Center (AITC) is used to manage these clinical research initiatives and requires its own ATO. CSP operations and local production systems are covered under the Albuquerque VHA ATO.

Overview

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

1 *General Description*

A. *What is the IT system name and the name of the program office that owns the IT system?*

Cooperative Studies Program (CSP), Office of Research and Development (ORD) of the Department of Veterans Affairs (VA)

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

The Cooperative Studies Program (CSP) is within the Office of Research and Development (ORD) of the Department of Veterans Affairs (VA), Veterans Health Administration (VHA). Using its expertise in clinical research, CSP conducts multi-site clinical trials and research on key diseases that impact our nation's Veterans. The system is used to manage these clinical research initiatives.

The Clinical Trial Management System (CTMS) is comprised of two components. The Enterprise Content Management (ECM) in SharePoint and the Clinical Trials Support Center (CTSC) which is an internal/external facing website. CTSC was used to provide membership services for external SharePoint users. This service is not currently active. CSP is hosted at the Austin Information Technology Center (AITC).

The system has recently completed a technical refresh and is planned for a major change to remove the ECM from the ATO boundary and integrate the CTMS with Single Sign On (SSO).

C. *Who is the owner or control of the IT system or project?*

Department of Veterans Affairs (VA)

2. Information Collection and Sharing

D. What is the expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual?

Data collected for research projects is shared with National Institutes of Health. They are the sponsor of these projects and have Institutional Review Board (IRB) approval. They will typically have anywhere from 100 to 500 participants. Currently there is only one NIH project due for deployment in 2024.

E. What is a general description of the information in the IT system and the purpose for collecting this information?

The Cooperative Studies Program (CSP) is within the Office of Research and Development (ORD) of the Department of Veterans Affairs (VA), Veterans Health Administration (VHA). Using its expertise in clinical research, CSP conducts multi-site clinical trials research on key diseases that impact our nation's Veterans.

The system hosted at the Austin Information Technology Center (AITC) is used to manage these clinical research initiatives. CSP business processes have created the need for an integrated Clinical Trial Management System (CTMS). This system provides a bridge that is available on the VA Intranet as well as the Internet that provides clinical sites functionality to manage their drugs, device, or clinical supply inventory as well as manage participant enrollment, randomization, and drug or device assignment. It provides information to clinical personnel, allows for data collection, data clarification, form collection workflow, adverse event reporting and workflow, and data query tools for auditing and monitoring of ongoing research projects.

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

The CTSC component is used for management of drugs, device, or clinical supply inventory as well as manage participant enrollment, randomization, and drug or device assignment.

G. Is 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?

In some cases, there are sources of information that come from research sites. In these cases, Protected Health Information (PHI) collected by the system could be associated with a study-specific participant identifier. This ensures a participant's health information cannot be linked with a participant without using a special crosswalk code. Crosswalk codes are stored separately from PHI to prevent unintentional links between PII and PHI. This model is applied consistently with both components of the CTMS across all participating sites.

3. Legal Authority and SORN

H. What is the citation of the legal authority to operate the IT system?

The Secretary of Veterans Affairs established these guidelines pursuant to the authorities in and requirements of Title 10 U.S.C. chapters 106a, 510,1606 and 1607 and Title 38, U.S.C. Section 501(a), and Chapters 11, 13, 15,18, 23, 30, 31, 32, 33, 34, 35, 36, 39, 51,53, and 55 provide the legal authority for operating the CSP. The System of Record (SORN) for CSP under the VA Office of Research and Development is listed as 34VA10.

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

No

4. System Changes

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

No

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

No

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. It must also match the information provided in question 3.4 of the PTA.

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

☒ Name
☐ Social Security Number
☐ Date of Birth
☐ Mother's Maiden Name
☐ Personal Mailing Address
☐ Personal Phone Number(s)
☐ Personal Fax Number
☒ Personal Email Address
☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
☐ Financial Information
☐ Health Insurance Beneficiary Numbers Account numbers

□ Certificate/License numbers[1]
□ Vehicle License Plate Number
□ Internet Protocol (IP) Address Numbers
□ Medications
□ Medical Records
□ Race/Ethnicity
□ Tax Identification Number
□ Medical Record Number
□ Gender
□ Integrated Control Number (ICN)
□ Military History/Service Connection
□ Next of Kin
☒ Other Data Elements (list below)

Other unique identifying numbers: Enrollment IDs are used as Crosswalk codes. These allow researchers to link data back to participants in separate systems.
*Name and Personal Email Address are for users of the system only.

