Privacy Impact Assessment for the VA IT System called:

Matter Tracking System Assessing

VACO

Secretary of VA / Congressional / Legal Affairs (SCLA) Product Line

Date PIA submitted for review:

January 31, 2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Lynn A Olkowski	Lynn.Olkowski@va.gov	202-632-8406
Information System Security Officer (ISSO)	Omobolaji Olaoye	Omobolaji.Olaoye@va.gov	240-484-9324
Information System Owner	Michael Ketelaar	Michael.Ketelaar@va.gov	321-639-1989

Abstract

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

The Matter Tracking System (MTS) is built on the Microsoft Dynamics 365 (MD365) platform. MTS has been configured in the Customer Relationship Manager (CRM) module to track investigations performed by the Office of Accountability and Whistleblower Protection (OAWP). OAWP receives a disclosure from a Complainant via an online form, phone call or email. Intake Analysts analyze disclosures and forwards them to the appropriate investigative organizations, as defined by the organization's scope. If the disclosure type falls within OAWP's scope, OAWP investigators investigate the case and track notes and documents in MTS.

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.*

Matter Tracking System Assessing; Office of Accountability and Whistleblower Protection (OAWP)

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

The Office of Accountability and Whistleblower Protection (OAWP) manages all internal affairs and has a broad and expansive mission to protect whistleblower rights and recommend discipline and/or termination of employees due to poor performance or misconduct. OAWP's Matter Tracking System (MTS) provides required congressional reporting capabilities and real-time reporting requirements mandated by the Department of Veterans Affairs (VA) Accountability and Whistleblower Protection Act of 2017, Public Law 115-41.

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

Office of Accountability and Whistleblower Protection (OAWP)

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.*

The expected number of individuals whose information is stored in the system is dependent on the number of disclosures made. MTS handles disclosures from across the Department of Veterans Affairs including the Veterans Health Administration (VHA), the Office of Information and Technology (OIT), the National Cemetery Administration (NCA), Veterans Benefits Administration (VBA) and other Veterans Affairs related entities.

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

The Office of Accountability and Whistleblower Protection (OAWP) collects and manages information, referred to as a Case/Matter, reported to OAWP from both anonymous and identified sources. A Case/Matter could be potential information or activity that is deemed illegal and unethical within the VA organization. The information of alleged wrongdoing can be classified in many ways: violation of VA policy/rules, law, regulation, as well as fraud and corruption. OAWP Matter Tracking System (MTS) is a system that receives concerns and complaints for the VA. The core OAWP processes are Disclosure, Investigation, Compliance Reporting, Document Management, and Employee Relations coordination. MTS integrates these processes to support data reuse when appropriate, cataloging documents for a Case/Matter, and enabling OAWP business processes to be followed.

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

There are no external connections.

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.

Matter Tracking System (MTS) utilizes Microsoft Dynamics 365 (MD365) which is a commercial off-the-shelf (COTS) product hosted on the Microsoft GovCloud, delivered as Software as a Service (SaaS) and is Federal Risk and Authorization Management Program (FedRAMP) approved.

3. Legal Authority and SORN

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

https://www.federalregister.gov/documents/2020/04/24/2020-08615/privacy-act-of-1974-system-of-records “Matter Tracking System (MTS)-VA,” (190VA70).

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?

SORN is completed with no planned revisions.

D. System Changes

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

No planned changes.

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

No planned changes.

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)

PII Mapping of Components (Servers/Database)

Matter tracking System Assessing consists of 0 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 Matter tracking System Assessing 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.

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?

Disclosures are initially submitted and entered directly into MTS by an individual such as VA employees, contractors, volunteers, or the general public. The submitter can choose to submit the disclosure anonymously or can choose to provide identifying information. The disclosures consist of allegations that are stored in the Matter Tracking System (MTS) application where OAWP will triage them for further investigation.

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.

N/A

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

N/A

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 via a website/portal, by an individual, or it is entered within the application directly from OAWP staff, depending on the method used to report an allegation. (Available options include phone, fax, email and website/portal.) Information is stored in the MTS database for use by the OAWP Intake and Referral and Investigations teams.

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.

N/A

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 OAWP Intake and Referral Team verifies the disclosure with the Complainant Party for accuracy when processing forms for potential investigation. The information does not need to be re-checked unless the Complainant Party requests to change or update any previously submitted information.

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.

