Privacy Impact Assessment for the VA IT System called:

D365: Cooperative Studies Program Clinical Research Pharmacy Coordinating Center

Veterans Health Administration

Office of Research and Development (ORD)

eMASS ID #2658

Date PIA submitted for review:

06/05/2025

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)	Albert Comple	Albert.Comple@va.gov	303-914-5439
Information System Owner	Russell Holt	Russell.Holt2@va.gov	970-501-0552

Abstract

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

The D365: Cooperative Studies Program Clinical Research Pharmacy Coordinating Center (D365 CSP PCC) project is set up to allow the capture of financial and internal employee data. This system will allow the financial tracking of the internal and external study budget information. Additionally, it will provide status updates and tracking of requested internal orders. This financial information is used to track internal and external study budget trends. This system will provide requested internal employee data to the Office of Research and Development (ORD) Cooperative Studies Program (CSP). The information collected is used to internally populate a PowerBI dashboard for CSP CRPCC's leadership to monitor trends.

Overview

The overview is the most important section of the Privacy Impact Assessment (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 business purpose of the program, IT system, or technology and how it relates to the program office and agency mission?*

The D365: Cooperative Studies Program Clinical Research Pharmacy Coordinating Center (D365 CSP PCC) system will capture financial and internal employee data for research study budgets/orders and allow leadership to monitor trends. This D365 system will replace a legacy spreadsheet tracking system and allow for role limiting and auditing.

B. *Who is the owner or has control of the IT system or project? If the system has an eMASS entry, ensure this information matches with the eMASS entry.*

The D365 CSP PCC system is owned by Veteran Affairs (VA) Veterans Health Administration (VHA) Office of Research and Development (ORD) Cooperative Studies Program (CSP).

2. *Information Collection and Sharing*

C. *Indicate the expected number of individuals whose information is stored in the system and include a brief description of the typical client or affected individual?*

The D365 CSP PCC system will be utilized by approximately 20 internal Veterans Affairs employees.

Check if Applicable	Demographic of individuals
☐	Veterans or Dependents
☒	VA Employees
☒	Clinical Trainees
☐	VA Contractors
☒	Members of the Public/ Individuals
☐	Volunteers

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

The D365 CSP PCC system will capture financial and internal employee data for study budgets/orders and allow leadership to monitor trends.

E. *What information sharing is conducted by the IT system? A general description of the modules and components, where relevant, and their functions.*

The D365 CSP PCC system will not share information with any internal VA systems nor any external systems.

F. *Are the modules/subsystems only applicable if information is shared?*

No external modules/subsystems are involved.

G. *Is the system operated in more than one site to include primary and secondary 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?*

The D365 CSP PCC is operated via the Microsoft Azure Government Cloud to maintain consistency of PII and controls.

3. Legal Authority and System of Record Notices (SORN)

H. *What is the citation of the legal authority?*

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 38 U.S.C. 501(a); 38 U.S.C. 73; 38 U.S.C. 75 SEC 4202; 5 U.S.C. Part III, Subparts D and E can be found in SORN

171VA056A - Human Resources Information Systems Shared Service Center (HRIS SSC)

SORN Number 34VA10 / 86 FR 33015 Veteran, Patient, Employee, and Volunteer Research and Development Project Records-VA

I. *What is the SORN?*

SORN 171VA056A - Human Resources Information Systems Shared Service Center (HRIS SSC)

SORN Number 34VA10 / 86 FR 33015 Veteran, Patient, Employee, and Volunteer Research and Development Project Records-VA

J. *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval.*

The SORN will not require amendment or revision and approval.

4. System Changes

K. *Will the business processes change due to the information collection and sharing?*

☐ Yes
☒ No
if yes, <<ADD ANSWER HERE>>

I. *Will the technology changes impact information collection and sharing?*

☐ Yes
☒ No
if yes, <<ADD ANSWER HERE>>

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 Information 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
☒ **Full** Social Security Number
☐ **Partial** 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
☐ Sex
☒ Integrated Control Number (ICN)
☒ Military History/Service Connection
☐ Next of Kin
☐ Date of Death
☒ Business Email Address
☐ Electronic Data Interchange Personal Identifier (EDIPI)
☒ Other Data Elements (List Below)

Other PII/PHI data elements:

- Job Title
- Employee ID
- Veteran Status
- Employee Education History
- Employee Licensing Information
- Clinical Trainees ID/Control Number and Amount Charged

1.2 List 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)

The D365: CSP PCC system will collect information directly from individual VA employees and clinical trainees through an application when they are applying for research studies.

