Privacy Impact Assessment for the VA IT System called:

Cooperative Studies Program (CSP)

Veterans' Healthcare Administration (VHA)

Date PIA submitted for review:

December 7, 2020

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Grewal, Rita K.	Rita.Grewal@va.gov	202-632-7861
Information System Security Officer (ISSO)	Carroll, Tristan M.	Tristan.carroll@va.gov	210- 617-5300
Information System Owner	Brown, Christopher	Christopher.Brown@va.gov	202-270-1432

Abstract

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

The CSP-Cooperative Studies Program is a division within the Clinical Science Research & Development Service of the Department of Veterans Affairs (VA), Veterans Health Administration (VHA) Office of Research and Development. 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:

- *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.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *If your system is a regional GSS, VistA, or LAN, include a list of the hospitals/medical centers, or other regional offices that fall under your system. Additionally, what region is the system under?*
- *A general description of the information in the IT system.*
- *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?*
- *Does the system use cloud technology? If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517.*

- *Does a contract with Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII?*
- *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 is the magnitude of harm if privacy related data is disclosed, intentionally or unintentionally? Would the reputation of the CSP or its customers (VA) be affected?*

The CSP-Cooperative Studies Program is a division within the Clinical Science Research & Development Service of the Department of Veterans Affairs (VA), Veterans Health Administration (VHA) Office of Research and Development. 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.

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 mange 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.

The CTMS is comprised of two components. The Enterprise Content Management (ECM) in SharePoint and the Clinical Trials Support Center (CTSC) which is an external facing website. CTSC is used to provide membership services for external SharePoint users. There is currently no PII or PHI on the ECM component, so this PIA only applies to specific projects on CTSC. Currently the only project collecting PII is the Heath for Every Veteran project. PHI collected is associated with study encoded participant identifiers and cannot be readily linked to individuals without crosswalk codes. Data collected for this project is only shared with Health Science Research and Development (HSR&D). They are the sponsor of the project and have Central Institutional Review Board (CIRB) approval. These projects typically have anywhere from 100 to 2500 participants.

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 operation. The System of Record (SORN) for CSP under the VA Office of Research and Development is listed as 34VA12.

Section 1. Characterization of the Information

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

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

Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy- Protected Information. For additional information on these information types and definitions, please see VA Directives and Handbooks in the 6500 series (https://vaww.va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

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

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

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

PII Mapping of Components

CTMS consists of two key components but only one is used to collect PII. Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by CTMS and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

PII Mapped to Components

Components of the information system (servers) 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
CTSC	**Yes**	**Yes**	Name Social Security Number Date of Birth Phone Number(s) Mailing Address Email Address Emergency Contact Information Enrollment ID	Participant Reimbursement	**Encryption**
CTMS	**No**	**N/A**	**N/A**	**N/A**	**N/A**

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.

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 mange participant enrollment, randomization, and drug

or device assignment. 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 drug supplies.

Another critical function of the CTMS is for content management. The source of this information comes from CSP employees and contractors that manage research workflow. This is typically adverse event reporting and workflow, and data query tools for the auditing and monitoring of ongoing research projects.

In rare cases there are sources of information that come from research participants. These are typically surveys collecting information about patient's quality of life. In these cases, Personal Health Information (PHI) collected by the system is associated with a study-specific participant identifier. This ensures a Veteran's health information cannot be linked with a Veteran without using a special crosswalk code. Crosswalk codes are stored separately from PHI to prevent unintentional links between PII and PHI.

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.

Data from Albuquerque production sources is transmitted directly to databases supporting CTMS. Content from CSP employees, contractors, study investigators, and participants is collected from client server-based applications. SharePoint is used for the content management and CTSC custom applications are used for all other CSP research operational activities.

1.4 What is the purpose of the information being collected, used, disseminated, created, or maintained?

Include a statement of why the particular SPI is collected, maintained, used, or disseminated in the system is necessary to the program's or agency's mission. Merely stating the general purpose of the system without explaining why this particular type of information should be collected and stored is not an adequate response to this question.

If the system collects, uses, disseminates, or maintains publicly available or commercial data, include a discussion of why commercial data is relevant and necessary to the system's purpose.

This question is related to privacy control AP-2, Purpose Specification.

Through collaborative efforts within VA and with other federal, university, and private industry partners, CSP accomplishments have included key research findings across a range of diseases and have helped to provide definitive evidence for clinical practice within the VA and the nation. From its initial beginnings in the 1940s, the CSP continues to be a national and international leader in clinical research.

1.5 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.

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

1.6 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.

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

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

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

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

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

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

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

Follow the format below when entering your risk assessment:
Privacy Risk: CSP collects Personally Identifiable Information (PII) and other highly delicate Personal 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.
Our facility employs all security controls in the respective high 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 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.

Name: Veteran's identification.

Social Security Number: used to verify Veteran identity and as a file number for Veteran.

Phone Number(s): Used for correspondence with the Veteran.

Date of Birth: Require for inclusion exclusion criteria.

Mailing Address: Used for correspondence with the Veteran.

Email Address: Used to verify the identity of the Veteran who is being reviewed.