N/A

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

https://www.federalregister.gov/documents/2020/04/24/2020-08615/privacy-act-of-1974-system-of-records "Matter Tracking System (MTS)-VA," (190VA70).

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

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

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

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

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

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

<u>Principle of Data Quality and Integrity:</u> 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:

<u>Privacy Risk:</u> The names of the Government employee and/or their phone numbers and email are data elements available to the public and typically do not cause a PII concern. However, in certain cases, when these innocuous data elements are combined with other pieces of data, it has the potential to become sensitive PII. For example, in MTS, the name of the individual becomes PII due to the fact it is associated with a very sensitive investigation (whistleblower). Failure to account and mitigate privacy risks in this case may cause substantial harm, embarrassment, inconvenience, and/or unfairness to an individual.

<u>Mitigation:</u>

- Only data elements required to execute the background investigation business processes are collected. These data elements are minimal identifying characteristics, i.e.: Name, Facility Name, Organizational Unit
- PII information is voluntarily submitted by users.
- MTS adheres to information security requirements instituted by the VA Office of Information Technology (OIT) and the VA Enterprise Cloud (VAEC) Program.
- MTS System Categorization Level is Moderate and the data is stored in a FEDRAMP certified High environment protected by High level security controls
- Both contractor and VA employees are required to take Privacy, Health Insurance Portability and Accountability Act (HIPAA), and information security training annually
- MTS access is granted only to Role Holders with a need to access the data.
- OAWP defined the software product configuration requirements to customize data access needs for each role holder category, as well as limiting access within organizational boundaries

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.

Information Collected	Business Purpose (Internal to VA)
Name of VA Employee	Used to contact individual.
Home or Mailing Address	Used to contact individual.
Telephone Numbers (Home, Office, Cell)	Used to contact individual.
Email Address	Used to contact individual.

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.

Incoming disclosures are reviewed and processed by OAWP Intake Analysts. If the user submits the completed form with an email address, they will receive an acknowledgement message that includes the case number assigned to their submission. Their submission will be reviewed, and they will be informed of the progress of the review and additional actions. MTS does not synthesize information. Information is collected and stored in integrated SharePoint libraries.

OAWP is dedicated and empowered to provide transparency and build public trust and confidence throughout the entire VA system. The office is committed to preserving the cultural integrity of the Department while conducting balanced, fair and efficient investigation of VA whistleblower and Veteran disclosures, timely remedial resolutions and responsive recommendations. Additionally, OAWP provides the protection of valued VA whistleblowers against retaliation for their disclosures.

OAWP is made up of the following divisions, which fulfill the following roles:

Intake and Referral: Comprised of trained team members that help quickly facilitate resolution of VA employee whistleblower disclosures made on the Department. The division determines if matters fall within OAWP's scope and takes the appropriate course of action on each matter. The team provides guidance, oversight, analysis and training on the whistleblower program and ensures all VA administrations implement recommendations from audits and investigations carried out by various entities including Office of Special Counsel (OSC) and Office of Inspector General (OIG).

Investigations: The primary entity within the VA for investigating senior leader misconduct and wrongdoing as well as allegations of whistleblower retaliation. The division makes recommendations and communicates Department policies that govern investigating non-criminal allegations of misconduct or malfeasance including whistleblower retaliation and other accountability matters throughout the Department. The division works closely with senior management to prepare disciplinary actions in instances of senior leader misconduct or poor performance.

Compliance: The Compliance division reports OAWP's recommendations regarding disciplinary and accountability actions to the VA Secretary and Congress. The Compliance division must also report to Congress any recommendations that were not taken by Superiors for confirmed wrongdoing/retaliation. The Compliance division is governed by the Department of Veterans Affairs (VA) Accountability and Whistleblower Protection Act of 2017, Public Law 115-41.

Quality: The OAWP Quality division is responsible for performing internal audits on investigations. Investigative cases are evaluated for proper process, policy, procedure and documentation as defined by OAWP.

Training: The OAWP Training division provides training to VA employees on the Accountability Law and provides guidance to management officials on the implementation of the Accountability Act and whistleblower protections. It is also responsible for training OAWP divisions on policy and procedures.

Stakeholder Engagement: The Stakeholder Engagement division communicates with OAWP stakeholders. It includes the FOIA office, which serves as the primary entity responding to requests for data contained in the Office of Accountability and Whistleblower Protection systems.

Information Systems Management: Serves as the primary lead for maintaining the MTS system, providing system support, performing reporting, analytical and performance consultative services to OAWP, granting access requests, providing process improvement and configuration of workflows. Team members develop and maintain solutions for caseload data tracking and management.

