Privacy Impact Assessment for the VA IT System called:

Order Tracking Manager Dermatology (OTM DERM)

Veterans' Health Administration

Infrastructure Operations

eMASS ID 2581

Date PIA submitted for review:

January 24, 2025

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Nancy katz-johnson	Nancy.katz-johnson@va.gov	203-535-7280
Information System Security Officer (ISSO)	Roland Parten	*Roland.Parten@va.gov*	*(205) 534-6179*
Information System Owner	Keith Ruiz	*Keith.Ruiz@va.gov*	*(412) 523-8453*

Abstract

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

Order Tracking Manager Dermatology is used by VA to assist healthcare staff who have a role in caring for patients in the dermatological clinic. OTM contains various dashboards that allow an authorized user to create an organize custom views for diagnostic, appointments, alerts, and orders.

Order Tracking Manager Dermatology is a web-based system. It provides support Clinical Care Dermatology Department and administrative staff and supports approximately 50+ users. These users are primarily located in Philadelphia VA Medical Center.

The Order Tracking Manager Dermatology operating environment includes the identified authorization boundaries which are Windows Server 2022 servers, VSOA_PFS Service, IIS Service, Document Storage System (DSS) Patient Flow Suite (PFS) and corresponding application module, SSOi (via IAM) – 2 Factor Authentication with PIV and/or eToken. *and* Veterans Health Information Systems and Technology Architecture (VistA).

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?

Order Tracking Manager-DERM (OTM-Derm) application provide a customized user-friendly Windows Graphical User Interface (GUI) for entering clinical and administrative information that assist with the assessment of ongoing care using current patient data for completed procedures. Order Tracking Manager-DERM (OTM-DERM) application record diagnostic findings, including clinical data, charting, and sequenced treatment planning. Order Tracking Manager-DERM (OTM-Derm) applications interface with the Veterans Health Information Systems and Technology Architecture (VistA) System using the RPC Broker, VistA Service Oriented Architecture (VSOA) or VistA KIDS (Kernel Installation & Distribution System) technologies.

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.

VA Owned and Operated

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?

Order Tracking Manager-Dermatology (OTM-Derm) applications are used at all VHA licensed medical centers clinical and administrative personnel (10,000+) which includes healthcare providers and veterans or dependents.

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?

Order Tracking Manager Dermatology (OTM-Derm) is a web-based application pulling real-time information from VistA for the purpose to assist healthcare staff who have a role in caring for patients in the dermatological clinic. OTM contains various dashboards that allow an authorized user to create an organize custom views for diagnostic, appointments, alerts, and orders.

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

Order Tracking Manager-Dermatology (OTM-Derm) application uses information from the Veterans Health Information Systems and Technology Architecture (VistA) System. The patient information is shared from VistA and housed only in VistA but is viewable/accessible from OTM. Example of information shared" Name (Last name, First Name, Middle Initial), SSN, DOB,

Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health Insurance Beneficiary Numbers; Account Numbers, Current Medications, Previous Medical Records, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), Date of activity, current and previous medical records information such as clinic name/location, health summaries, lab, consult, imaging, progress notes surgeries, discharge summaries, medications, allergies, date of activity.

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

There are no modules or subsystems. OTM is a module of the DSS Enterprise ATO.

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?

Currently the system is only available/operating at the Philadelphia VA Medical Center

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

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

<< Order Tracking Manager-Dermatology (OTM-Derm)'s legal authorities for operating the system are found in the SORNS that apply to the particular component or minor system:

Veterans Health Information Systems and Technology Architecture (VistA) Records – VA, SORN 79VA10 https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf. Authority for maintenance of the system: Title 38, United States Code, section 7301(a).

Patient Medical Record – VA, SORN 24VA10A7 https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf. Authority for maintenance of the system: Title 38, United States Code, Sections 501(b) and 304.

I. What is the SORN?

Veterans Health Information Systems and Technology Architecture (VistA) Records – VA, SORN 79VA10 https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf. Authority for maintenance of the system: Title 38, United States Code, section 7301(a).

Patient Medical Record – VA, SORN 24VA10A7 https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf. Authority for maintenance of the system: Title 38, United States Code, Sections 501(b) and 304.

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

These systems are not in the process of being modified nor is it using cloud technology.

4. System Changes

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

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

b. 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:
- Service-Connected Disabilities and Percentage
- Primary Eligibility Code and Means Test Status
-Network Account Information

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?