Emergency Contact Information: Needed for emergencies when family members need to be contacted.

Enrollment ID: This is 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?

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

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.

2.3 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:

The minimum-security requirements for CSP's high impact system cover 17 security-related areas with regard to protecting the confidentiality, integrity, and availability of VA information systems and the information processed, stored, and transmitted by those systems. The security-related areas 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. Our facilities employ all security controls in the respective high 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. VA Records Management Policy and the VA Rules of Behavior in Talent Management System (TMS) govern how Veterans' information is used, stored, and protected.

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

Name, Social Security Number, Phone Number(s), Date of Birth, Mailing Address, Email Address, Emergency Contact Information and Enrollment ID.

3.2 How long is information retained?

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

The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.
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 from the Archivist of the United States. System of Record currently entitled ''Veteran, Patient, Employee, and Volunteer Research and Development Project Records—VA'' (34VA12).

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

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

The 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'' (34VA12).

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

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

Security awareness training is provided to all information system users (including managers, senior executives, and contractors) as part of initial training for new users, when required by system changes, and at least annually thereafter via the VA Talent Management System (TMS).

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 <u>PRIVACY IMPACT ASSESSMENT: Retention of information</u>

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

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

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

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

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

Follow the format below:
Privacy Risk: There is 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'' (34VA12).

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA. NOTE: Question 5 on Privacy Threshold Analysis should be used to answer this question.

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?

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 data element types such as PII/PHI that are shared/received with the Program Office or IT system***	***Describe the method of transmittal***
VA Office of Research & Development (ORD)	Data collected by the CSP CTSC in support of VA ORD sponsored projects is	Data elements are study specific. Currently, there are 3 non-CSP, VA ORD	Data extracts are made available via an internally hosted web server (behind VA
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 data element types such as PII/PHI that are shared/received with the Program Office or IT system***	***Describe the method of transmittal***
Health Science Research and Development (HSR&D)	available to authorized study team members (VA ORD personnel). Project teams require access to their project data to execute study protocols approved by their Research &	projects hosted by the CSP system (no future non-CSP studies are planned to utilize the CSP CTSC). **Heath for Every Veteran project**: This study is the only study that collects PII. PII is	firewall) whose access is restricted to authorized VA study personnel and encrypted using FIPS 140-2 compliant algorithms (HTTPS-TLS1.2 utilizing VA
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 data element types such as PII/PHI that are shared/received with the Program Office or IT system***	***Describe the method of transmittal***
	Development Committee and VA Institutional Review Board (IRB).	stored in a separate database from PHI. PHI collected is associated with a study encoded participant	furnished certificates). **Data extracts are not available through the internet-facing**

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 data element types such as PII/PHI that are shared/received with the Program Office or IT system*	*Describe the method of transmittal*
		identifier and cannot be readily linked to an individual without a crosswalk code. **Weight Loss Project:** This project collects data elements associated with Veteran weight, weight loss, and attributed behaviors (e.g. amount of time spent in vigorous activity each week). 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. **Embedded Fragmentation (VA BLAST) project:** This project collects data elements related to embedded metallic and non-metallic fragments in Veterans. It also collects associated medical information (e.g. adverse events attributed to embedded fragments). All data elements are associated	**portion of the CSP system. The survey sites made available are for data collection only. 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.
This question is related to privacy control UL-1, Internal Use.

Follow the format below:
Privacy Risk: Privacy risk is limited to the Health for Every Veteran project as it is the only VA CTSC project that collects/stores PII. All other project data is stored with and encoded participant identifier. For the Health for Every Veteran project, PII links an individual to the project as a participant.

Mitigation: PII is stored in a separate database from PHI so Veteran health information can only be linked to a specific Veteran 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: This question is #7 in the Privacy Threshold Analysis.

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 data element types such as PII/PHI that are shared/received with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
N/A				

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

No PII/PHI is accessible from outside of the VA network.

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

Follow the format below:
Privacy Risk: No privacy risk exists as all data collected for use by external entities is limited to inventory management. No PII or PHI is collected within the system.

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.

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’’ (34VA12). PII/PHI is only collected from individuals who have volunteered to participate in VA sponsored clinical trials. Prior to a participant being given access to a clinical trial survey, the participant must provide a valid, signed informed consent form to the clinical trial study team. Informed consent forms for each study are reviewed and approved by the study's Research & Development committee as well as the VA Institutional Review Board. Once a participant is enrolled in a study and has given explicit consent to participate in the study, the participant is granted access to the survey tool. At the time of login each participant must review the VA approved system use statement for electronic systems (provided below). In addition, survey questions are not mandatory, participants have the option of completing a survey with missing or incomplete questions.

System Use Warning Statement
This U.S government system is intended to be used by authorized users for viewing and retrieving information only, except as otherwise explicitly authorized. VA information resides on and transmits through computer systems and networks funded by VA. All use is considered to be with an understanding and acceptance that there is no reasonable expectation of privacy for any data or transmissions on Government Intranet or Extranet (non-public) networks or systems. All transactions that occur on this system and all data transmitted through this system are subject to review and action including (but not limited to) monitoring, recording, retrieving, copying, auditing, inspecting,

investigating, restricting access, blocking, tracking, disclosing to authorized personnel, or any other authorized actions by all authorized VA and law enforcement personnel. All use of this system constitutes understanding and unconditional acceptance of these terms. Unauthorized attempts or acts to either (1) access, upload, change, or delete information on this system, (2) modify this system, (3) deny access to this system, or (4) accrue resources for unauthorized use on this system are strictly prohibited. Such attempts or acts are subject to action that may result in criminal, civil, or administrative penalties.