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.

That would depend on the situation and decided during the OAWP investigation

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?

MTS data in transit is encrypted and secured via Hypertext Transfer Transport Protocol - Secure (HTTPS), which runs on TCP/IP port 443. Data at rest is stored encrypted in the Microsoft GovCloud which has a FedRAMP high rating.

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

N/A

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

Access to Personally Identifiable Information (PII) in the Matter Tracking System requires VA network access via PIV card and PIN, which is authenticated through Active Directory Federated Services (ADFS), using a Security Assertion Markup Language (SAML) token. In addition, OAWP MTS users must have a specific role assigned in order to access the MTS system. Roles are defined by the access required in order to perform specific job functions. Investigative case data within MTS is publicly accessible via the Freedom of Information Act once a case is closed. Active cases are secured via role-based access rules, as well as VA network accessibility utilizing two-factor authentication (PIV card and PIN) as stated above.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

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

2.4a How is access to the PII determined?

Access to PII is limited by the MTS application to only those data items deemed necessary for OAWP personnel to perform their job, as determined by their management team and their job description.

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

User roles are implemented to restrict user's access to only the specific information required to perform their job function. Roles within the system are determined and requested by OAWP management. User access is provided by MTS System Administrators following receipt of request from appropriate individuals

2.4c Does access require manager approval?

Yes, individual roles are requested by OAWP management.

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

System Administrators can provide that information as needed

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

The Department of Veterans Affairs ensures that the practices stated in the PIA are reinforced by requiring Contractors and VA employees to complete all VA trainings including VA Privacy and Information Security Awareness and Rules of Behavior (VA 10176) and Privacy and HIPAA Training (VA 10203). Contractors and VA employees are required to agree to all rules and regulations outlined in trainings, along with any consequences that may arise if failure to comply

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*

Information Retained
Name of VA Employee
Home or Mailing Address
Telephone Numbers (Home, Office, Cell)
Email Address

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.*

MTS records retention policy and guidelines are set by VA Human Resources and Administration (VA HR&A) and detailed in the Records Retention Period for Adverse Action Files memorandum. Under the guidance of this memorandum, adverse action files, including administrative grievances, disciplinary actions, and performance-based actions, must be maintained for seven years from the time the file is closed.

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?

MTS records retention policy and guidelines are set by VA Human Resources and Administration (VA HR&A) and detailed in the Records Retention Period for Adverse Action Files memorandum.

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

Under the guidance of this memorandum, adverse action files, including administrative grievances, disciplinary actions, and performance-based actions, must be maintained for seven years from the time the file is closed. MTS purges records after seven years. Additionally, MTS follows the Office of Personnel Management (OPM) and VA-wide records retention policies.

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.

Records are destroyed 7 years after record is closed or becomes inactive. Electronic records will be permanently deleted from MTS by the System Administrator.

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.

Along with the Business Owner, the Product Owner(s) will screen all VA Role Holders that will have access to the PII data within MTS. Only approved VA Role Holders will have access to MTS data for the sole purpose of conducting investigations from disclosures. Unless otherwise approved by a senior VA executive, use of PII within MTS for testing new applications or information systems is an inappropriate use of the MTS data.

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

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

<u>*Principle of Minimization:*</u> *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?*

<u>Principle of Data Quality and Integrity:</u> 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:

<u>Privacy Risk:</u> If information is retained longer than specified, privacy information may be released to unauthorized individuals.

<u>Mitigation:</u> There is no vulnerability risk to having archived records and active records existing in different locations, and there is no risk of the data scaling above the available system capacity. In addition, all data at rest within the MTS security boundary is encrypted in accordance with FIPS 140-2, as well as protected by FEDRAMP certified "High" security controls. Collectively, these controls within the MTS security boundary provide maximum protection to all MTS data.

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?

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

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:

<u>Privacy Risk:</u> If appropriate safeguards are not in place, then Privacy information shared within the Department may result in unauthorized data access.

<u>Mitigation:</u> MTS is limited to only basic PII data elements required to investigate disclosures.