Order Tracking Manager-Derm (OTM-Derm) information is collected from the VistA system that assist with the assessment of ongoing care using current patient data for completed procedures.

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.

Order Tracking Manger-Derm (OTM-Derm) application does not use data from a commercial aggregator of information or is data taken from the public website(s).

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

Order Tracking Manager-Dermatology (OTM-Derm) application use RPC Broker, VistA Service Oriented Architecture (VSOA) or VistA KIDS (Kernel Installation & Distribution System) technologies which permit the application end users to retrieve and store clinical and administrative data within the Veterans Health Information Systems and Technology Architecture (VistA) System. The Order Tracking

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

Manager-Dermatology (OTM-Derm) diagnostic information, coding and crediting, progress notes (TIU (Text Integration Utilities)) are saved in VistA.

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?

Received via electronic transmission from VistA.

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?

Order Tracking Manager-Dermatology (OTM-Derm) information is not collected on a form and is not subject to the Paperwork Reduction Act.

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 Order Tracking Manager-Dermatology (OTM-Derm) application are Graphical User Interface (GUI) front-end for data input into the Veterans Health Information Systems and Technology Architecture (VistA), patient files as well as the Patient Care Encounter (PCE), Text Integration Utility (TIU), Computerized Patient Record Search (CPRS) Problem List, and Vitals packages. This technology allows doctors and staff to access a patient`s entire medical record and enables them to enter diagnostic findings, treatment plan procedures and patient-specific notes into the patient`s Electronic Health Record. Application users require a VistA account with CPRS VistA secondary menu option/security key/VistA Person Class Code, etc. to retrieve and store new data.

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?

Order Tracking Manager-Dermatology (OTM-Derm does not check for accuracy by accessing a commercial aggregator of information.

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

Title 38 United States Code (U.S.C.) §§1701, 1703, 1710(c), 1712, 3104 and Title 38 Code of Federal Regulation (CFR) Chapter 17 authorizes the provision of Veterans medical, nursing home, and domiciliary care and associated record-keeping.

SORN 79VA10 "Veterans Health Information Systems and Technology Architecture (VistA) Records-VA", https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf. Authority for maintenance of the system: Title 38, United States Code, section 7301(a).

SORN 24VA10A7 "Patient Medical Record-VA", https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf. Authority for maintenance of the system: Title 38, United States Code, Sections 501(b) and 304.

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: 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: The Order Tracking Manager-Dermatology (OTM-Derm) application retrieve Personally Identifiable Information (PII), Protected Health Information (PHI), and other highly delicate Sensitive Personal Information (SPI). If this information were to be breached or accidentally released to inappropriate parties or the public, it could result in financial, personal, and/or emotional harm to the individuals whose information is contained in the system.

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

Section 2. Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

2.1 Describe how the information in the system 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 (Last name, First Name, Middle Initial)	Used as a person's identifier	Not used
SSN	Assists in uniquely identifying the person's medical record.	Not used
Date Of Birth	Assists to identify patient age and confirm patient identity	Not used
Personal Mailing Address	Used to contact the individual	Not used
Personal Phone Number(s)	Used to contact the individual	Not used
Personal e-mail Address	Used to contact the individual	Not used
Health Insurance Beneficiary Numbers Account Numbers	Used to file claims	Not used
Current Medications	Assists to determine medical history and healthcare outcome and used to administer medication	Not used
Previous Medical Records	Assists to determine medical history and healthcare outcome	Not used
Race/Ethnicity	Assists to determine Race/Ethnicity.	Not used

Medical Record Number	Assists in uniquely identifying the person's medical record	Not used
Other Unique Identifying Number (ICN Internal Control Number)	Assists in uniquely identifying the person's medical record	Not used
Service-Connected Disabilities & Percentages	Assists to determine medical history and healthcare outcome	Not used
Primary Eligibility Code & Means Test Status	Assists to determine medical history and healthcare outcome	Not used
Network Accounts Information	Used to identify specific employee(s)	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?

Order Tracking Manager-Dermatology (OTM-Derm) application does not contain a database and no data is saved within the application. Therefore, there is no data to analyze.

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.

Order Tracking Manager-Dermatology (OTM-Derm) application does not contain a database and no data is saved within the application. Therefore, there is no data to analyze.

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?

