Privacy Impact Assessment for the VA IT System called:

# D365 – VA OIG Healthcare Evaluation and Report Transformation System (VA OIG HEARTS)

## Veteran Affairs Corporate Office (VACO)

## Office of Inspector General, Office of Healthcare Inspections

Date PIA submitted for review:

9/11/2023

System Contacts:

*System Contacts*

| | Name | E-mail | Phone Number |
|---|---|---|---|
| Privacy Officer | Roy Fredrikson | Roy.Fredrikson@va.gov | 202-461- 4533 |
| Information System Security Officer (ISSO) | Albert Comple | Albert.Comple@va.gov | 720-856- 2811 |
| Information System Owner | Russell Holt | Russell.Holt2@va.gov | 970-903- 6991 |

## Abstract

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

The D365 – Veterans Affairs Office of Inspector General Healthcare Evaluation and Report Transformation System (D365-VA OIG HEARTS) solution will facilitate the inspection of healthcare facilities and report-writing. VA OIG HEARTS is a new solution that will allow the OIG's Office of Healthcare Inspections directorate (OHI) directorate to manage matrixed inspection teams, create reports on their inspections of VHA healthcare facilities, and analyze and improve the inspection process.

The OIG's Office of Healthcare Inspections directorate (OHI) goals for this solution include: 1. Decreasing the workload of inspectors to collect inspection data, 2. Increasing the quality and reliability of inspection data, 3. Decreasing the workload of inspectors, editors, and reference reviewers to complete reports, 4. Increasing the quality and reliability of report references, 5. Enabling the observation and measurement of program execution, and 6. Strengthening the process of revising and developing inspection topics.

The Microsoft Dynamics365 solution utilizes Azure Active Directory access and authentication.

## Overview

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

*1 General Description*

*A. The IT system name and the name of the program office that owns the IT system.*

D365 – Veterans Affairs Office of Inspector General Healthcare Evaluation and Report Transformation System (VA OIG HEARTS) is owned by the Office of the Inspector General (OIG) Office of Healthcare Inspections (OHI).

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

VA OIG HEARTS is a new solution that will allow the OIG's Office of Healthcare Inspections directorate (OHI) directorate to manage matrixed inspection teams, create reports on their inspections of VHA healthcare facilities, and analyze and improve the inspection process.

*C. Indicate the ownership or control of the IT system or project.*

VA OIG HEARTS is VA controlled by the Office of the Inspector General (OIG) Office of Healthcare Inspections (OHI). The Microsoft Azure platform that VA OIG HEARTS uses, is non-VA owned and operated by Microsoft Corporation.

*2. Information Collection and Sharing*

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

VA OIG HEARTS will store information about approximately 80 inspectors and their inspection details to create reports that analyze inspections of VHA healthcare facilities.

E. *A general description of the information in the IT system and the purpose for collecting this information.*

VA OIG HEARTS will store information about inspectors and their inspection details to create reports that analyze inspections of VH healthcare facilities.

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

No information sharing conducted by this system.

G. *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.*

This system is operated in a single site. The system is cloud-based.

*3. Legal Authority and SORN*

H. *A citation of the legal authority to operate the IT system.*

SORN Inspector General Hotline (Complaint Center) https://www.govinfo.gov/content/pkg/FR-2019-04-17/pdf/2019-07649.pdf. 2019-04-17/pdf/2019-07649.pdf

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

This SORN will add cloud usage and storage when it is amended.

*D. System Changes*

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

The completion of this PIA will not result in changes to business processes.

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

The completion of this PIA will not result in changes to technology.

## Section 1. Characterization of the Information

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

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

*Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy- Protected Information. For additional information on*

*these information types and definitions, please see VA Directives and Handbooks in the 6500 series (https://vaww.va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.*

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

*The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1.*

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

- ☒ Name
- ☒ Social Security Number
- ☐ Date of Birth
- ☐ Mother's Maiden Name
- ☐ Personal Mailing Address
- ☒ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☒ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☐ Financial Information
- ☐ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers*
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☐ Medications
- ☒ Medical Records
- ☒ Race/Ethnicity
- ☐ Tax Identification Number
- ☐ Medical Record Number
- ☐ Gender
- ☐ Integrated Control Number (ICN)
- ☐ Military History/Service Connection
- ☐ Next of Kin
- ☒ Other Data Elements (list below)

<<Add Additional Information Collected But Not Listed Above Here (For Example, A Personal Phone Number That Is Used As A Business Number)>>
*Specify type of Certificate or License Number (e.g. Occupational, Education, Medical)

- Title
- Work Phone
- Work Email

**PII Mapping of Components (Servers/Database)**

**VA OIG HEARTS** consists of **ZERO** key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **VA OIG HEARTS** 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 the server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

*Internal Database Connections*

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

**1.2 What are the sources of the information in the system?**
*These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.*

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

The data for the VA OIG HEARTS system is being provided by the individuals performing the inspections. The VA OIG HEARTS system creates reports using the data inputted by inspectors.