- MTS does not “auto” collect identity or privacy data directly from individuals. MTS receives the data from Authoritative Data Sources authorized to collect the data.
- MTS system adheres to information security requirements instituted by the VA Office of Information Technology(OIT) and the VA Enterprise Cloud (VAEC) Program
- MTS System Categorization Level is Moderate - and the data is stored in a FEDRAMP certified High environment protected by High level security controls.
- Both contractor and VA employees are required to take Privacy, Health Insurance Portability and Accountability Act (HIPAA), and information security training annually
- MTS access is granted only to Role Holders (OAWP Personnel) with a need to access the data as per their respective job function
- MTS Business Owner defines the requirements for - data access needs for each role holder category, as well as limiting access within organizational boundaries.
- Release of PII to unauthorized individuals is prohibited by the Privacy standards mandated to all VA employees, affiliates, trainees, volunteers, and contractors.

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.

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

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

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

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

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
There are no connections	N/A	N/A	N/A	N/A

external to VA for MTS.				

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

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

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

Follow the format below:

Privacy Risk: Not applicable. MTS does not have external connections. It does not share data outside of the VA.

Mitigation: Not applicable.

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.

Yes, a notice is provided. SORN: Matter Tracking System (MTS)-VA (190VA70), Document Number: 2020-08615.

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

N/A

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.

The OAWP provides the following notifications to users:

"Thank you for your submission." {After a disclosure is entered into the website.}
"Thank you for completing the Intake Survey."

On the OAWP.va.gov website:

"The Office of Accountability and Whistleblower Protection (OAWP) promotes and improves accountability within the Department of Veterans Affairs (VA)

- The office receives and investigates:
  - allegations of misconduct and poor performance against VA senior leaders,
  - allegations of whistleblower retaliation against VA supervisors.
- The office receives whistleblower disclosures from VA employees and applicants for VA employment, and if they do not involve whistleblower retaliation or senior leader misconduct or poor performance, refers it for investigation within VA while the office monitors the investigation.
- The office is responsible for tracking and confirming VA's implementation of recommendations from audits and investigations carried out by VA's Office of Inspector General, VA's Office of the Medical Inspector, the U.S. Office of Special Counsel, and the U.S. Government Accountability Office.
- The office educates employees and stakeholders on whistleblower rights and protections. "

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.

Personal information entered into MTS is strictly voluntary. There is no penalty or denial of service attached, and there are very few required fields on the form. Complainants have the option to submit disclosures anonymously as well.

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.

If information is omitted, it may hinder the efforts of the OAWP staff to investigate matters effectively, however, personal information entered into MTS is voluntary and Complainants have the option to remain anonymous. While remaining anonymous limits OAWP's ability to contact the Complainant, as well as provide status updates on their case, it is not penalized in any way. Complainants check boxes on the Intake form stating which information they are willing to share.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

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

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

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

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

Privacy Risk: Individuals are informed that filing a disclosure is voluntary. A potential risk would be if an individual did not read the notice on the registration page.

Mitigation: Per 38USC323, the Assistant Secretary OAWP, cannot disclose the identity of an individual making a whistleblower disclosure to OAWP without the individual's consent except as provided by the Privacy Act. PII stays within OAWP.

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.***

Complainants discuss their case with OAWP Intake Analysts and Investigators who verify the information recorded in MTS is accurate. OAWP also has a Freedom of Information Act (FOIA) office whose purpose is to respond to information requests regarding investigative cases. Personnel can send FOIA requests to VAAccountabiityTeam@va.gov to obtain copies of their disclosure and files once the case is closed

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).

N/A

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.

N/A

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.

Complainants discuss their case with OAWP Intake Analysts and Investigators who verify the information recorded in MTS is accurate, to the best of the Complainants knowledge. Intake Analysts use various tools to confirm the identity of Persons of Interest and Witnesses. Tools used include

HRSMART data and the VA Exchange Global Address List. (These are separate systems from MTS.)

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.

Complainants discuss their case with OAWP Intake Analysts and Investigators who verify the information recorded in MTS is accurate. If needed, OAWP Intake and Investigative staff correct the data in MTS as the case develops. Email and phone calls are methods of communication with the Complainant, which are documented in MTS. OAWP also retains a copy of the original disclosure in MTS for reference.

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 can follow the FOIA process by sending an email to VAAccountability@va.gov.

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?

<u>Principle of Individual Participation:</u> 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:

<u>Privacy Risk:</u> An individual may want to review the content of their record to check for data accuracy. The magnitude of harm associated with this risk to the VA is low.

<u>Mitigation:</u> Individuals provide information directly to the MTS application via the OAWP Intake Portal (website) or by calling the hotline. Any validation performed would merely be the individual personally reviewing the information before he/she provides it. Intake Analysts and Investigators also review content with individuals during interviews. NOTE: There is an effort underway to allow the Complainant to review the data they entered on the website prior to submitting, however the functionality has not been promoted to Production as of yet. (Expected in Summer/Fall 2022.)