PII Mapping of Components (Servers/Database)

CSP's CTMS has been analyzed to determine if any components collect PII elements. The type of PII collected by **Cooperative Studies Program** and the reasons for the collection of the PII are in the table below.

Note: Due to the PIA being a public facing document, please do not include server names in the table.
The first table of 3.9 in the PTA should be used to answer this question.

Internal Components Table

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	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
Production SQL Server	**Yes**	**Yes**	**Enrollment IDs**	Clinical Trial Management	Encryption

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

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

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

[1] *Specify type of Certificate or License Number (e.g., Occupational, Education, Medical)

CSP’s CTMS main operation is to provide information for ongoing research projects. Study site personnel use the site to manage their drugs, device, or clinical supply inventory as well as manage participant enrollment, randomization, and drug or device assignment. This information is used to track usage and resupply sites as needed from the Pharmacy distribution center.

1.2b Describe why information from sources other than the individual is required? For example, if a program’s system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question indicate why the system is using this source of data.

CSP’s CTMS main operation is to provide information for ongoing research projects. CSP provides services to VA as well as non-VA clinical sites. It provides these sites functionality to manage their drugs, device, or clinical supply inventory as well as manage participant enrollment, randomization, and drug or device assignment. CTMS works in conjunction with internal VA Pharmacy Coordinating Center inventory management systems.

1.2c Does the system create information (for example, a score, analysis, or report), list the system as a source of information?

The source for clinical material information comes from production systems at the research pharmacy in Albuquerque. Participant information comes from clinical sites that participate in CSP projects or research partners that manage projects where CSP manufactures and or distributes clinical materials. The system collects usage and tracking information for these clinical materials.

1.3 How is the information collected?

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

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

This information is transferred between SQL databases at the Pharmacy in Albuquerque and the SQL databases hosted at the AITC for the CTMS application.

1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, what is the form’s OMB control number and the agency form number?

Information is not collected on a form. Data from Albuquerque production sources is transmitted directly to databases supporting CTMS. Content from CSP employees, contractors, and study investigators is collected from client server-based applications.

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

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

1.4a Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your *organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.*

Data is checked for completeness by periodic system audits and manual verifications. All custom applications follow a strict validation process.

1.4b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?

No.

1.5 What specific legal authorities, arrangements, and agreements defined the collection of information?

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders. This question is related to privacy control AP-1, Authority to Collect

The Secretary of Veterans Affairs established these guidelines pursuant to the authorities in and requirements of Title 10 U.S.C. chapters 106a, 510,1606 and 1607 and Title 38, U.S.C. Section 501(a) and Chapters 11, 13, 15,18, 23, 30, 31, 32, 33, 34, 35, 36, 39, 51,53, and 55 provide the legal authority for operating the CSP.

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. (*Work with your System ISSO to complete this section)*

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

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

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

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

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

Follow the format below when entering your risk assessment:

Privacy Risk: CSP collects Personally Identifiable Information (PII) and other sensitive Protected Health Information (PHI). If this information was breached or accidentally released to inappropriate parties or the public, it could result in financial loss and diminished participation in our research due to loss of public trust.

Mitigation: The Department of Veterans Affairs is careful to only collect the information necessary to identify the parties involved in an incident, identify potential issues and concerns, and aid the affected parties so that they may find the help they need to get through their crisis. CSP employs a variety of security measures designed to ensure that the information is not inappropriately disclosed or released. These security measures include access control; awareness and training; audit and accountability; certification, accreditation, and security assessments; configuration management; contingency planning; identification and authentication; incident response; maintenance; media protection; physical and environmental protection; planning; personnel security; risk assessment; systems and services acquisition; system and communications protection; and system and information integrity. The CSP application employs all security controls in the respective Moderate impact security control baseline unless specific exceptions have been allowed based on the tailoring guidance provided in NIST Special Publication 800-53 and specific VA directives.

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 that 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.

PII/PHI Data Element	Internal Use	External Use
Name	This is used to identify users of the system. *Does not include study participants	This is used to identify users of the system. *Does not include study participants
Email Address:	This is used to identify and communicate users of the system. *Does not include study participants	This is used to identify and communicate users of the system. *Does not include study participants
Enrollment ID:	This is used as a unique identifier assigned to participants after they have been registered in a research protocol.	This is used as a unique identifier assigned to participants after they have been registered in a research protocol.