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.

Information is not collected from sources other than the individuals applying to the program.

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

The D365: CSP PCC system will create trending reports to allow leadership to monitor trends.

1.3 Methods of information collection

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?

The D365: CSP PCC system will collect information directly from individual VA employees and clinical trainees applying for the service.

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?

The information is not subject to the Paperwork Reduction Act because it is online and not a paper-based application.

1.4 Information checks for accuracy, and 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.

The D365: CSP PCC Workforce Support information is assessed for accuracy during any update. The D365: CSP PCC finance information is checked on a periodic basis for accuracy once transactions entered into the system are completed.

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, the system does not use a commercial aggregator to check for accuracy.

1.5 Identify the specific legal authorities, arrangements, and agreements that 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

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 38 U.S.C. 501(a); 38 U.S.C. 73; 38 U.S.C. 75 SEC 4202; 5 U.S.C. Part III, Subparts D and E can be found in SORN 171VA056A - Human Resources Information Systems Shared Service Center (HRIS SSC)

SORN Number 34VA10 / 86 FR 33015 Veteran, Patient, Employee, and Volunteer Research and Development Project Records-VA

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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

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

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

Principle of Minimization: The information is directly relevant and necessary to accomplish the specific purposes of the program.

Principle of Individual Participation: The program, to the extent possible and practical, collects information directly from the individual.

Principle of Data Quality and Integrity: VA policies and procedures must ensure that personally identifiable information is accurate, complete, and current.
This 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: Sensitive Personal Information (SPI) including personal contact information, SSN and medical information may be released to unauthorized individuals. Unsecured Sensitive Personal Information (SPI) may be exposed. Data breach at the facilities level. Data breach at the network level.

Mitigation: Depending on level of authority granted to the respective user by their home department via the VA, each system user will have sensitivity level of access to veteran data based on role-based permissions. The roles will be reviewed on a regular basis to ensure that appropriate information is shared with appropriate users. All employees with access to Veteran's information are required to complete the VA Privacy, Information Security Awareness training and Rules of Behavior annually. Multilevel security products from leading security vendors and proven security practices ensure network security. To prevent malicious attacks through unmonitored ports, external firewalls allow

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	Identification purposes	Not used
Date of Birth	Identification purposes	Not used
Social Security Number	Identification purposes	Not used
Job Title	Identification purposes	Not used
Employee Business Email	Communication purposes	Not used
Employee ID	Identification purposes	Not used
Physical Work Location	Identification purposes	Not used
Veteran Status	Application information	Not used
Employee Education History	Application information	Not used
Employee Licensing Info	Application information	Not used
Emergency Contact Name	Communication purposes	Not used
Emergency Contact Phone	Communication purposes	Not used
Emergency Contact Relationship	Communication purposes	Not used
Trainee Contact Name	Identification purposes	Not used
Trainee ID/Control Number	Identification purposes	Not used
Trainee Amount Charged	Analysis	Not used

2.2 Describe the types of tools 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?

Reports are generated to review contract and purchasing requirements for evaluation and to gather data for study, building and center expenditures.

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 new information about individuals is created by the system.

2.3 How the information in the system is 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?

In accordance with VA Directive 6500, information within VA system is FIPS 2.0 encrypted. Also, access to system is limited, requires PIV; and access to system and components are audited in accordance with VA Directive 6500.

2.3b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs? (refer to PTA question 3.8).

Social Security Numbers are masked with limited system users having view privileges.

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

Contractor and VA employees are required to take Privacy, HIPAA, and information security training annually. HTTPS using SSL encryption is used between internal VA systems. Personnel accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information.

2.4 <u>PRIVACY IMPACT ASSESSMENT: Use of the information.</u>

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:

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

<u>Principle of Use Limitation:</u> 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?