Data at rest is encrypted when it resides within VistA. Data in transit is protected by HTTPS, FIPS 140-2 AES-256 TLS. RPC Broker traffic is limited to the VA LAN/WAN which is encrypted.

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).

Application protection: Only available to approved users, some applications use Patient Identifiers (PID) randomly generated within the application, some applications view SSNs in partial form, and/or application databases are encrypted.

VistA protection: Sensitive patient record tracking, only available to approved users via menus and keys, VistA Database, IRIS, is encrypted. SSN is viewable in partial form.

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

Application protection: Only available to approved users, some applications use Patient Identifiers (PID) randomly generated within the application, some applications view SSNs in partial form, and/or application databases are encrypted.

VistA protection: Sensitive patient record tracking, only available to approved users via menus and keys, VistA Database, IRIS, is encrypted. SSN is viewable in partial form.

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?

Order Tracking Manager-Dermatology (OTM-Derm) application end users require a Veterans Health Information Systems and Technology Architecture (VistA) account and Active Directory

network account; and VistA application-specific VistA menus and/or VistA security keys and may require role-based Active Directory security groups.

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?

Order Tracking Manager – Dermatology (OTM-Derm) application access is the responsibilities of the applications end users' local site OI&T personnel. Local site OI&T personnel follows their local policies, SOP and procedures and coordinate access with the applications end users' supervisor.

2.4c Does access require manager approval?

Yes, - Order Tracking Manager – Dermatology (OTM-Derm) application access requires manager/supervisor approval.

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

Order Tracking Manager-Dermatology (OTM-Derm) application interface with the Veterans Health Information Systems and Technology Architecture (VistA) System using the RPC Broker, and/or VistA Service Oriented Architecture (VSOA) technologies. Order Tracking Manager-Dermatology (OTM-Derm) application provides data input into the Veterans Health Information Systems and Technology Architecture (VistA) System files, as well as the Patient Care Encounter (PCE), Text Integration Utility (TIU) and Clinical Patient Record System (CPRS) Problem List packages.

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

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

All VHA staff are responsible for assuring safeguards for the PII. Organizational and non-organizational users are required to take the Talent Management System (TMS) VA Privacy and Information Security Awareness and Rules of Behavior Training yearly. VHA facilities ISSO is responsibility to monitor VistA access and verify the TMS training has been completed and current.

The system owner and managers are responsible for safeguarding PII/PHI.

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 (Last name, First Name, Middle Initial)
Social Security Number
Date of Birth
Personal Mailing Address
Personal Phone Number(s)
Personal e-mail Address
Health Insurance Beneficiary Numbers Account Numbers
Current Medications
Previous Medical Records
Race/Ethnicity
Medical Record Number
Other Unique Identifying Number (ICN Internal Control Number)
Service-Connected Disabilities and Percentage
Primary Eligibility Codes and Means Test Status

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 https://www.archives.gov/records-mgmt/grs? This question is related to privacy control DM-2, Data Retention and Disposal.*

Order Tracking Manager-Dermatology (OTM-Derm) does not retain date within itself, but information is retained within Vista. The data is retained in accordance with the records disposition authority approved by the Archivist of the Unites States. The retention period for specific data will depend on which SORN that applies to that data. Here are the details for the SORNs this system uses:

SORN 79VA10, ‘‘Veterans Health Information Systems and Technology Architecture (VistA) Records-VA’’ https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28340.pdf states: Record Control Schedule (RCS) 10–1, Item 2000.2 Information Technology Operations and Maintenance Records destroy 3 years after agreement, control measures, procedures, project,

activity, or when transaction is obsolete, completed, terminated or superseded, but longer retention is authorized if required for business use (DAA–GRS–2013–0005– 0004, item 020). RCS 10–1, Item 2100.3 2100.3, System Access Records destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use (DAA–GRS–2013–0006–0004, item 31).

SORN 24VA10A7, "Patient Medical Record-VA" https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf states: "paper records and information stored on electronic storage media are maintained for seventy-five (75) years after the last episode of patient care and then destroyed/or deleted. VHA Records Control Schedule (RCS 10-1, Chapter 6, 6000.1d (N1–15–91–6, Item 1d) and 6000.2b (N1–15–02–3, Item 3)."

RCS 10-1: https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf.

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?

All records are within the system of records indicated with disposition authority approved by the Archivist of the Unites States.

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

As outlined in question 3.2 above record retention as it applies to data by SORN is as follows:

SORN 79VA10:
RCS 10–1, Item 2000.2, disposition authority DAA–GRS–2013–0005– 0004, item 020.
RCS 10–1, Item 2100.3, disposition authority DAA–GRS–2013–0006– 0004, item 31.
SORN 24VA10A7
RCS 10-1, Chapter 6, 6000.1d, disposition authority (N1–15–91–6, Item 1d) and 6000.2b (N1–15–02–3, Item 3).
SORN 121VA10,
GRS 5.2, Item 020, disposition authority DAA-GRS2022-0009-0001. (https://www.archives.gov/files/records-mgmt/grs/grs05-2.pdf).
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.

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.

Order Tracking Manager-Dermatology (OTM-Derm) patches (VistA KIDS build and GUI executable) are not released for National installation prior to testing. With an approved MOU (Memorandum of Understanding) from the IOC site(s), the vendor, Document Storage System (DSS), Test Patches are installed and tested in the VistA Pre-Production Test System. IOC site(s) tester(s) complete the Test Site(s) User's Acceptance VistA Pre-Production System document prior to VistA Production System installation. Test patients are created in the VistA Pre-Production Systems to be used when testing new Order Tracking Manager-Dermatology (OTM-Derm) Patches. VistA Pre-Production Systems test patients' data are scrambled. Test shortcuts located on the Test application server.

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 Privacy Officer (PO) 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: 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: PII or PHI may be held for longer than it is required to be maintained. This extension of retention periods increases the risk that information may be breached or otherwise put at risk of access by unauthorized persons.

Mitigation: Of those applications that data is stored, the databases are encrypted, or the drive is encrypted. Access to these databases is restricted to only authorized users, administrative accounts. The standard user does not have access directly to the stored data.

To mitigate the risk posed by information retention, DSI adheres to the disposition authority approved by the Archivist of the United States. When the retention date is reached for a record, the individual's information is carefully disposed of. The individual's information is carefully disposed of following the procedures listed in 3.4.

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 **Order Tracking Manger-Dermatology** consists of **1** 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 **Order Tracking Manger-Dermatology** 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
Veterans Health Information Systems and Technology Architecture (VistA)	Yes	No	Name (Last name, First Name, Middle Initial), SSN, DOB, Personal Mailing Address; Personal Phone Number(s); Personal e-mail Address; Health, Race/Ethnicity; Medical Record Number, Other Unique Identifying Number (ICN Internal Control Number), Service-Connected Disabilities and Percentages, Primary Eligibility Code and Means Test Status	Ensure correct record is retrieve from VistA	VistA Database is encrypted Behind an MDIA, Uses access and verify code for authentication, and retention history

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***
Veterans Health Administration Veterans Health Information Systems and Technology (Vis	Assists to determine medical history and healthcare outcome	Name Social Security Number Date of Birth Personal Mailing Address Personal Phone Number(s) Personal Email Address Health Insurance Beneficiary Numbers Account Number Medications Records Race/Ethnicity Medical Record Number Internal Control Number (ICN) Service-Connected Disabilities and Percentages Primary Eligibility Code and Means Test Status	RPC (Remote Procedure Call) Broker Technology/standard is consistent with VA policies and standards, including, but not limited to, VA Handbooks 6102 and 6500; VA Directives 6004, 6513, and 6517; and National Institute of Standards and Technology (NIST) standards, including Federal Information Processing Standards (FIP

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

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

Section 5. External Sharing/Receiving and Disclosure

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

5.1 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 information is shared/received with	***List the purpose of information being shared / received / transmitted***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)***	***List agreements such as: Contracts, MOU/ISA, BAA, SORN. 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				

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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:

Privacy Risk: There is no external sharing.

Mitigation: There is no external sharing.

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.

The VHA Notice of Privacy Practice (NOPP)
https://www.va.gov/vhapublications/ViewPublication.asp?pub_ID=9946
explains the collection and use of protected health information to individuals receiving health care from VA. The NOPP is mailed every three years or when there is a major change to all enrolled Veterans. Non Veterans receiving care are provided the notice at the time of their encounter.

This Privacy Impact Assessment (PIA) also serves as notice As required by the eGovernment Act of 2002, Pub.L. 107–347 §208(b)(1)(B)(iii), the Department of Veterans Affairs "after completion of the [PIA] under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means."

A Privacy Act Statement is provided on all forms that collect information that will be maintained in a privacy act system of records. The statement provides the purpose, authority and the conditions under which the information can be disclosed.

SORN 79VA10 "Veterans Health Information Systems and Technology Architecture (VistA) Records–VA" https://dvagov.sharepoint.com/sites/vacovetsprivacy/vhapo/Documents/SORNs/79VA10P2_VISTA_012521.pdf

SORN 24VA10A7 "Patient Medical Record-VA" https://www.govinfo.gov/content/pkg/FR-2020-10-02/pdf/2020-21426.pdf.

6.1b If notice was not provided, explain why.

Notice was provided as indicated in question 6.1a above.

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

Notice was provided as indicated in question 6.1a above.

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.

Order Tracking Manager-Dermatology (OTM-Derm) extracts data that exists and was generated in the course of routine medical care. Information is requested when it is necessary to administer benefits to veterans and other potential beneficiaries. While an individual may choose not to provide information, this may prevent them from obtaining the benefits necessary to them.

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.

Information is requested when it is necessary to administer benefits to veterans and other potential beneficiaries. While an individual may choose not to provide information, this may prevent them from obtaining the benefits necessary to them.

Employees and VA contractors are also required to provide the requested information to maintain employment or their contract with *VHA*

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:

<u>Principle of Transparency:</u> This is referring to sufficient notice provided to the individual.

<u>Principle of Use Limitation:</u> 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:** There is a risk that an individual may not receive notice that their information is being collected, maintained, processed, or disseminated by the Veterans' Health Administration and the local facilities prior to providing the information to the VHA.

Mitigation: This risk is mitigated by the common practice of providing the NoPP when Veterans apply for benefits. Additionally, new NoPPs are mailed to beneficiaries at least every 3 years and periodic monitoring is performed to check that all employees are aware of the requirement to provide guidance to Veterans and that the signed acknowledgment form, when applicable, is scanned into electronic records, The NoPP is also available at all VHA medical centers from the facility Privacy Officer.

The System of Record Notices (SORNs) and Privacy Impact Assessment (PIA) are also available for review online, as discussed 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 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.***

There are several ways a veteran or other beneficiary may access information about them. The Department of Veterans' Affairs has created the My HealtheVet program to allow online access to their medical records. More information on this program and how to sign up to participate can be found online at http://www.myhealth.va.gov/index.html. Veterans and other individuals may also request copies of their medical records and other records containing personal data from the medical facility's Release of Information (ROI) office.

VHA Directive 1605.01, Privacy and Release of Information, Paragraph 7 outlines policy and procedures for VHA and its staff to provide individuals with access to and copies of their PII in compliance with the Privacy Act and HIPAA Privacy Rule requirements. VHA also created VA form 10-5345a for use by individuals in requesting copies of their health information under

right of access.VA Form 10-5345a is voluntary but does provide an easy way for individual to request their records.

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 Privacy Act provisions.

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 information in the system falls under Privacy Act systems of record and individuals have a right of access to request a copy of the information about themselves.

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 are required to provide a written request to amend or correct their records to the appropriate Privacy Officer or System Manager as outlined in the Privacy Act SOR. Every Privacy Act SOR contains information on Contesting Record Procedure which informs the individual who to contact for redress. Further information regarding access and correction procedures can be found in the notices listed in Appendix A. The VHA Notice of Privacy Practices also informs individuals how to file an amendment request with VHA.

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.

Veterans are informed of the amendment process by many resources to include the VHA Notice of Privacy Practice (NoPP) which states:

Right to Request Amendment of Health Information.
You have the right to request an amendment (correction) to your health information in our records if you believe it is incomplete, inaccurate, untimely, or unrelated to your care. You must submit your request in writing, specify the information that you want corrected, and provide a

reason to support your request for amendment. All amendment requests should be submitted to the facility Privacy Officer at the VHA health care facility that maintains your information.

If your request for amendment is denied, you will be notified of this decision in writing and provided appeal rights. In response, you may do any of the following:

- File an appeal.
- File a "Statement of Disagreement"
- Ask that your initial request for amendment accompany all future disclosures of the disputed health information.

Individuals seeking information regarding access to and contesting of VA benefits records may write, call, or visit the nearest VA regional office. Additional notice is provided through the SORS listed in 6.1 of this PIA and through the Release of Information Office where care is received.

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.