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.

No individuals outside VA will have access to MTS. The MTS Business Owner will determine the individuals that require access to MTS and approve all access requests. The MTS Product Owner is responsible for managing the MTS licenses, which includes tracking the users currently authorized to access the system, removing access privileges for those no longer authorized to access the system, as well as tracking the remaining number of available licenses.

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?

N/A

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.

MTS users are categorized into role holder categories that execute different tasks associated with OAWP functions. Each role holder has specific access privileges within MTS that are limited to the specific data access needs for that role holder. The MTS software product is configured to deny role holders from accessing information beyond the access privileges assigned to their role.

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.

VA contract employee access is verified through the Contracting Officer's Representative (COR) and other VA supervisory/administrative personnel before access is granted to any VA system. Contractor access is reviewed annually at a minimum. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of behavior training via the VA Talent Management System (TMS). All contractors are vetted using the VA background investigation process and must obtain the appropriate level background investigation for their role. Contractors with systems administrative access are required to complete additional role-based training prior to gaining system administrator access. Generally, contracts are reviewed at the start of the initiation phase of acquisitions and again during procurement of option years.

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.

MTS role holders are subjected to same annual privacy and security training requirements as all VA employees. 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 prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training which all personnel must complete via the VA's Talent Management System (TMS). After the user's initial acceptance of the Rules, the user must 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.

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Complete
2. *The System Security Plan Status Date:* December 1, 2021
3. *The Authorization Status:* 3 Year ATO
4. *The Authorization Date:* January 14, 2021
5. *The Authorization Termination Date:* January 14, 2024
6. *The Risk Review Completion Date:* August 24, 2020
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

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

N/A

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)*

MTS is a MD365 SaaS hosted on Microsoft's GovCloud.

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.*

The VA owns the Data. Contract 47QTCA22D003G is a VA Wide Enterprise Licensing Agreement Contract awarded to Dell Federal Systems. The contract list references to VA Data and Privacy. From Section 9: "The Contractor shall ensure adequate LAN/Internet, data, information, and system security in accordance with VA standard operating procedures and standard PWS language, conditions, laws, and regulations. The Contractor's firewall and web server shall meet or exceed VA minimum requirements for security. All VA data shall be protected behind an approved firewall. Any security violations or attempted violations shall be reported to the VA Program Manager and VA Information Security Officer as soon as possible. Contractor shall follow all applicable VA policies and procedures governing information security, especially those that pertain to certification and accreditation. Section 12b: "Adequate security controls for collecting, processing, transmitting, and storing of Personally Identifiable Information (PII),as determined by the VA Privacy Service, must be in place, tested, and approved by VA prior to hosting, operation, maintenance, or use of the information system, or systems by or on behalf of VA. Additional information can be obtained from the Contracts COR".

9.3 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.

This question is related to privacy control DI-1, Data Quality.

No ancillary data is collected by this cloud application.

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.

Dynamics 365 is hosted in Microsoft's GovCloud and offered as a Software as a Service (SaaS). MTS is built on Dynamics 365. Access and Support are jointly managed between the Service Provider and OAWP's ISM team

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).

MTS is not utilizing RPA at this time

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**

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

Signature of Responsible Officials

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

Lynn A Olkowski Digitally signed by Lynn A Olkowski
Date: 2023.02.27 08:54:20 -06'00'

Privacy Officer, Lynn A Olkowski

Omobolaji O. Olaoye 1063577 Digitally signed by Omobolaji O. Olaoye 1063577
Date: 2023.02.27 10:19:28 -05'00'

Information System Security Officer, Omobolaji Olaoye

Michael L. Ketelaar 481604 Digitally signed by Michael L. Ketelaar 481604
Date: 2023.02.27 08:28:16 -05'00'

Information System Owner, Michael Ketelaar

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).

SOR Number/ Federal Register Citation	System Title	Publication Date	Summary Description	Point of Contact
190VA70/ 85 FR 23134	Matter Tracking System (MTS)-VA	4/24/2020	The information in this system is used for reporting and tracking incidents contemplated by the Department of Veterans Affairs Accountability and Whistleblower Protection Act of 2017 and includes records from Whistleblowers, Disclosing Parties and Persons of Interest.	Tanya Guimont

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