The mission of the project is to deliver exceptional customer service, and the information stored in the system is used to create a record of a Veteran to ensure timely and accurate assistance is given. Access is determined by the program and upon approval, it is the responsibility of the project making the request to ensure compliance with VA regulations and policies regarding configurations, privacy restrictions, network access and authorities or operates (including but not limited to: VA 6500, TIC, PIA/PTAs, SORN, and application ATOs). Needed access / Approved submitters request access via Service Now with the needed roles.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented? How are the documented, i.e. Policy, SOP, other. And where is this documentation located?

Yes, criteria, procedures, controls, and responsibilities are documented. Standard operating procedure is as follows: when a new user license is added to CRM, the business owner checks with the supervisor to see what PII access is required to perform daily tasks. PII access is limited to only those users who require it.

2.4c Does access require manager approval?

Yes, access requires manager approval.

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

Yes, it is the responsibility of the D365 CSP PCC system managers to ensure compliance with VA regulations and policies regarding configurations, privacy restrictions, network access and authorities to operate, including but not limited to: VA 6500, TIC, PIA/PTAs, SORN, and application ATOs.

2.4e Who is responsible for assuring safeguards for the PII as identified in eMASS?

It is the responsibility of the D365 CSP PCC system managers to ensure compliance with VA regulations and policies regarding configurations, privacy restrictions, network access and authorities to operate, including but not limited to: VA 6500, TIC, PIA/PTAs, SORN, and application ATOs.

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

All information collected will be retained by the system to ensure an accurate accounting of program historical information is maintained.

3.2 How long is information retained?

In some cases, VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. If the system is using cloud technology, will it be following the NARA approved retention length and schedule https://www.archives.gov/records-mgmt/grs? This question is related to privacy control DM-2, Data Retention and Disposal.

https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

Disposition instruction - Temporary. Cutoff at the end of the fiscal year after completion of the research project. Destroy 6 years after cutoff. May retain longer if required by other Federal regulations or the European General Data Protection regulations.

As stated in the SORN: Policies and practices for retention and disposal of records: Records in this system are retained and disposed of in accordance with the schedule approved by the Archivist of the United States, VHA Records Control Schedule 10–1, Item Numbers 1930.2 and 1930.4.

3.3 The retention schedule 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. Please work with the system 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?

Records stored are under the approved disposition authority outlined in Records Control Schedule (RCS) 10-1https://www.va.gov/VHApublications/RCS10/rcs10-1.pdf.

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

Records Control Schedule (RCS) 10-1. https://www.va.gov/VHApublications/RCS10/rcs10-1.pdf.

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.

VA policy states that all Federal records contained on paper, electronic, or other medium be properly managed from their creation through their final disposition, in accordance with Federal laws, the General Records Schedule (GRS) and the VHA Records Control Schedule (RCS) 10-1. The GRS can be found on the National Archives and Record Administration website. The VHA RCS 10-1 is the main authority for the retention and disposition requirements of VHA records. The RCS provides a brief description of the records and states the retention period and disposition requirements. It also provides the NARA disposition authorities or the GRS authorities, whichever is appropriate for the record, in addition to program and service sections. No additional procedures for elimination of SPI have been established at this time.

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.

The PII information collected is not used for research, testing or training.

<u>3.6 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. (Work with your System Privacy Officer (PO) to complete all Privacy Risk questions inside the document in 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: The project retains only the information necessary for its purpose, additionally, the PII is retained only for as long as necessary and relevant to fulfill the specified purposes.

Principle of Data Quality and Integrity: The PIA should describe 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: The risk to maintaining data within the SFGCP is that longer retention times increase the risk that information can be compromised or breached.

Mitigation: To mitigate the risk posed by information retention, Microsoft Azure adheres to the VA RCS schedules for each category or data it maintains. When the retention data is reached for a record, the team will carefully dispose of the data by the determined method as described in question 3.4. All electronic storage media used to store, process, or access VA records will be disposed of in adherence with the latest version of VA Directive 6500.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

PII Mapping of Components

4.1a **D365 CSP PCC** consists of 1 (one) key components (servers/databases/instances/applications/software/application programming interfaces (API)). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by D365 CSP PCC 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 3.9a 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
N/A	N/A	N/A	N/A	N/A	N/A

4.1b List internal organizations information is shared/received/transmitted, the information shared/received/transmitted, and the purpose, and how the information is transmitted.

NOTE: Question 3.9b (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

IT system and/or Program office. Information is shared/received with	*List the purpose of the information being shared /received with the specified program office or IT system*	*List PII/PHI data elements shared/received/transmitted.*	*Describe the method of transmittal*
N/A	N/A	N/A	N/A

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the VA network 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 in this section.).

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

Follow the format below:

Privacy Risk: There is a risk that information may be shared with unauthorized VA personnel.

Mitigation: Safeguards are implemented to ensure data is not sent to unauthorized VA employees, including employee security and privacy training and required reporting of suspicious activity. Use of secure passwords, access for need-to-know basis, Personal Identification Verification (PIV) Cards, Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized for the system.

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 List the external organizations (outside VA) that information shared/received. and information shared/received, and the purpose, and how the information transmitted and what measures are taken to ensure it is secure.

The sharing of information outside the agency must be compatible with the original collection. The sharing must be covered by an appropriate routine use in a SORN. If not covered, 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 IT System or External Program Office	***List the purpose of information***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)***	***List agreements such as:***	***List the method of transmission***

information is shared/received with	***being shared / received / transmitted***		***Contracts, MOU/ISA, BAA, SORN. etc. that permit external sharing (can be more than one)***	***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 external data sharing for this system.

<u>Mitigation:</u> No external data sharing for this system.

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 The notice provided to the individual before collection of the information. Please provide a copy and/or screen shot of a web notice of the notice as an Appendix-A 6.1 on the last page of the document. (A notice may include a posted privacy policy, a Privacy Act notice on forms, notice given to individuals by the sources system, or a system of records notice published in the Federal Register.) If notice was not provided, explain why.

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 Provide the Privacy Notice provided to the public by this system or any source systems. Include a copy of the notice in Appendix A of the PIA, the Federal Register citation, or Privacy Statement from collection of information such as forms or surveys.

NOTICE FM-OCD-010: The information collected on this form, including your contact details, education information, and emergency contacts, is used to update our employee records in compliance with the Privacy Act of 1974. We protect your personal data with appropriate security measures and only share it with authorized personnel or as required by law. Your social security number is masked, and only limited users have viewing privileges. By filling out this form, you acknowledge and consent to the collection, use, and disclosure of your information as described. If you would like a copy of the information we keep on file, please contact Tracey Putnam at tracey.putnam@va.gov.

6.1b If notice was not provided, explain why.

Not applicable. 1a.

6.1c Provide how the notice provided at the time of collection meets the purpose of use for this system.

The notice is located on the internal form used to collect the 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.

Yes, individuals can decline to provide information, and no penalty occurs for declining to provide the information.

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.

Individuals provide their consent to cover all uses (current or potential) of the collected employee data when they read/acknowledge the Privacy Notice provided to them as detailed in Question 6.1a.

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. (Work with your Privacy Officer (PO) 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: This is referring to sufficient notice provided to the individual.

Principle of Use Limitation: The information used only for the purpose for which notice was provided either directly to the individual or through a public notice. The procedures in place must 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: The applicant may not be aware their information is being stored in the D365 CSP PCC system.

Mitigation: All applicants will be notified on Internal form FM-OCD-010 that their information is being collected. They are also notified who to contact if they have questions.

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 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 VA Public Access Link-Home (efoia-host.com) to obtain information about FOIA points of contact and information about agency FOIA processes.***

Access to working areas where information is maintained in VA facilities and VA Central Office is controlled and restricted to VA employees and VA contractors on a need-to-know basis. All users of the system are required to complete annual information system security training activities including basic security awareness training and specific information system security training provided via the Talent Management System (TMS). Members of the public are not allowed access to the system.

Any individual wanting access to their personal data stored in the system may contact Tracey Putnam at tracey.putnam@va.gov to request their personal data.

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)?

The system 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?

The system 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.

Individuals wanting to correct inaccurate or erroneous information in the system should contact Tracey Putnam at tracey.putnam@va.gov.

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 are made aware of the procedures for obtaining a copy of or correcting their information via the Privacy Notice detailed in Question 6.1a.

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.

The employee would contact their manager if the identified person does not respond to the correction request.