Formal redress via the amendment process is available to all individuals, as stated in questions 7.1-7.3. In addition to the formal procedures discussed in question 7.2 to request changes to one's health record.

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: There is a risk that members of the public will not know the relevant procedures for gaining access to, correcting, or contesting their information.

Mitigation: The risk of incorrect information in an individual's records is mitigated by authenticating information, when possible, Additionally, staff verifies information in medical records and corrects information identified as incorrect during each patient's medical appointments. The NOPP discusses the process for requesting an amendment to one's records.

The Release of Information (ROI) office is available to assist Veterans with obtaining access to their health records and other records containing personal information. The Veterans' Health Administration (VHA) established My HealtheVet program to provide Veterans remote access to their medical records. The Veteran must enroll and have access to the premium account to obtain access to all the available features. In addition, VHA Directive 1605.01 Privacy and Release of Information establishes procedures for Veterans to have their records amended where appropriate.

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? F

Local VHA site Administrative Officer/Supervisor/ADPAC/designee(s) submit an ePAS request for new application user's Veterans Health Information Systems and Technology Architecture (VistA) System account and the new application users have completed the Talent Management System (TMS) VA Privacy and Information Security Awareness and Rules of Behavior Training. Staff roles are determined by the VistA Person Class codes. Providers must have a valid Person Class in VistA File 200 (New Person) File. Local VHA site OI&T is responsible to complete the ePAS request. OI& Technical staff complete the ePAS approval for System Administrator (grant server access), Application Administrator (manage application), and/or VistA Management (manage VistA System related tasks)

Talent Management System (TMS) Inform Security for IT Specialist, Information Security for System Admin, Elevated Privileges for System Access, and VA Privacy and Information Security Awareness and Rules of Behavior Training. Non-Mail enabled account (NMEA) and associated token (USB/OTP) to access the servers.

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

8.1b 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?

Other agencies do not have access to COTS Interface Division servers/applications.

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.

Each Order Tracking Manager-Dermatology (OTM-Derm) application require application-specific VistA menu option(s) and/or VistA security key(s) to retrieve, create, and store data in VistA.

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

Yes, VA Contractors will have access to the system and PII.

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

Contractors and vendors partner with the COTS Enterprise staff to maintain DSI applications on VA owned servers. Elevated Privileges for contractors are managed and approved in the ePAS system and reviewed annually by the Contracting Officer Representative (COR). All contractor access is determined by roles, menus and keys that are assigned according to least privilege. Contractors are required to complete required Information Security training and system administrator training and comply with national rules of behavior as part of their contractual obligations.

8.2c. Does the contractor have a signed confidentiality agreement?

No. DSS employees are required to protect the confidential information of DSS and its customers, which includes the VA. All VA contracts have confidentiality provisions that requires DSS and its employees to comply with.

8.2d. Does the contractor have an implemented Business Associate Agreement for applicable PHI?

Yes, The VA has a BAA with DSS.

8.2e. Does the contractor have a signed non-Disclosure Agreement in place?
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.

No. DSS has never signed NDAs with the VA, but our VA contracts have confidentiality provisions that requires DSS and its employees to comply with.

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

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

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

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

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

8.4a If Yes, provide:

1. The Security Plan Status: Approved
2. The System Security Plan Status Date: 20-Apr-2023
3. The Authorization Status: Authority to Operate (ATO)
4. The Authorization Date: 08-Jun-2023
5. The Authorization Termination Date: 07-Jun-2025
6. The Risk Review Completion Date: 31-May-2023 7. The FIPS 199 classification of the system (LOW/MODERATE/HIGH): High

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.***

Order Tracking Manager-Dermatology (OTM-Derm) is a minor application under the DSI Enterprise ATO.

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)***

System does not use cloud technology.

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.*

System does not use cloud technology.

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.

System does not use cloud technology.

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.

System does not use cloud technology.

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).

System does not use cloud technology.

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.

NANCY KATZ-JOHNSON

Digitally signed by NANCY KATZ-JOHNSON
Date: 2025.03.26 11:23:35 -04'00'

Privacy Officer, Nancy katz-johnson

ROLAND PARTEN

Digitally signed by ROLAND PARTEN
Date: 2025.03.26 10:06:32 -05'00'

Information System Security Officer, Roland Parten

KEITH RUIZ

Digitally signed by KEITH RUIZ
Date: 2025.04.02 08:45:09 -04'00'

Information System Owner, Keith Ruiz