*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 from other sources is not required for this system.

*1.2c If the system creates information (for example, a score, analysis, or report), list the system as a source of information.*

VA OIG HEARTS creates reports and is, therefore, a source of information.

**1.3 How is the information collected?**
*These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.*

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

Information is collected and entered into the system by inspectors and is used to create reports. No information is received via transmission from another system.

*1.3b 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.*

The information collected is not subject to the Paperwork Reduction Act.

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

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

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

The information in the VA OIG HEARTS system will not be checked against any other source of information. The system will not store information impacting the cited privacy controls.

*1.4b 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 system does not check for accuracy by assessing a commercial aggregator of information.

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

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

The Privacy Act of 1974, as amended, 5 U.S.C. § 552a, establishes a code of fair information practices that govern the collection, maintenance, use, and dissemination of information about individuals that are maintained in systems of records by federal agencies.

The SORN for the system states the authority of maintenance of the system falls under the following:
(https://www.oprm.va.gov/privacy/systems_of_records.aspx).
Inspector General Hotline (Complaint Center) 66VA53 2019-07649.pdf (govinfo.gov)

**1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information**

*Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks.* (*Work with your System ISSO to complete this section)*

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

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

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

*Principle of Individual Participation: Does the program, to the extent possible and practical, collectinformation 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:** More privacy data means more opportunities for unauthorized access, lack of appropriate controls to securing case and legal issue data may result in financial penalties, lawsuits, identity theft and distrust.

**Mitigation:** Data security rules are assigned to determine which data users can access and how this data can be accessed (view, add/edit, delete). Sharing models define company-wide defaults and data access based on a role hierarchy. Security can be applied at the:
• Record level – which matters, documents and other records a user can access and how these can be accessed.
• Screen level – which screens or data on a record can be accessed and how these can be accessed.
• Field level – which fields on a matter or other type of record a user can access and how these can be accessed.

## 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 – used to identify individuals.
- Title – used for communication.
- Work Email – used for communication.
- Work Phone – used for communication.
- Veterans Social Security Number – might be seen during an investigation.
- Veterans Personal Phone Number – might be seen during an investigation.
- Veterans Personal Email Address – might be seen during an investigation.
- Veterans Race/Ethnicity – might be seen during an investigation.
- Veterans Medical Records – might be seen during an investigation.

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

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

The D365 VA OIG HEARTS system will utilize Microsoft Dynamics 365 analysis and reporting capabilities to review and report on the healthcare facilities inspections data inputted into the system by the inspectors.

*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.*

The D365 VA OIG HEARTS system is intended to improve the process of healthcare facilities inspections. The only information about individuals will be to identify inspectors and associate them with the inspections they performed. This information will only be accessed by VA OIG office personnel and will not be used to make determinations about the inspectors.

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

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

Data in transit are protected by HTTPS site-to-site encryption. PII data are encrypted at rest with Microsoft Defender.

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

SSNs will only be in partial form (last 4) in this system. MS DEFENDER is used to protect data at rest.

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

D365 VA OIG HEARTS is an encrypted secure system. User roles determine who has visibility into PII/PHI.

## 2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

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

*2.4a How is access to the PII determined?*

Strict control measures are enforced to ensure that access to and disclosure are limited to a need-to-know based on the official duties, including personnel in the VA OIG Office of Investigations. Access to the computerized information is limited to VA OIG employees by means of passwords and authorized user identification codes.

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

Yes, controls are in place to ensure data is used and protected in accordance with legal requirements, VA policies, and VA's stated purpose for using the data. Controls include mandatory training completion for all employees, volunteers, and contractors. Additionally, audits are performed to ensure information is accessed and retrieved appropriately. VA and Microsoft D365 have implemented required security and privacy controls for Federal information systems and organizations according to NIST SP 800-53 and VA Handbook 6500, Risk Management Framework for VA Information Systems. Per the approval of the

Acting Assistant Secretary for Information Technology [the VA Authorizing Official (AO)]. VA Records Management Policy and the VA Rules of Behavior in Talent Management System (TMS) govern how Veterans' information is used, stored, and protected.