2.2 What types of tools are used to analyze data and what type of data may be produced?
These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

2.2a Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis?

CSP utilizes systems and tools that are VA Technical Reference Model (TRM) approved for use within the VA. Data is analyzed in compliance with Section 552a (e)(2) of the Privacy Act of 1974 to enhance public confidence that any PII collected and maintained by VA is accurate, relevant, timely, and complete for the purpose for which it is to be used. Data generated from analysis is done outside of the CSP system. It is maintained and stored on the VA network according to each study's protocol and data management plan. Data management plan is reviewed and approved by the research sites ISSO and PO.

2.2b If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.

No

2.3 How is the information in the system secured?
These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

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

Data in transit is protected by SSL encryption certificates which are renewed annually. Data at rest is encrypted at the storage level using ONTAP 9.6 version & AFF A700 is the Netapp storage array.

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

Doesn't collect SSNs.

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

In order to protect participant personally identifiable information/protected health information (PII/PHI) the following activities occur as part of the overall information assurance activities:

1. The information with each application is categorized in accordance with Federal Information Processing Standard (FIPS) 199 and NIST SP 800-60. As part of the categorization any PII is identified.

2. The VA has policies which direct and guide the activities and processes performed by the VA. The policies are periodically reviewed to ensure completeness and applicability.

3. The NIST SP 800-53 controls are selected based on the categorization. The controls provide protection for PII while developed or stored by an application or IT system, physically transported, between facilities, least privilege, stored offsite, or transmitted between IT centers.

4. If there is any PII in the CSP encrypted database, it's not exposed on the front end and it's built into a separate schema so that it's not accessible from the web interface. CSP employs transport layer protocol security (TLS) and for encryption at rest CSP uses the VM encryption and then during transit CSP uses HTTPS for the web server.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

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

2.4a How is access to the PII determined?

Access to CSP PII is determined through role base access control (RBAC), and least privilege.

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

CSP access criteria, procedures, controls, and responsibilities are documented in CSP Access Control (AC) and Privacy Standard Operating Procedures (SOPs).

2.4c Does access require manager approval?

Yes, access to any CSP data requires manager’s approval.

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

SQL Database triggers and audit logs.

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

The Information System Owner (ISO) is responsible for safeguarding PII.

Section 3. Retention of Information

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

3.1 What information is retained?

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

Enrollment ID.- Participants only
Name – System users only
Personal Email Address – System users only

3.2 How long is information retained?

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

The records contained in this system have not been scheduled and will be kept indefinitely until such time as they are. The records may not be destroyed until VA obtains an approved records disposition authority Version Date: May 1, 2021, Page 10 of 34 from the Archivist of the United States. System of Record currently entitled ‘‘Veteran, Patient, Employee, and Volunteer Research and Development Project Records—VA’’ (34VA10).

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

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

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

Yes.

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

The records may not be destroyed until VA obtains an approved records disposition authority from the Archivist of the United States. System of Record currently entitled ''Veteran, Patient, Employee, and Volunteer Research and Development Project Records—VA'' (34VA10).

3.4 What are the procedures for the elimination or transfer of SPI?

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

Data that is collected is destroyed in accordance with RCS 10-1. The specific process is to shred documents, place into locked bins, and have contents incinerated. Paper documents are destroyed to an unreadable state in accordance with the Department of Veterans' Affairs VA Directive 6371, (April 8, 2014), VA Publications.

Electronic data and files of any type, including Protected Health Information (PHI), Sensitive Personal Information (SPI), Human Resources records, and more are destroyed in accordance with VA Directive 6500 VA Cybersecurity Program (February 24, 2021) and VA Handbook 6500.1 Electronic Media Sanitization. When required, this data is deleted from their file location and then permanently deleted from the deleted items or Recycle bin. Magnetic media is wiped and sent out for destruction. Digital media is shredded or sent out for destruction. https://www.va.gov/vapubs/search_action.cfm?dType=1

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

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

It is CSPs policy to only use test data in development and pre-production. All pre-production applications are populated with test data so they can be used for testing and training. Associated system specific PII(s) listed in Section 1, are never used for testing information systems in development or pre-production prior to deploying to production. Test data is used to ensure the system generates notifications correctly and flows through the workflows correctly.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

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

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

Follow the format below:

Privacy Risk: There is a risk that the information maintained by CSP could be retained for longer than is necessary to fulfill the VA mission. Records held longer than required are at greater risk of being unintentionally released or breached.

Mitigation: The records contained in this system have not been scheduled and will be kept indefinitely until such time as they are. The records may not be destroyed until VA obtains an approved records disposition authority from the Archivist of the United States. System of Record currently entitled ‘‘Veteran, Patient, Employee, and Volunteer Research and Development Project Records—VA’’(34VA10).

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
VA Office of Research & Development (ORD), National Institutes of Health (NIH)	Data collected by the CSP CTMS in support of VA ORD sponsored projects is available to authorized study team members (VA ORD personnel). Project teams require access to their project data to execute study protocols approved by their Institutional Review Board (IRB) of record.	PII/PHI data elements: - Enrollment ID. Data element is study specific. Currently, there are no non-CSP, VA ORD projects hosted by the system. There is one research project that will be deployed later this year (2024) PII is stored in a separate database from PHI. PHI collected is associated with a study encoded participant identifier and cannot be readily linked to an individual without a crosswalk code. All data elements are associated with a study encoded participant identifier and cannot be readily linked to an individual without a crosswalk code which is not collected or stored in the system.	Data retrieval is only available within the VA network.

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

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

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

Follow the format below:

Privacy Risk: Privacy risk is limited to enrollment ID.

Mitigation: PII is stored in a separate database from PHI so health information can only be linked to a specific participant with a special crosswalk code. The only access to PII is through an internally hosted website that is only available within the VA intranet and only accessible to personnel approved by the project's leadership. Windows authentication is used to authenticate user. Access and permissions are controlled by the study team and are role-based to limit data to need-to-know.

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.

If no External Sharing listed on the table above, ***(State there is no external sharing in both the risk and mitigation fields).***

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:

<u>Privacy Risk:</u> No privacy risk exists as all data collected for use by external entities is limited to enrollment IDs and inventory management.

<u>Mitigation:</u> 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 6.1 on the last page of the document. Also

provide notice given to individuals by the source system (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?

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

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

A privacy notice is provided to research participants prior to participation. All participants must also sign a HIPPA acknowledgement form. The informed consent form or information sheet for each study provides information on how their data will be used. A partial screen shot of typical verbiage can be seen in Appendix A-6.1.

All PII and PHI besides the enrollment IDs are managed on separate systems so this may be irrelevant to this PIA document.

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

Not Applicable. Individuals cannot participate in research without informed consent.

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

Each Privacy Act statement in the study forms explains the purpose of the information collected, copies of each form's Privacy Act Information.

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.

All information provided by consenting clinical trial participants is done so voluntarily. They can also decline to participate in the research project without penalty or denial of service.

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.*

Each research study has its own specific informed consent form which outlines data collection and use. Each informed consent form must be reviewed and approved by the Institutional Review Board of record.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

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

Privacy Risk: Clinical trial data collected for non-consented participants.

Mitigation: Participants cannot access the system. Participants must first consent to participate in a study before being enrolled. Upon successful enrollment, the participant is assigned a unique identifier that is used for identification. The crosswalk for this identifier and the PII is maintained separately. Login information is assigned to the study unique identifier, so site personnel are prevented from recording information without first going through the enrollment process. Operational data for resupply of materials to sites is low risk and has no associated PII. Assignments are tied to the crosswalk codes.

Section 7. Access, Redress, and Correction

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

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

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

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

As outlined in the System of Record Notice (SORN) CSP 34VA10, in the Record Access Procedures, individuals seeking content of records should contact the system manager.

If someone or their authorized representative are requesting medical records associated with CSP data, at minimum will follow the FOIA request process. The informed consent and/or HIPAA Authorization will notify the participant if they'll have access to their research data.

All PII and PHI besides the enrollment IDs are managed on separate systems so this may be irrelevant to this PIA document.

7.1b If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR)?

CSP is not exempt from the access provisions of the Privacy Act.

7.1c If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information?

CSP is a Privacy Act System.

7.2 What are the procedures for correcting inaccurate or erroneous information?

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed? If the correction procedures are the same as those given in question 7.1, state as much. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Operational data collected for resupply of clinical materials to sites is low risk and has no associated PII. Assignments for medication are tied to the crosswalk codes. CSP data corrections are dictated by study protocol. Typically, administrators will be directed by study team leads on what and how when discrepancies occur.

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.

Individuals would be notified of the Enrollment ID they are assigned and if it is changed. Participants do not have access to correct their own information.