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 clinical trial has its own specific informed consent form which outlines data collection and use. Each informed consent form must be reviewed and approved by a VA Research & Development Committee as well as a VA Institutional Review Board.

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?

Clinical trial data collected for non-consented Veteran.*<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:
Privacy Risk: Clinical trial data collected for non-consented Veteran.

Mitigation: Participants cannot access the system without first consenting to participate in a study and being enrolled in a study. Upon successful enrollment, the participant is assigned a unique identifier that is used to identify the participant. This identifier is not associated with any PII so it disassociates clinical trial data from the participant's PII. Login information is assigned to the study unique identifier, so a participant is 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?

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.

Data collection for clinical trial surveys is a one-time process. While a participant is in the process of completing a survey, he/she may change the answers to his/her survey, but once a survey is

submitted, the survey is locked, and the participant may not revisit the survey, or the information submitted (identical to mailing in a paper survey). In the case of the "Health for Every Veteran" project (the only project to collect PII), a participant may elect to sign into the system and complete a new contact information form. The participant, however, cannot review the contact information once it has been submitted as the system does not allow for the retrieval of PII, only collection. 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.

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.

Data collection for clinical trial surveys is a one-time process. While a participant is in the process of completing a survey, he/she may change the answers to his/her survey, but once a survey is submitted, the survey is locked, and the participant may not revisit the survey, or the information submitted (identical to mailing in a paper survey). In the case of the "Health for Every Veteran" project (the only project to collect PII), a participant may elect to sign into the system and complete a new contact information form. The participant, however, cannot review the contact information once it has been submitted as the system does not allow for the retrieval of PII, only collection. 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.

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.

Survey data may not be corrected upon submission. In the case of the "Health for Every Veteran" project, participants are notified they may update contact information through in-system prompts.

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.

Survey data may not be corrected upon submission. In the case of the "Health for Every Veteran" project, participants are notified they may update contact information through in-system prompts.

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:
Privacy Risk: "Health for Every Veteran" is the only applicable project as all other projects simply collect deidentified clinical trial survey information. In the case of the "Health for Every Veteran" project, PII is only collected for the purpose of reimbursement of study participation. Risk of incorrect contact data is delay in participant reimbursement.

Mitigation: Participants in the "Health for Every Veteran" project may reenter contact information through the survey website.

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.

Clinical studies hosted by the Cooperative Studies Program system can be classified into two major categories: Drug/Device studies and Survey studies. Drug/Device studies are used by study personnel to manage logistical information (i.e. supply-chain management, ancillary supply management). Survey studies are used by Veteran study participants to record deidentified health information. Each category of study has its own access process.

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. In addition, the user must specify a unique username and password that conforms to the system's strong password criteria (minimum of 8 characters, must include a lower-case letter, upper-case letter, number, and special character). The study moderator will review the access request and determine whether the user should be granted access to the system.

Survey Studies
Survey studies are limited to participants enrolled in the study. Potential participants are screened to ensure they meet the studies inclusion/exclusion criteria as described in the study protocol. If a participant is eligible to participate in the study, they are given an informed consent form and information necessary to make a conscious decision as to whether they wish to participate in the study. If the participant signs the informed consent, the study team enrolls the participant into the study and assigns them a unique participant ID which is used to identify the participant within the study. In addition, they will provide the participant with the URL to login to the study website and the access code associated with the participant ID number. The study team will also unlock the survey for the participant to allow them to complete the survey upon successful login. Once the participant completes and submits the survey, the survey is locked, and the participant is no longer able to access the form, or any information submitted with the form. If the study utilizes multiple surveys (typically collected at different time points), the study team will unlock subsequent surveys and notify the participant that the new survey is available for completion within the website.

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 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 through the use of the Talent Management System (TMS).

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

If Yes, provide:

1. *The date the Authority to Operate (ATO) was granted,*
2. *Whether it was a full ATO or ATO with Conditions,*
3. *The amount of time the ATO was granted for, and*

4. *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.***

ATO Granted 3/5/2020 Decision: 180-Day

The FIPS 199 classification of CSP is High

Section 9. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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

Signature of Responsible Officials

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

RITA K GREWAL 114938

Digitally signed by RITA K GREWAL 114938
Date: 2021.01.12 12:13:02 -05'00'

PO, Grewal, Rita K.

Tristan M. Carroll 1758903

Digitally signed by Tristan M. Carroll 1758903
Date: 2021.01.12 16:12:29 -06'00'

Information Security Systems Officer, Carroll, Tristan M.

Christopher Brown 101386

Digitally signed by Christopher Brown 101386
Date: 2021.01.12 15:22:52 -06'00'

System Owner, Brown, Christopher

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).