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 Privacy Officer (PO) to complete all Privacy Risk questions in this section).*

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: *The individual must be provided with the ability to find out whether a project maintains a record relating to them.*

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

Principle of Individual Participation: *The mechanism by which an individual is able to prevent information about them obtained for one purpose from being used for other purposes without their knowledge.*
This question is related to privacy control IP-3, Redress.

Follow the format below:

Privacy Risk: The risk exists that the individual accidentally provides incorrect information.

Mitigation: Individuals provide information directly to D365 CSP CCP. The individual personally reviews information before providing it, as validation of the information. Individuals may provide updated information for their records by submitting new forms or indicating to the VA that new information supersedes the previous data.

Section 8. Technical Access and Security

The following questions are intended to describe technical safeguards and security measures. (Work with your ISSO to complete this section).

8.1 The procedures in place to determine which users may access the system, must be 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?

Access to D365 CSP CCP is secured, controlled, and limited to select personnel. To gain access the user must have a VA Windows Active Directory account. Secondarily, users must be granted role-based permissions.

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?

No users from other agencies will have access to the system.

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.

Roles have been created for System Customization for administrative personnel, Purchasing for Finance section, and Workforce Support for Individual data collection. The roles have the access to complete the required duties.

8.2. Contractor signed Non-Disclosure Agreement (NDA), Business Associate Agreement (BAA) etc. in place.

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.

8.2a Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

No contractor agreements are required as this system is being developed internally by a VA employee.

8.2a. Will VA contractors have access to the system and the PII?

No contractor will have access to this system as it is being developed internally by a VA employee.

8.2b. What involvement will contractors have with the design and maintenance of the system?

No contractor will have access to this system as it is being developed internally by a VA employee.

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

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

Personnel accessing information systems must read and acknowledge the VA Rules of Behavior (ROB) prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training which all personnel must complete via the VA's Talent Management System (TMS). After the user's initial acceptance of the Rules, the user must reaffirm their acceptance annually as part of the security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system.

8.4 The Authorization and Accreditation (A&A) completed for the system.

8.4a If completed, provide:

1. *The Security Plan Status:*
2. *The System Security Plan Status Date:*
3. *The Authorization Status:*
4. *The Authorization Date:*
5. *The Authorization Termination Date:*
6. *The Risk Review Completion Date:*
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* 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 not completed or In Process, provide your ***Initial Operating Capability (IOC) date.***

IOC date was April 2020.

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. ***(Refer to question 1.8 of the PTA)***

D365 CSP PCC is a Software as a Service (SaaS) Microsoft Azure Government (MAG) Cloud Model.

9.2 Does the contract with the Hosting 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 3.3.1***

of the PTA) *This question is related to privacy control AR-3, Privacy Requirements for Contractors, and Service Providers.*

Yes, D365 CSP PCC has a contract with MAG (Contract number 47QTCA22D003G).

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.

No ancillary data is collected by D365 CSP PCC.

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.

Yes, for all cloud deployments the VA own data and identities.

The responsibilities for data, endpoints, accounts and access management are retained and accountable for security and privacy by the VA organization.

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).

No RPA is used.

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: 2025.06.22 16:27:12 -04'00'

Privacy Officer, Michelle Christiano

ALBERT COMPLE

Digitally signed by ALBERT COMPLE
Date: 2025.06.23 10:34:42 -06'00'

Information System Security Officer, Albert Comple

RUSSELL HOLT

Digitally signed by RUSSELL HOLT
Date: 2025.06.23 12:33:03 -06'00'

Information System Owner, Russell Holt

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).

> NOTCE FM-OCD-010: The information collected on this form, including your contact details, education information, and emergency contacts, is used to update our employee records in compliance with the Privacy Act of 1974. We protect your personal data with appropriate security measures and only share it with authorized personnel or as required by law. Your social security number is masked, and only limited users have view privileges. By filling out this form, you acknowledge and consent to the collection, use, and disclosure of your information as described. If you would like a copy of the information we keep on file, please contact Tracey Putnam at tracey.putnam@va.gov.

HELPFUL LINKS:

Records Control Schedule 10-1 (va.gov)

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 Directive 1605.04
IB 10-163p (va.gov)