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and

Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems.
Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Individuals would be notified of the Enrollment ID they are assigned and if it is changed. Participants do not have access to correct their own information..

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

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

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

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

Follow the format below:

Privacy Risk:

Although unlikely, if participant is assigned an incorrect enrollment ID, they could receive incorrect therapy treatment.

Mitigation:

Study personnel are required to enter check codes when entering enrollment IDs.

Section 8. and Security

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

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

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

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

Clinical studies hosted by the Cooperative Studies Program (CSP) system can be classified as Drug/Device studies. Drug/Device studies are used by study personnel to manage logistical information (i.e. supply-chain management, ancillary supply management).

8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

Drug/Device Studies: These study websites are limited to authorized study personnel. Each study has one or more moderators designated at the beginning of the study. These moderators review all future access requests and control access/permissions to their study website. When a new user desires access to a study website, he/she must complete an online registration form that establishes enough information so a moderator may determine whether the user should be granted access. Typically, this involves name, email, study site number (hospital number), and role within the study. The study moderator will review the access request and determine whether the user should be granted access to the system. These users are typically study coordinators or study sponsor delegates.

8.1c Describe the different roles in general terms that have been created to provide access to the system? For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

Users are limited by their role in the projects. Examples of these roles are:

View only user (monitor, auditor)
Site User
Study Team
Study Team lead (Moderator)
CSP Administrator

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

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII. This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.

Yes, contractors will have access to the system. Access is required to provide technical support and data management tasks. Contracts are reviewed annually at a minimum. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of behavior training via the VA's TMS. All contractors are cleared using the VA background investigation process and must obtain a Moderate Background Investigation (MBI).

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.

Individuals who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of behavior training via the VA's TMS. Users are required to complete information system security training activities including annual security awareness training and specific information system security training. The training records are retained for 7 years. This documentation and monitoring are performed using the Talent Management System (TMS).

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* September 22, 2023
3. *The Authorization Status:* Authorization to Operate
4. *The Authorization Date:* July 16, 2023
5. *The Authorization Termination Date: July* 15, 2023
6. *The Risk Review Completion Date:* June 28, 2023
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

8.4b If No or In Process, provide your ***Initial Operating Capability (IOC) date.***
CSP has current authorization. See response for 8.4A

Section 9 – Technology Usage

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

9.1 Does the system use cloud technology? If so, what cloud model is being utilized?
If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS),

Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.
Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1*. (Refer to question 3.3.1 of the PTA)*

Not Applicable. The Cooperative Studies Program components are hosted on-premises in the Austin Information Technology Center and do not use cloud technology.

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

Not Applicable. The Cooperative Studies Program components are hosted on-premises in the Austin Information Technology Center, and do not utilize cloud technology or maintain a contract with a Cloud Service Provider.

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.

Not Applicable. The Cooperative Studies Program components are hosted on-premises in the Austin Information Technology Center, and do not utilize cloud technology, so no CSP is collecting ancillary data.

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.

Not Applicable. The Cooperative Studies Program components are hosted on-premises in the Austin Information Technology Center, and do not utilize cloud technology, therefore no data is held by a cloud provider and the NIST 800-144 statement is not applicable.

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).*

Not Applicable. The Cooperative Studies Program components are hosted on-premises in the Austin Information Technology Center, and do not utilize Robotics Process Automation, Bots, or Artificial Intelligence.

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**
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.

MICHELLE CHRISTIANO

Digitally signed by MICHELLE CHRISTIANO
Date: 2024.07.12 07:54:54 -04'00'

Privacy Officer,Michelle Christiano

ERICK DAVIS

Digitally signed by ERICK DAVIS
Date: 2024.07.15 09:50:21 -05'00'

Information System Security Officer, Erick Davis

TEMPERANCE LEISTER

Digitally signed by TEMPERANCE LEISTER
Date: 2024.07.15 09:39:03 -05'00'

Information System Owner, Temperance Leister

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; screen shot of a website collection privacy notice).

https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=8928

HELPFUL LINKS:

General Records Schedule
https://www.archives.gov/records-mgmt/grs.html

National Archives (Federal Records Management):
https://www.archives.gov/records-mgmt/grs

VA Publications:
https://www.va.gov/vapubs/

VA Privacy Service Privacy Hub:
https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):
VHA Notice of Privacy Practices
VHA Handbook 1605.04: Notice of Privacy Practices