*2.4c Does access require manager approval?*

Yes, managers must approve any new users accessing the application.

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

Yes, Identity Access Management (IAM) systems verify credentials and collect audit logs based on access requested and may contain PII that might have been captured into order to authenticate to the resource.

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

Accessibility to data is granted based on the permission sets and role-based hierarchy applied based on FedRAMP Microsoft Azure platform. Account creation is managed and offered through VA via two factor authentication (2FA) Personal Identity Verification (PIV) card and/or Access VA.

Single Sign On external (SSOe) is used to provide credential access to VA modules/communities residing in the application, the determinant of access is organizational affiliation rather than personal identity.

The managers will reject any applications from individuals who do not work with them, do not require access, or are not using the correct e-mail address. IAM systems verify credentials and collect audit logs based on access requested and may contain PII that might have been captured into order to authenticate to the resource.

## 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
Personal Phone Number
Personal Email Address
Race
Medical Records/Treatment History

Title
Work Email
Work Phone

### 3.2 How long is information retained?

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

The information is retained following the policies and schedules of VA's Records Management Service, General Control Schedule 10-1 can be found at the following link: https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf.

Records Schedules for VA Inspector General records can be found at the following link: https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-veterans-affairs/rg-0015/daa-0015-2013-0004_sf115.pdf. Working Papers (Disposition Authority # DAA-0015-2013-0004-0007).

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

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

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

The information is retained following the policies and schedules of VA's Records Management Service, General Control Schedule 10-1 can be found at the following link: https://www.va.gov/vhapublications/RCS10/rcs10-1.pdf.

The information is retained following the policies and schedules of VA's Records Management Service. Records Schedules for VA Inspector General records can be found at the following link:https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-veterans-affairs/rg-0015/daa-0015-2013-0004_sf115.pdf. Working Papers (Disposition Authority # DAA-0015-2013-0004-0007). Records for this system are collected from existing systems of record for legal analysis and action, including disciplinary action and defense of the OIG in administrative and civil

litigation. Disposition instructions: Temporary, destroy 3 years after submission of report, but longer retention is authorized if required for business use.

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

Microsoft D365 complies with all VA retention and disposal procedures specified in VA Handbook 6300 and VA Directive 6500. Records contained in the Microsoft Azure FedRAMP cloud will be retained as long as the information is needed in accordance with a NARA-approved retention period. VA manages Federal records in accordance with NARA statues including the Federal Records Act (44 U.S.C. Chapters 21, 29, 31, 33) and NARA regulations (36 CFR Chapter XII Subchapter B). SFGCP records are retained according to the Record Control Schedule 10-1 Section 4 (Disposition of Records).

Request for Records Disposition Authority. Disposition Authority: DAA-0015-2013-0004. https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-veterans-affairs/rg-0015/daa-0015-2013-0004_sf115.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.*

All electronic storage media used to store, process, or access records will be disposed of in adherence with the VA Directive 6500. (https://www.va.gov/vapubs/search_action.cfm?dType=1)

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

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

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

D365 VA OIG HEARTS does not use PII information of the users stored in this application for research, testing or training. Users accessing the tool would have to undergo basic Privacy training such as, Privacy and Information Security Awareness and Rules of Behavior and information security training annually.

**3.6 PRIVACY IMPACT ASSESSMENT: Retention of information**

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

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

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

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

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

Follow the format below:

**Privacy Risk:** There is risk associated with longer retention time. The system could exceed the retention times to fulfill the VA mission. With longer retention times, the system is at a greater risk of data breach.

**Mitigation:** By adhering to the data retentions times, D365 VA OIG HEARTS mitigates the risk posed for information maintained in the system. VA Directive 6500 Cybersecurity Program serves as the authoritative source for addressing and managing a cybersecurity breach or attack (also known as a cyber incident) to contain and limit the damage.

## Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

*Data Shared with Internal Organizations*

| ***List the Program Office or IT System information is shared/received with*** | ***List the purpose of the information being shared /received with the specified program office or IT system*** | ***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*** | ***Describe the method of transmittal*** |
|---|---|---|---|
| *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 Department and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).*

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

Follow the format below:

**Privacy Risk:** No known privacy risk.

**Mitigation**: Not applicable.

## Section 5. External Sharing/Receiving and Disclosure

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

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

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

**NOTE: Question 3.10 on Privacy Threshold Analysis should be used to answer this question.**

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

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

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

*Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.*
*This question is related to privacy control UL-2, Information Sharing wgith Third Parties*

*Data Shared with External Organizations*

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

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

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

*Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum Of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.*

*Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.*
*This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing*

Follow the format below:

**Privacy Risk:** Not applicable for this system.

**Mitigation:** Not applicable 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 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an Appendix-A 6.1 on the last page of the document. Also provide notice given to individuals by the source system (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register.) If notice was not provided, why not?**

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

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

The Department of Veterans Affairs does provide public notice that the system does exist. This notice is provided in 2 ways:

1. The SORN defines the information collected from Veterans, use of the information, and how the information is accessed and stored. Inspector General Hotline (Complaint Center) 66VA53 2019-07649.pdf (govinfo.gov)
2. This Privacy Impact Assessment (PIA) also serves as a notice of the VA OIG HEARTS system.

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

Notice provided via VA Privacy Policy

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

This system is an internally used VA system utilized by and for VA employees, so the notice is not applicable for this system.

**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.*

The information collected in this system involves VA OIG employees gathering healthcare inspection data. When agreeing to work for the VA, employees have consented to the collection of information about their performance.

**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/employees do not have a right to consent to uses of the information or to review or to contest the information in this system because the system is a platform for legal staff to collect, review, and analyze healthcare performance information. The work product from the analyses in this system is finalized into agency decisions. Agency decisions and relevant records are disclosed to individuals pursuant to the publicly available due process and discovery rules of each legal venue involved. The accuracy and completeness of any relevant decisions and records are subject to grievance and appeal procedures in these legal venues, which are publicly available.

**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 System ISSO to complete all Privacy Risk questions inside the document this section).*

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

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

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

**Privacy Risk:** Risk is associated with individuals being unaware of the system.

**Mitigation:** The VA mitigates this risk by providing the public with notice that the system exists, as discussed in detail in question 6.1.

## Section 7. Access, Redress, and Correction

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

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

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

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

An individual who seeks access to or wishes to contest records maintained under his or her name in this system must submit a written request to the Chief, Information Release Office (50CI). However, a majority of records in this system are exempt from the records access and contesting requirements under 5 U.S.C. 552a (j) and (k). To the extent that records in this system of records are not subject to exemption, they are subject to access and contest. A determination as to whether an exemption applies shall be made at the time a request for access or contest is received.

*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 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.*

This system is not 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.*

Inaccurate or erroneous information is corrected by a combination of manual input by VA employees and by system automated rules incorporated in VA OIG HEARTS.

### 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 do not have a right to consent to particular uses of the information or to review or to contest the information in this system because the system is a platform for legal staff to collect, review, and analyze information from existing systems; the records and the analyses remain subject to privileges recognized by the relevant courts and administrative venues. The work product from the analyses in this system is finalized into agency decisions. Agency decisions and relevant records are disclosed to individuals pursuant to the publicly available due process and discovery rules of each legal venue involved. The accuracy and completeness of any relevant decisions and records are subject to grievance and appeal procedures in these legal venues, which are publicly available.

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

*Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems.* ***Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.***
*This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.*

Individuals do not have a right to consent to particular uses of the information or to review or to contest the information in this system because the system is a platform for legal staff to collect, review, and analyze information from existing systems; the records and the analyses remain subject to privileges recognized by the relevant courts and administrative venues. The work product from the analyses in this system is finalized into agency decisions. Agency decisions and relevant records are disclosed to individuals pursuant to the publicly available due process and discovery rules of each legal venue involved. The accuracy and completeness of any relevant decisions and records are subject to grievance

and appeal procedures in these legal venues, which are publicly available.

### 7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

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

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

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

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

Follow the format below:

**Privacy Risk:** Risk is associated with individuals having no proper guidance regarding access, redress and correction of their information being captured by VA OIG HEARTS.

**Mitigation:** By publishing this PIA, and the applicable SORN, the VA makes the public aware of the information being captured by VA OIG HEARTS.

## 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?

*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.*

Managers must approve the VA employees accessing/ requiring to access the VA OIG HEARTS application. The access to the application the manager/ sponsor should provide a description of the user needs, user's role, and security caveats that apply to the user. The roles will be governed by the permission sets that allow field level control of the information and data. Per VA Directive 6500, the

Office of Information Technology (OIT) develops, disseminates, and reviews/updates a formal, documented policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; along with formal, documented procedures to facilitate the implementation of the control policy and associated controls.

*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?*

Users from other agencies will not 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.*

Role-based hierarchy of profiles and permission sets are applied for users accessing the platform. Only authorized VA users can access this tool. Users access the application using Single Sign On (SSO) and two factor authentication to log into the VA OIG HEARTS application.

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

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

The Digital Transformation Center (DTC) contractor team supports the VA Dynamics 365 (D365) production environment and as such has access to the system and data contained therein. This includes PII and VA Sensitive Information. The user roles will be governed by permission sets that allow field level control of the information and data. This information is documented in the user provisioning process with the Digital Transformation Center. The VA DTC members are not primary users of VA Dynamics 365. The ISO will monitor and review VA-related support contracts on a regular basis to ensure no gaps in support for the users. The VA DTC team will maintain users, update applications and components, introduce new functionality, govern deployment activities, and ensure user operability. The VA DTC 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 Talent Management System (TMS).

The contracted Microsoft D365 system integrators/developers working on the system utilize dummy/test data while configuring and testing the system and do not have access to production PHI and PII. No confidentiality agreement has been developed for contractors for this system.

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

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

General Training includes VA Privacy and Information Security Awareness and Rules of Behavior, TMS 10203 - Privacy and Health Insurance Portability and Accountability Act (HIPPA), VA On-Boarding enterprise-wide training, and annual information security training. After the user's initial acceptance of the Rules, the user must reaffirm their acceptance annually as part of the privacy and security awareness training. Acceptance is obtained via electronic acknowledgment and is tracked through the TMS system.

**8.4 Has Authorization and Accreditation (A&A) been completed for the system?** No

*8.4a If Yes, provide:*

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

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

*8.4b If No or In Process, provide your* ***Initial Operating Capability (IOC) date.***

The Designated Security Classification for the system is a MODERATE. The eMASS ATO approval is in process, and the initial operating capability date is projected as 12/7/2023.

## Section 9 – Technology Usage

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

**9.1 Does the system use cloud technology? If so, what cloud model is being utilized?**

*If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). This question is related to privacy control UL-1, Information Sharing with Third Parties.*

***Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1**. (Refer to question 3.3.1 of the PTA)*

All Dynamics 365 CRM applications are hosted in Microsoft Azure Government (MAG).

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

*Yes, VA has full ownership of the PII/PHI that will be shared through the D365- VA OIG HEARTS system. Contract Agreement with Service Provider Microsoft Azure, Contract No. 47QTCA22C003G*

**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.*

Ancillary data is not collected by the system. VA has full ownership over the data stored in the system.

**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.*

The Office of Inspector General has full authority over the data stored in D365-VA OIG HEARTS.

**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).*

The system does not use RPA.

## Section 10. References

### Summary of Privacy Controls by Family

*Summary of Privacy Controls by Family*

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

Fredrikson, Roy (OIG)

Digitally signed by Fredrikson, Roy (OIG)
Date: 2023.09.22 12:39:46 -04'00'

**Privacy Officer, Roy Fredrikson**

ALBERT COMPLE

Digitally signed by ALBERT COMPLE
Date: 2023.09.22 10:47:04 -06'00'

**Information Systems Security Officer, Albert Comple**

RUSSELL HOLT

Digitally signed by RUSSELL HOLT
Date: 2023.09.27 12:05:33 -06'00'

**Information Systems 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).

Inspector General Hotline (Complaint Center) 66VA53 2019-07649.pdf (govinfo.gov)

Notice provided via VA Privacy Policy

## HELPFUL LINKS:

**Record Control Schedules:**

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

**General Records Schedule 1.1: Financial Management and Reporting Records (FSC):**

https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

**National Archives (Federal Records Management):**

https://www.archives.gov/records-mgmt/grs

**VHA Publications:**

https://www.va.gov/vhapublications/publications.cfm?Pub=2

**VA Privacy Service Privacy Hub:**

https://dvagov.sharepoint.com/sites/OITPrivacyHub

**Notice of Privacy Practice (NOPP):**

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices