Privacy Impact Assessment for the VA IT System called:

# Equal Employment Opportunity EcoSystem (EEOE), designated as "E²"

# VA Office of Information & Technology (OIT)
# Office of Resolution Management, Diversity & Inclusion (ORMDI)

Date PIA submitted for review:

5/31/2023

System Contacts:

| Role | Name | E-mail | Phone Number |
|---|---|---|---|
| Privacy Officer | Zulema Bolivar | Zulema.Bolivar@va.com | 202-461-6932 |
| Information System Security Officer (ISSO) | LaToya Butler-Cleveland | LaToya.Butler-Cleveland@va.gov | 202-461-6893 |
| Information System Owner | Glenn Thomas | Glenn.Thomas@va.gov | 202-461-0293 |

## Abstract

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

The Office of Resolution Management, Diversity and Inclusion (ORMDI), Department of Veterans Affairs (VA) is utilizing an electronic records management system, titled "Equal Employment Opportunity Ecosystem (EEOE)" (designated as "E²"), to manage and execute the VA's Equal Employment Opportunity (EEO) Program to include processing EEO Complaints, Conflict Resolution and Settlement Agreements, this program integrates Religious Accommodations (38CFR Parts 2 and 15 and Public Law 105-114); the Harassment Prevention Program (HPP) to proactively respond to allegations of harassment and ensure prompt corrective measures are taken to decrease harassing behavior in the workplace (Title 38, Code of Federal Regulations, Chapter 1, Parts 15 and 18); the Reasonable Accommodation and Personal Services (RA/PAS) processes to help those with a disability apply for a job, perform the duties of a job or enjoy the benefits and privileges of employment (Rehabilitation Act of 1973 and the Americans with Disabilities Act (ADA) Amendments Act of 2008 (ADAAA)); the External Civil Rights Discrimination Complaints Program (ECP) to address issues of discrimination in federal programs and activities (Title VI of the Civil Rights Act of 1964), and the Management Services Directorate (MSD) will have an integrated, collaborative system to capture budget, human resources, contracts, and facility/space requirements for ORMDI. ORMDI's E² system is a comprehensive and secure repository for electronic records management to include identification, retrieval, maintenance, routine destruction, report generation, and compliance management. E² supports secure agencywide collaboration and communication by connecting these separate Program Offices and facilities located in various geographic areas using a secure and common platform.

## 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.***

Equal Employment Opportunity EcoSystem (EEOE), designated as "E²"
Office of Resolution Management, Diversity & Inclusion (ORMDI)

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

The Deputy Assistant Secretary for Resolution Management, Diversity & Inclusion (DAS/RMDI) has been delegated authority to supervise and control the operation of the administrative equal employment opportunity (EEO) discrimination complaint processing system within the whole of VA. The DAS/RMDI exercises exclusive authority to establish and modify discrimination complaint processing procedures. In pursuit of these objectives, the Equal Employment Opportunity Ecosystem (EEOE) or (E2) was created to give the VA's Office of Resolution Management, Diversity & Inclusion ORMDI) the ability to perform their mission for the following programs:

- Equal Employment Opportunity (EEO) Program – ORMDI is responsible for administering the VA's Equal Employee Opportunity (EEO) complaint process (38CFR Parts 2 and 15 and Public Law 105-114). The EEO Program addresses allegations of discrimination to include the processing of EEO Complaints Informal and Formal, Conflict Resolutions (CR) and Settlement Agreements.
- Reasonable Accommodation Management System (RAMS) – A system to help those with a disability apply for a job, perform the duties of a job, or enjoy the benefits and privileges of employment. This support is the Reasonable Accommodation and Personal Services (RA/PAS) processes. The purpose of the program is to allow the VA to collect and maintain temporary records on employees with disabilities and applicants for employment, who are receiving reasonable accommodations as required by the Rehabilitation Act of 1973 and the Americans with Disabilities Act (ADA) Amendments Act of 2008 (ADAAA).
- Harassment Prevention Program (HPP) – An enterprise-wide and centralized tracking, monitoring, and reporting system to proactively respond to allegations of harassment, whether or not accompanied by an EEO bases. VA Directive 5979 establishes the Department of Veterans Affairs harassment prevention policy and outlines roles and responsibilities to help VA maintain a workplace free from harassment. This includes reporting harassment allegations to VA leadership to ensure that prompt corrective measures are taken to decrease harassing behavior in the workplace. HPP is responsible for providing education and awareness training on the harassment program.
- External Civil Rights Discrimination Complaints Program (ECP) – The Office of Resolution Management Diversity Inclusion (ORMDI) is VA's liaison with the Department of Justice (DOJ) for addressing issues of discrimination in federal programs and activities. Through the External Complaints Program, civil rights discrimination complaints may be filed against VA under Title VI of the Civil Rights Act of 1964 and other similar statutes, such as Title IX of the Education Amendments of 1972, Age Discrimination Act of 1975, Section 504 of the Rehabilitation Act of 1973, and various Presidential Executive Orders.
- Management Services Directorate (MSD) – MSD will have an integrated, collaborative system to capture budget, human resources, contracts, and facility/space requirements for ORMDI.

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

VA Partnership

*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.***

EEO:

- There are approximately 9878 cases currently in E2 with 32,821 cases to be added from the legacy system, by the end of the year. Each case can have one or many Aggrieved Parties and many contacts and Counselors or Supervisors also associated.
- E2 is the main repository of essential documents in the Equal Employment Opportunity Ecosystem (EEO) process Employees make complaints via government email, government phone lines, verbally to their supervisor or through a representative. Complainant information is entered into the application, which are then managed in the Dynamics 365 Online via entry screens, workflow processes, email notifications, document (letter) templates, a shared document repository, and common reporting architecture.

RAMS:

- Currently there are 8,677 cases in RAMS, and it is anticipated that the system will store an additional approximately 5,000 names and Protected Health Information (PHI) and on Department of Veteran Affairs employees enterprise wide, annually. The RAMS system will be used enterprise wide across all three administrations.
- E2 is the main repository of essential documents in the Reasonable Accommodation Management System (RAMS) process. RAMS and A system to help those with a disability apply for a job, perform the duties of a job, or enjoy the benefits and privileges of employment. This support is the Reasonable Accommodation and Personal Services (RA/PAS) processes. PAS provides employees with "targeted disabilities" assistance with performing activities of daily living that an individual would typically perform if they did not have a disability, and that is not otherwise required as a reasonable accommodation.

HPP:

- HPP currently has approximately 3,600 cases and at its historical growth rate is adding approximately 1,500 cases per year. However, growth of reported and tracked cases is expected to double in 2024 to add 3,000 cases per year.
- The Harassment Prevention Program is an enterprise-wide department within the Office of Resolution Management. Incidents are reported by VA Employees, Student/Fellows, Volunteers, Contractors, Veterans or Visitors. HPP reports harassment allegations to VA leadership in order to ensure that prompt corrective measures are taken to decrease harassing behavior in the workplace. HPP is responsible for providing education and awareness training on the harassment program.

ECP:

- Currently approximately 200 new cases are processed per year, but this number is expected to double or triple in the next few years.
- The Office of Resolution Management Diversity Inclusion (ORMDI) is VA's liaison with the Department of Justice (DOJ) for addressing issues of discrimination in federal

programs and activities. The External Complaints Program receives and refers for investigation, complaints from Veterans, or anyone closely associated with a Veteran (Fiduciary, caretaker, or some beneficiary) acting on their behalf, who believe they have been discriminated against on the basis of their race, color, national origin (limited English proficiency), age, sex, disability, or reprisal in federally conducted and federally assisted programs or activities. Federally conducted programs are those that are directly administered by the Department, such as healthcare and other VA benefits. Federally assisted programs are those programs that receive Federal financial assistance.

MSD:

- There are approximately 450 current resources information being stored in the E2 MSD system and over the next year this will increase up to 1,000.
- The Management Services Directorate (MSD) is owned by the Department of Veteran Affairs, Office of Resolution Management Diversity & Inclusion (ORMDI). E2 MSD will be the main repository of essential information for the budget, human resources, contracts, and facility/space requirements for ORMDI contracts and resources.

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

- EEO - General Description of Information: Equal Employment Opportunity (EEO) Program is the main repository of essential documents in the EEO complaint process. EEO processes – EEO Complaints Informal and Formal, Conflict Resolutions (CR) and Settlement Agreements: Aggrieved Parties, Complaint, legal documents, statement of witnesses, reports of interviews, records of investigations, fact finding reports, recommendations, final decisions, request for reconsideration and reconsideration decisions, contact information and case details.
- EEO - Purpose for Collecting Information: An employee, former employee, or applicant for employment, who believes discrimination occurred on the bases of race, color, religion, sex, sexual orientation, transgender orientation, national origin, age (40 or over), disability, genetic information, or retaliation for EEO activities, may initiate a complaint of discrimination. Once a written complaint is received, it will be reviewed for procedural sufficiency and then referred to the primary Administration (Veterans Health Administration, Veterans Benefits Administration or National Cemetery Administration) for further processing, including the investigative process (which will address those issues that were raised in the complaint) and the findings or resolution of those issues involved

- RAMS - General Description of Information: A system to support the Reasonable Accommodation and Personal Services (RA/PAS) processes gathers the following information: Contact information on employees with disabilities and applicants for employment, who are receiving reasonable accommodations, Reason for Request (Medical documentation goes only to the assigned Reasonable Assignment Coordinator), Accommodation Requested. Process Meeting Notes.
- RAMS - Purpose for Collecting Information: ORMDI Reasonable Accommodations Personal Assistance Services (PAS) provides employees with targeted disabilities assistance with performing activities of daily living that an individual would typically

perform if they did not have a disability, and that is not otherwise required as a reasonable accommodation. In general, an accommodation is a change in the work environment or in the way things are customarily done that would enable an individual with a disability to enjoy equal employment opportunities. The law requires federal agencies to provide reasonable accommodation to an employee or job applicant with a disability, unless doing so would cause significant difficulty or expense for the employer ("undue hardship"). Information captured includes type of accommodation request, medical documentation such as limitation, diagnosis, prognosis, nature of the disability, the need for accommodation, reconsideration request and decisions, notes, forms and support materials.

- HPP - General Description: The Harassment Prevention Program (HPP) requires that immediate and appropriate corrective actions are taken to eliminate harassing conduct regardless of whether the conduct violated the law or whether an employee pursues an EEO complaint. The HPP will solely focus on taking whatever action is necessary to promptly bring the harassment to an end, or to prevent it from occurring at all.

  The harassment prevention procedures do not affect rights under the EEO complaint process. The harassment prevention procedures process is entirely separate and apart from the EEO complaint process. This means that an employee who reports allegations of harassment in accordance with VA Directive 5979 and VA Handbook 5979 has not filed an EEO complaint. An employee who wishes to file a discrimination complaint should contact an EEO counselor at (888) 566-3982 for more information within 45 days of the alleged harassing conduct. An employee may report harassment using the HPP procedures and file an EEO complaint simultaneously.

- HPP Purpose for Collecting Information: These records are maintained for the purpose of conducting internal investigations into allegations of harassment brought by current or former EEOC employees, contractors, applicants, interns, and volunteers and taking appropriate action in accordance with EEOC Order 560.005.

- ECP – General Description of Information: ECP records include the Reporting Individual, Target of Alleged Conduct and Alleged Harasser Point of Contract Information, Administration and Facility Information, Incident Information, Supportive Measures Requested, Notification to the facility; Investigator findings; preventative or corrective action taken; written follow up documents
- ECP - Purpose for Collecting Information: The Office of Resolution Management Diversity Inclusion (ORMDI) is VA's liaison with the Department of Justice (DOJ) for addressing issues of discrimination in federal programs and activities. Through the External Complaints Program, civil rights discrimination complaints may be filed against VA under Title VI of the Civil Rights Act of 1964 and other similar statutes, such as Title IX of the Education Amendments of 1972, Age Discrimination Act of 1975, Section 504 of the Rehabilitation Act of 1973, and various Presidential Executive Orders. ORMDI's External Civil Rights Discrimination Complaints Program, or ECP, has oversight responsibility for the processing of external discrimination complaints and serves as the intake office for these complaints.

- MSD - General Description of Information: Information captured for MSD includes ORMDI personnel point of contract, pay, job title and description, performance, telework, leave, information. MSD also manages the contracts for ORMDI so acquisition/budget information and facility/space information.
- MSD - Purpose for Collecting Information: MSD will have an integrated, collaborative system to capture budget, human resources, contracts, and facility/space requirements for ORMDI.

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

Case and Contact Information is provided to other Internal VA Entities to effect notifications.

G. *What modules share information?*

The following E2 modules share information with these Internal Entities:

| E2 Module /Application | Internal System Name | Data Direction & Information | Type of Connection | Agreements Established |
|---|---|---|---|---|
| EEO<br>RAMS<br>HPP<br>ECP | Veterans Benefits Administration (VBA)/email | Bidirectional Contact information, case details | Internal VA | N/A |
| EEO<br>RAMS<br>HPP<br>ECP | Veterans Health Administration (VHA)/email | Bidirectional Contact information, case details | Internal VA | N/A |
| EEO<br>RAMS<br>HPP<br>ECP | The Department of Veterans Affairs Central Office (VACO)/email | Bidirectional Contact information, case details | Internal VA | N/A |
| EEO<br>RAMS<br>HPP<br>ECP | National Cemetery Administration (NCA)/email | Bidirectional Contact information, case details | Internal VA | N/A |
| EEO<br>RAMS<br>HPP<br>ECP | Office of Information Technology | Bidirectional Contact Information, case details | Internal VA | N/A |
| EEO | VA Office of General Counsel | Unidirectional from EEO to OGC (Election created for EEOC Hearing, OEDCA Final Agency Decision (FAD), EEOC Appeal) | Internal VA | N/A |

*H. 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.*

ORMDI EEO Ecosystem (EEOE) is hosted in Dynamics 365 Online, a Government Cloud Service Provider (CSP). EEOE is a Software-as-a- Service (SaaS) offering as defined in NIST SP800-145. Both the primary and backup data centers are owned by Microsoft, who is the VA contracted Cloud Service Provider (CSP). Hosting occurs at a Primary and Alternate site with direct connections to the VA TIC (Trusted Internet Connection) from each location. EEOE is an internal system to be used enterprise wide across the Department of Veteran Affairs three administrations.

*3.* ***Legal Authority and SORN***

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

Legal authority to operate EEOE is found in:

1 Title 29 United States Code (U.S.C.), Sections 791, 792, and 793

2 Title 38, United States Code (U.S.C.), Part I, Chapter 3, Department of Veterans Affairs, Chapter 5, Authority and Duties of the Secretary, and Chapter 7, Employees

3 Title 38, Code of Federal Regulations, Chapter 1, Parts 15 and 18

4 Public Law 105-114, Veterans' Benefits Act of 1997, Title 1 – Equal Employment Opportunity in the Department of Veterans Affairs

5 5 U.S.C. § 2301, Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002 (noFear), as amended by Elijah E. Cummings Federal Employee Antidiscrimination Act of 2020

6 29 C.F.R. § 1604, Guidelines on Discrimination Because of Sex

7 29 C.F.R. § 1605, Guidelines on Discrimination Because of Religion

8 29 C.F.R. § 1611, Privacy Act Regulations

9 29 C.F.R. § 1614, Federal Sector Equal Employment Opportunity

10 29 C.F.R. § 1630, Regulations to Implement the Equal Employment Provisions of the Americans with Disabilities Act

11 29 U.S.C. § 621 et seq., Age Discrimination in Employment,

12 29 U.S.C. § 791; Sections 501, 504, and 505 of the Rehabilitation Act of 1973 (Public Law 93-112)

13 Rehabilitation Act of 1973

14 Code of Federal Regulations (CFR), Sections 1611, 1614, and 1630 (1614.203 – Rehabilitation Act)

15 38 C.F.R., Part 2 and 15, Delegation of Authority – Equal Employment Opportunity (EEO) Responsibilities

16 38 C.F.R., Part 15 – Enforcement of Nondiscrimination on the Basis of Handicap in Programs or Activities Conducted by the Department of Veterans Affairs

17 38 C.F.R., Part 18 – Nondiscrimination in Federally-Assisted Programs of the Department a of Veterans Affairs – Effectuation of Title VI of the Civil Rights Act of 1964

18 38 C.F.R., Part 18a, Delegation of Responsibility in Connection with Title VI, Civil Rights Act of 1964

19 38 C.F.R., Part 18b, Practice and Procedure under Title VI of the Civil Rights act of 1964 and Part 8 of This Chapter

20 42 U.S.C. 1201 et seq., Title 1 of the Americans with Disabilities Act (ADA) of 1990 and the ADA Amendments Act of 2008 (ADAA)

21 42 U.S.C. § 2000d, Title VI, Civil Rights Act of 1964

22 42 U.S.C. § 2000e et seq., Title VII, Civil Rights

23 42 U.S.C. § 2000e-16, Employment by Federal Government.

24 42 U.S.C. § 2000e(k), Pregnancy Discrimination Act (PDA) of 1978

25 42 U.S.C. § 4151 et seq., Architectural Barriers Act.§

26 42 U.S.C. § 6101-6107, Age Discrimination Act of 1975

27 45 C.F.R. Subpart D – Discrimination on the Basis of Sex in Education Programs or Activities Prohibited, § 86.31, Education programs or activities

28 45 C.F.R. Part 160; 45 C.F.R. Subparts A and E, Part 164, Health Insurance Portability and Accountability Act (HIPPA) of 1996, Standards for Privacy of Individually Identifiable Health Information

29 Executive Order 13548 -- Increasing Federal Employment of Individuals with Disabilities

30 Executive Order 13164, Establish Procedures to Facilitate the Provision of Reasonable Accommodation

31 EEOC Notice 915.002 dated June 18, 1999, Enforcement Guidance: Vicarious Employer Liability for Unlawful Harassment by Supervisors

32 EEOC Guidance on the ADAA

33 EEOC Regulations to Implement the Equal Employment Provisions of the Americans with Disabilities Act, as Amended (29 CFR 1630 Appendix)

34 EEOC Policy Guidance on Executive Order 13164, Requiring Agencies to Establish Procedures to Facilitate the Provision of Reasonable Accommodation

35 EEOC Enforcement Guidance: Reasonable Accommodation and Undue Hardship under the Americans with Disabilities Act

36 VA Handbook 5975.1, Processing Requests for Reasonable Accommodation from Employees and Applicants with Disabilities

37 VA Directive 5979, Harassment Prevention Policy

38 VA Handbook 5979, Harassment Prevention Procedures

39 VA Directive 5977 EEO Complaints Process

40 VA Handbook 5977, EEO Complaints Process

41 VA Directive 6300, Records and information Management

42 VA Handbook 6500, VA 6500 AC-8 – System Use Notification

43 The Privacy Act of 1974

44 EEOC/GOVT-1 – Equal Employment Opportunity in the Federal Government Complaint and Appeals Records

45 The System of Record (SORN) #203VA08 – Department of Veteran Affairs (VA), Office of Resolution Management, Diversity and Inclusion (ORMDI)

46 38 CFR Part 1, RIN 2900-AR95, June 9, 2023, Exemption of "Diversity and Equal Employment Opportunity (EEO) Program Records, "In this notice of proposed rulemaking, VA proposes to exempt this system of records from certain provisions of the Privacy Act in order to prevent interference with harassment and sexual harassment administrative investigations. WP 2023-010 Exemption of Harassment Prevention Program Records – VIEWS 09690147

47 The System of Record (SORN) #09VA05 – Employee Unfair Labor Practice Charges and Complaints, Negotiated Agreement Grievances and Arbitrations – VA

48 The System of Record (SORN) #106VA17 – Compliance Records, Response and Resolution of Reports of Persons Allegedly Involved in Compliance Violations – VA

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

Recent SORN notice 203VA08 published 05/20/2022 to encompass E2:

"SUMMARY:

Office of Resolution Management, Diversity and Inclusion (ORMDI) at the Department of Veterans Affairs (VA) is establishing a new System of Records, entitled Diversity and Equal Employment Opportunity (EEO) Program Records (203VA08), to manage and execute the Equal Employment Opportunity (EEO) Program, Harassment Prevention Program (HPP), Reasonable Accommodation/Personal Assistance Services (RA/PAS) Program, Reasonable Accommodation/Religious Observance, Practice or Belief (hereinafter "Religious Beliefs") Program, External Civil Rights Discrimination Program (ECP), and VA's Diversity and Inclusion programs, including building a model EEO program integrating Affirmative Employment, Special Emphasis, and Religious Accommodations."

SORN Notice includes the cloud technology implement for the secure repository:

"POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Diversity and Equal Employment Opportunity (EEO) Program Records are maintained on paper and electronically at VA facilities by supervisors, management officials, local reasonable accommodation coordinators, and other designated VA staff. Electronic records are also maintained in: Equal Employment Opportunity EcoSystem (EEOE), designated as E-Squared (E2), a comprehensive and secure repository for electronic records management to facilitate identification, retrieval, maintenance, routine destruction, report generation and compliance management; and Light Electronic Action Framework (LEAF), a technology and framework for rapid implementation and deployment of projects that require secure records management, including identification, retrieval, maintenance, routine destruction, report generation, policy compliance, and document routing to create a culture of transparency and accountability."

*D. System Changes*

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

No

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

No

## Section 1. Characterization of the Information

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

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

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

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

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

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

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

Add Additional Information Collected But Not Listed Above Here:

- National Origin
- Sexual Orientation
- Gender Identity
- Religion
- Business email
- Business phone
- Business address
- Position
- Facility
- Facility address
- Facility phone number
- Station, Office, Administration
- Station, Office, Administration address
- Station, Office, Administration phone number
- Date of Request
- EEO Complaint Form (4939) – allegations and requested relief
- RAMS Form 0857 series – type of accommodation and supportive measures requested
- ECP Form 10-0381
- Correspondence and other documents pertinent to the complaint or case, e.g., employment data, reasonable accommodation records, applications for employment, disciplinary actions, etc., notes, memos or supporting materials. Any record relevant to the allegations or complaint
- Affidavits
- Witness Statements,
- Reports of Interviews
- Records of Investigations
- Fact Finding Reports
- Recommendations
- Preventative or Corrective action taken
- Legal documents (final agency decisions, reconsideration decisions, and actions)
- Mailing and contract information for representatives and witnesses
- The person allegedly responsible
- Job Status, Job Title, Series and Grade information
- Mediator POC Information

- Attorney or Representative POC Information
- Dates of meetings
- Settlement agreements
- health care provider limitations, health care provider recommendations,
- The employee may submit their own medical support and records which may contain their address and data of birth. The employee can redact this information before submitting the addition medical documentation.
- Budget Information
- HR Employee Recruitment Information
- HR Employee Credit Card Application and supporting documents
- Facility/Administrative Space Requirements

Information created by EEOE:

- System record resolution rates
- Processing time
- Savings reports
- Offer rates
- Case closure/performance metrics
- Settlement Report metrics
- Basis of Complaints
- EEO Complaint Data by type, formal/informal, location and by individuals
- Participation rates, and other EEOE data
- Emails with Notice Forms as required by law

(No Personal data is aggregated in these reports)

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

Equal Employment Opportunity Ecosystem consists of one key component (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by Equal Employment Opportunity Ecosystem and the reasons for the collection of the PII are in the table below.

**Note**: Due to the PIA being a public facing document, please do not include the server names in the table. The first table of 3.9 in the PTA should be used to answer this question.

*Internal Database Connections*

| Database Name of the information system collecting/storing PII | Does this system collect PII? (Yes/No) | Does this system store PII? (Yes/No) | Type of PII (SSN, DOB, etc.) | Reason for Collection/ Storage of PII | Safeguards |
|---|---|---|---|---|---|
| Power Apps Dataverse SaaS (VA ORMDI Prod) | yes | yes | Employee name<br>First Name,<br>Last Name,<br>Address,<br>Email Addresses,<br>Phone Number,<br>DOB,<br>Race,<br>Ethnicity,<br>National Origin,<br>Sex,<br>Age,<br>Position,<br>Facility,<br>Facility address,<br>Facility phone number,<br>Information concerning issue/claim,<br>Specifics of the complaint (harassment, discrimination, etc.),<br>Legal agreements,<br>Witness POC Information,<br>Witness testimony,<br>Health information if necessary (e.g., disability related) RAMS does collect data that is HIPPA protected.<br>Any record relevant to the allegations.<br>Recommendation for future harassment prevention or determinations/decisions,<br>Budget,<br>Human Resources,<br>HR Employee Recruitment Credit Card application and supporting documents, | Contact Information,<br>Case details,<br>Process the Reasonable Accommodation Request,<br>Process the EEO and HPP Complaint,<br>Processing the ECP Complaint,<br>Fiscal Budgeting,<br>Facilities Management,<br>Contract Management,<br>Human Resources Support | Data is encrypted in transit and at rest.<br>Access to the system is limited; access is audited |

| 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 |
|---|---|---|---|---|---|
| | | | Facility/Administrative Space Requirements | | |

**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.*

The source of PII from a CRM perspective is the Web Services layer.

*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?*

All initial case information is collected directly from the individual (Aggrieved Party, Complainant, Employee, Witness, Legal Representatives, or Veteran), or the Global Listing Address (GAL).
Supportive information is provided by the following:

- Veterans Benefits Administration (VBA) – Compiling personal information
- Veterans Health Administration (VHA) – Compiling personal information
- National Cemetery Administration (NCA) – Compiling personal information
- The Department of Veterans Affairs Central Office (VACO) – Compiling personal information
- The Office of Information Technology – Compiling personal information

*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.*

- Witness Testimonies: Compiling case information
- Legal Representatives: Compiling case information
- Global Listing Address (GAL): Personnel contact, email, job information
- Veterans Benefits Administration (VBA): Compiling personal information
- Veterans Health Administration (VHA): Compiling personal information
- National Cemetery Administration (NCA): Compiling personal information
- The Department of Veterans Affairs Central Office (VACO): Compiling personal information
- The Office of Information Technology: Compiling personal information

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

- EEO: Complaint Form 4939
- EEO: Settlement agreements
- RAMS: Form 0857 series
- RAMS: information obtained from medical documentation provided by the employee
- HPP: Incident Form 10221a
- ECP: VA Form 10-0381
- EEO, RAMS, HPP, & ECP: Memos, letters, emails and other documents pertinent to the complaint, incident or accommodation, (e.g., employment data, reasonable accommodation records, applications for employment, disciplinary actions, etc).
- EEO, HPP & ECP: Affidavits
- EEO, RAMS & ECP: Legal documents (final agency decisions, and actions)
- EEO, RAMS, HPP & ECP: Decisions, reconsiderations decisions, recommendations, notifications
- EEO, RAMS HPP, & ECP: Compile information into reports for analysis
    - System record resolution rates
    - Processing time
    - Savings reports
    - Offer rates
    - Case closure/performance metrics
    - Settlement Report metrics
    - Basis of Complaints
    - EEO Complaint Data by type, formal/informal, location and by individuals
    - Participation rates, and other EEOE data
- MSD: Request and interaction data come from system users and this data is gathered for the process of servicing employees and reporting to management.

**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:

- Directly from the complainant and witnesses
    - VA Form 4939 (OMB Control Number: 2900-0716) – During or shortly after the interactive discussion with the employee, authorized users will access E2 and complete necessary portions of the request to record information pertaining to the request
    - VA Form 0857 series – Reasonable Accommodation information collected from medical documentation and the 0857 series forms that have been provided by the employee

    - VA Form 10221a – Management or the Harassment Prevention Coordinator (HPC) completes the form on behalf of the alleger
    - VA Form 10-0381 – Civil Rights Complaint information collected from the patient or other VHA customer
- Personnel-related information from HR
    - Information collected directly from the employee via face to face, email, phone call and or third party
- From the VA GAL - Personnel contact, email, job information
- Veterans Benefits Administration (VBA) – Compiling personal information via email
- Veterans Health Administration (VHA) – Compiling personal information via email
- National Cemetery Administration (NCA) – Compiling personal information via email
- The Department of Veterans Affairs Central Office (VACO) – Compiling personal information vis email
- The Office of Information Technology – Compiling personal information via email

*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.*

- EEO: VA Form 4939 (OMB Control Number: 2900-0716)
- RAMS: VA Form 0857A – OMB 2900-0767
- RAMS: VA Form 0857K – OMB 2900-0767
- HPP: VA Form 10221a
- ECP: VA Form 10-0381 - OMB Number 2900-0662

**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*.

Information is supplied by:

- The Complainant/Aggrieved Party/Alleger – the Complainant/Aggrieved Party/Alleger is responsible for ensuring its accuracy
- Personnel records supplied by the HR office – the HR manager certifies its accuracy
- Direct testimony from witnesses that is reviewed and signed by the witnesses

This is an internal system to be used enterprise wide across the Department of Veteran Affairs three administrations. Employees make requests via government email, government phone lines, verbally to their supervisor or through a representative. There is no third-party system check as the person provides the needed information to process the request as required by law. The

employee basic data is be pulled from the Global Address List (GAL) which the employer and employee are responsible to ensure is accurate.

*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.*

There is no third-party system check as the person provides the needed information to process the request as required by law. The employee basic data will be pulled from the Global Address List (GAL) which the employer and employee are responsible to ensure is accurate.

**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***

EEOE uses the following legal authorities, arrangements, and agreements to define the collection of information:

1 42 U.S.C. 2000e-16(b) and (c) Employment by Federal Government:
   A. (b)Equal Employment Opportunity Commission; enforcement powers; issuance of rules, regulations.; annual review and approval of national and regional equal employment opportunity plans; review and evaluation of equal employment opportunity programs and publication of progress reports; consultations with interested parties; compliance with rules, regulations, etc.; contents of national and regional equal employment opportunity plans; authority of Librarian of Congress; and,
   B. (c)Civil action by employee or applicant for employment for redress of grievances; time for bringing of action; head of department, agency, or unit as defendant
2 29 U.S.C. 206(d)-Prohibition of sex discrimination
3 29 U.S.C. 633(a)-Non-discrimination on account of age in Federal Government employment
4 29 U.S.C. 791 – Employment of individuals with disabilities
5 29 CFR 1614.203 – Rehabilitation Act
6 Reorganization Plan No. 1 of 1978 – Federal Equal Employment Opportunity Activities
7 43 FR 19607 (May 9, 1978)
8 Exec. Order No. 12106 – Transfer of certain equal employment enforcement functions
9 44 FR 1053 (Jan. 3, 1979)
10 Rehabilitation Act of 1973
11 Americans with Disabilities Act (ADA) Amendments Act of 2008 (ADAAA).
12 Executive Order 13164, Establishing Procedures to Facilitate the Provision of Reasonable Accommodation
13 VA Handbook 5975.1, Processing Requests for Reasonable Accommodation from Employees and Applicants with Disabilities
14 VA Directive 6300, Records and information Management
15 VA Handbook 6500, AC-8 – System Use Notification

16 The Privacy Act of 1974
17 The System of Record (SORN) #203VA08 – Department of Veteran Affairs (VA), Office of Resolution Management, Diversity and Inclusion (ORMDI)
18 The System of Record (SORN) #09VA05 – Employee Unfair Labor Practice Charges and Complaints, Negotiated Agreement Grievances and Arbitrations – VA
19 The System of Record (SORN) #106VA17 – Compliance Records, Response and Resolution of Reports of Persons Allegedly Involved in Compliance Violations – VA
20 The System of Record (SORN) EEOC/GOVT- 1 – Equal Employment Opportunity in the Federal Government Complaint and Appeals Records

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

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

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

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

ORMDI is responsible for administering its mission per the following authorities:

- Equal Employee Opportunity (EEO) complaint process: 38CFR Parts 2 and 15 and Public Law 105-114, VA Directive 5977 - EEO Complaints Process, VA Handbook 5977 - EEO Complaints Process, EEOC/GOVT-1 – Equal Employment Opportunity in the Federal Government Complaint and Appeals Records
- Harassment Prevention Program (HPP) VA Directive 5979 – Harassment Prevention Policy, VA Handbook 5979 – Harassment Prevention Procedures, EEOC Notice 915.002 dated June 18, 1999, Enforcement Guidance on Vicarious Employer Liability for Unlawful Harassment by Supervisors
- Reasonable Accommodation/Personal Assistant Services (RA/PAS) Program Rehabilitation Act of 1973 and the Americans with Disabilities Act (ADA) Amendments Act of 2008 (ADAAA).
- External Civil Rights Discrimination Program (ECP): VA's liaison with the Department of Justice (DOJ) for addressing issues of discrimination in federal programs and activities, Title VI of the Civil Rights Act of 1964 and other similar statutes, such as Title IX of the Education Amendments of 1972, Age Discrimination Act of 1975, Section 504 of the Rehabilitation Act of 1973, and various Presidential Executive Orders.

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

Yes – the data collected is directly relevant and necessary to complete the specific purpose of the program.

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

Information is collected directly from Aggrieved Party or Complainant, Witnesses. Employees, or Veterans.

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

Aggrieved Party or Complainant and Witnesses receive a copy of the information and are responsible to correct the information.

Follow the format below when entering your risk assessment:
**Privacy Risk:**
1.Risk of people with no need to know accessing the information
2.Risk of people not relinquishing access privileges when they should
3.System operators could input the wrong information or process the request to the wrong stakeholder for action.

**Mitigation:**
1. Risk is manifested during the processing of complaints. Errors in the dissemination of information occur during the complaint process. To mitigate, monthly privacy messages are sent out to all ORMDI staff reviewing recent privacy events and providing suggestions to reduce the incidence of these events.
2. If there is no activity in an account for 6 months, the account is automatically terminated. Accounts are removed based on ORMDI's updated listing of HR managers.
3. Design team has developed script and coding to use the Global address listing (GAL) to streamline processing and minimize data input errors. All employees have access to ensure their information is correct in the GAL. The employee would need to request a help desk ticket to make changes

## 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.*

EEO and RAMS are internal systems to be used enterprise wide across the Department of Veteran Affairs three administrations. Employees make requests via government email, government phone lines, verbally to their supervisor or through a representative.

EEO: The records will include information collected on the EEO complaint form (4939) and all witness testimony, legal decisions, notes, and information needed to complete the process of a determination.
INTERNAL: This information is included in the investigative file and is used for adjudication purposes in the EEO process if the complainant so chooses.

RAMS: The records will include information from all VA 0857 forms and additional medical documentation provided by the Health Care Provider.
INTERNAL: Complete Reasonable Accommodation requests. The form allows a determination of eligibility and needs information concerning the nature of the disability and the need for accommodation, to include appropriate medical documentation when the disability and/or need for accommodation is not obvious.

HPP: The records will include information collected on VA 10221a and all witness testimony, legal decisions, notes, and information needed to complete the process of a determination.
INTERNAL: This information is included in the investigative file and is used for adjudication purposes in the EEO process if the complainant so chooses.

ECP: The records will include information collected on VA 10-0381 and all witness testimony, legal decisions, notes, and information needed to complete the process of a determination.
INTERNAL: This information is included in the investigative file and is used for adjudication purposes in the Civil Rights Discrimination Complaint process if the alleger so chooses.

MSD: The records include what is needed to manage and execute the budget, human resources, contracts, and facility/space requirements for ORMDI.
INTERNAL: Human Resource information is obtained and stored internally as needed. Human resources, contract, budget, and facilities information is included in HR files.

E2 SYSTEM EXTERNAL:
All records collected are available for the uses listed below:

a. To disclose pertinent information to the appropriate federal, state, or local agency responsible for investigating, prosecuting, enforcing, or implementing a statute, rule, regulation, or order, where the disclosing agency becomes aware of an indication of a violation or potential violation of civil or criminal law or regulation.

b. To disclose information to another federal agency, to a court, or to a party in litigation before a court or in an administrative proceeding being conducted by a federal agency when the government is a party to the judicial or administrative proceeding.

c. To provide information to a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of that individual.

d. To disclose to an authorized appeal grievance examiner, formal complaints examiner, administrative judge, equal employment opportunity investigator, arbitrator or other duly

authorized official engaged in investigation or settlement of a grievance, complaint or appeal filed by an employee.
e. To disclose, in response to a request for discovery or for appearance of a witness, information that is relevant to the subject matter involved in a pending judicial or administrative proceeding.
f. To disclose information to officials of state or local bar associations or disciplinary boards or committees when they are investigating complaints against attorneys in connection with their representation of a party before the Equal Employment Opportunity Commission (EEOC).
g. To disclose to a Federal agency in the executive, legislative, or judicial branch of government, in response to its request information in connection with the hiring of an employee, the issuance of a security clearance, the conducting of a security or suitability investigation of an individual, the classifying of jobs, or the lawful statutory, administrative, or investigative purpose of the agency to the extent that the information is relevant and necessary to the requesting agency's decision.
h. To disclose information to employees of contractors engaged by an agency to carry out the agency's responsibilities under 29 CFR part 1614.
I. To disclose information to potential witnesses as appropriate and necessary to perform the agency's functions under 29 CFR part 1614.

**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.*

All system data is available for reporting to help understand performance and support reporting requests:

- System record resolution rates
- Processing time
- Savings reports
- Offer rates
- Case closure/performance metrics
- Settlement Report metrics
- Basis of Complaints
- EEO Complaint Data by type, formal/informal, location, and by individuals
- Participation rates, and other EEOE data
- Congressional, Presidential, and EEOC Reporting

*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.*

EEO: Upwards of 5,000 complaints per year are filed and entered into EEOE. Data from these complaints are organized and sorted for management purposes (e.g., number of racial discrimination complaints filed at X facility). Also, the Senior Managers Report, a Congressionally mandated report summarizing findings of discrimination against VA's senior managers, is compiled and submitted on a quarterly and annual basis. The system will use Microsoft Power BI (Business Intelligence) and Excel to access general information and create reports (tallies only) on timeliness, trend analysis, costs, and over all legal compliance.

RAMS: Each Reasonable Accommodation case is stand alone and the PHI, PII associate with each case will not be cross referenced by any program. The RAMS system will use Microsoft Power BI (Business Intelligence) and Excel to access general information and create reports (tallies only) on timeliness, trend analysis, costs, and over all legal compliance.

HPP: Currently 1,500 complaints per year are filed and entered into EEOE. This is anticipated to double within the next year. Data from these complaints are organized and sorted for management purposes (e.g., number of sexual discrimination complaints filed at X facility). Also, the Senior Managers Report, a Congressionally mandated report summarizing findings of discrimination against VA's senior managers, is compiled and submitted on a quarterly and annual basis. The system will use Microsoft Power BI (Business Intelligence) and Excel to access general information and create reports (tallies only) on timeliness, trend analysis, costs, and over all legal compliance.

ECP: Currently approximately 200 complaints per year are filed and entered into EEOE. This is anticipated to triple within the next year. Data from these complaints are organized and sorted for management purposes (e.g., number of Civil Rights Discrimination complaints filed at X facility). The system will use Microsoft Power BI (Business Intelligence) and Excel to access general information and create reports (tallies only) on timeliness, trend analysis, costs, and over all legal compliance.

MSD: MSD currently has approximately 450 current resources and is anticipated to grow to 1000 over the next year. HR, contracting, facilities, and budget data is organized and sorted for management purposes (e.g., manpower dashboard report). The system will use Microsoft Power BI (Business Intelligence) and Excel to access general information and create reports (tallies only) on schedule, trend analysis, costs, and over all legal compliance.

### 2.3 How is the information in the system secured?

*These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.*

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

Data in Transit and at Rest is encrypted with FIPS 140-3 Compliant Encryption
EEOE is hosted on Microsoft Dynamics 365 CRM, a SaaS cloud model which is housed on the FedRAMP approved FISMA High Government Commercial Cloud VAEC environment.

*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 PII is limited by the E2 application to only those data items deemed necessary to process the EEO complaints, reasonable accommodation requests, Harassment Prevention complaints, External Civil Rights Discrimination Complaints, or perform MSD activities. This data is identified above, by policy and law. System documentation includes detailed system design and user guides that specify those areas of the system that contain PII and PHI, as well as how it is to be access and used by the EEO, RAMS, HPP, ECP, and MSD system users. Additionally, 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 users, verified by a Supervisor, approved by a Manager, and added by a System Administrator within each application.

The E2 application implements auditing which tracks user access to the system and all data accessed. The information is mapped in the CRM audit record by file identifying code. All three administrations VHA, VBA, and NCA ensure that the practices stated in the PIA are reinforced and VA employees are required 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) annually. All 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.

**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?*

All access to E2 is granted on the Least Privilege and Need to Know basis and is determined by is job, discipline, or business need. For EEO VA EEO Program Managers and ORMDI field office staff have access to data specific to their regions to conduct their work. RAMS and HPP have the same regional or area access limitations. ORMDI's Office of Policy and Compliance and senior leadership staff have access to required EEOE modules to perform their work. Within each module a role has been setup to allow Administration and Staff Office personnel the ability to generate reports on certain data fields in the system. All non-ORMDI employees or staff who have access to the system submit a signed or approved VA Form 9957 (Access Form).

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

Access Forms are used to request the role required to perform the job responsibilities. Access Forms with detailed instructions are provided to users, forms are filled out by users and sent to direct Supervisors, signed for approval by Supervisors and sent to Managers, signed for approval by Managers/Division Leaders, then sent to the System Administrator. System Administrators review the form for completeness and then provide access. Supervisors then work with the new user to ensure the correct role is assigned.

*2.4c Does access require manager approval?*

Yes – see 2.4b

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

When users log into E2, the access is tracked and recorded in audit logs. Any changes made to the system are tracked and recorded. Basically, the E2 application has implemented auditing which tracks user access to the system and all data entered or accessed. For examples, each time a user accesses an EEO casefile, it is captured in logs.

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

Access to PII is limited by in E2 to only those data items deemed necessary to process the reasonable accommodation or EEO requests and MSD Human Resource activities. This data is identified above, by policy and law. System documentation includes detailed system design and user guides that specify those areas of the system that contain PII and PHI, as well as how it is to be used by the RAMS and EEO. Additionally, user roles are implemented to restrict user's access to only the specific information required to perform their job function. Roles within each application of the system, are determined and requested by users, approved by Supervisors, and verified by Managers with a final verification and addition a system administrator.

The E2 system has implemented auditing which tracks user access to the system and all data accessed. The information is mapped in the CRM audit record by file identifying code. All three administrations VHA, VBA, and NCA ensure that the practices stated in the PIA are reinforced and VA employees will be required 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). All 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.

Privacy and HIPAA Training
This course is available in two formats, web-based and text. Annually, all employees who have access to PHI and/or VHA computer systems during each fiscal year must complete either of these course versions to meet the mandatory training requirement. This training provides guidance on privacy practices for the use and disclosure of protected health information (PHI) and Veteran rights regarding VHA data. It contains policy implementation content as described in VHA Handbook 1605.1. There is a substitute for VA 10203: VA 10204, Print Version.

VA Privacy and Information Security Awareness and Rules of Behavior
VA Privacy and Information Security Awareness and Rules of Behavior (ROB) provides information security and privacy training important to everyone who uses VA information systems or VA sensitive information.
After completing this course, you will be able to identify the types of information that must be carefully handled to protect privacy; recognize the required information security practices, legal requirements, and consequences and penalties for non-compliance; and explain how to report incidents.
You must electronically acknowledge and accept the ROB to receive credit for course completion. This course fulfills the fiscal year 2018 MANDATORY annual awareness training required for all VA employees. Certificates of completion for the course apply to the Information Security and Privacy Awareness requirements and to the ROB. This course was updated October 1, 2017.
Note:
*You should either take the online version of this course or coordinate with your supervisor and local TMS Administrator to get credit for attending an ISO-led presentation and signing the ROB. (TMSAdministrators can use item VA 832914 to record this training for learners who attend an ISO-led training. The ISO should ensure paper copies of signed ROB are retained for one year.)
Also see Section 8: Technical Access and Security.

## Section 3. Retention of Information

The following questions are intended to outline how long information will be retained after the initial collection.

**3.1 What information is retained?**

*Identify and list all information collected from question 1.1 that is **retained** by the system.*

*This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal*

All information listed in Section 1.1 is retained per the period determined by Record Management Schedules and OGC Hold/Feeze Lists.

**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.*

EEO: Per General Records Schedule 2.3: EEO discrimination complaint case files are destroy per the following:

Informal Process: Destroy 3 years after resolution of case but longer retention is authorized if required for business use: DAA-GRS-2018-0002-0012
Formal Process: Destroy 7 years after resolution of case but longer retention is authorized if required for business use: DAA-GRS-2018-0002-0013

Hard copy information filed in the official discrimination complaint file is retained in EEOE for at least seven years after the case is closed. An exception would be when the agency's Office of General Counsel (OGC) puts a litigation hold on a case file. In this instance, the information will be retained until OGC releases its litigation hold.

RAMS: Per General Records Schedule 2.3: Employee Relations Records are destroy when 3 years old but longer retention is authorized if required for business use: DAA-GRS-2022-0001-0001 and DAA-GRS-2022-0001-0002

HPP: Per General Records Schedule 2.3: Harassment complaint case files are destroy when 7 years old but longer retention is authorized if required for business use: DAA-GRS-2018-0002-0005

ECP: Per General Records Schedule 5.2 – Transitory and Intermediary Records Item 020. Destroy upon creation or update of the final record, or when no longer needed for business use, whichever is later: DAA-GRS-2022-0009-0002.

MSD: All information pertaining to the individual is retained as the individual is still assigned to the Department of Veterans Affairs. Once an employee departs the Department of Veteran Affairs, the case information will be maintained for three years IAW the following:

- Privacy Act of 1974
- 29 CFR 1611 - Privacy Act Regulations

- EEOC Order 150.003 - EEOC Privacy Act of 1974 (as amended)
- VA information security and privacy policies, including VA Handbook 6500 (Information Security Program).
- VA Handbook 5975.1
- General Records Schedule 2.3: Employee Relations Records: DAA-GRS-2022-0001-0001

ORMDI is currently in the process of deleting electronic files according to the records retention schedule.

**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.*
*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?*

Yes – Department of Veterans Affairs – Records Control Schedule 10-1, dated January 2021.

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

ORMDI follows Department of Veterans Affairs – Records Control Schedule 10-1, dated January 2021.

VA Handbook 5975.1, General Records Schedule (GRS) Code 20 –
DAA-GRS-2022-0001-0001
DAA-GRS-2022-0001-0002
DAA-GRS-2018-0002-0005
DAA-GRS-2018-0002-0012
DAA-GRS-2018-0002-0013
DAA-GRS-2022-0009-0002

https://www.archives.gov/files/records-mgmt/grs/grs02-3.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.*

It is VA policy that all Federal records contained on paper, electronic, or other medium are properly managed from record creation through final disposition, in accordance with Federal laws, the General Records Schedule and the Department of Veteran Affairs Record Control Schedule 10-1 dated January 2021. Further, Section 1 – Purpose of the VHA Records Control Schedule 10-1 states that "The Records Control Schedule (RCS) 10-1 provides Veterans Health Administration (VHA) records retention and disposition requirements for VHA Central Office, Program Offices, and field facilities and Section 4 – Disposition of Records states that "The RCS 10-1 contains retention and disposition requirements for VHA records authorized by NARA or assigned a GRS authority. Record disposition refers to the transfer of records to an approved records storage facility, transfer of permanent records to NARA, the destruction of records, or other appropriate actions to dispose of records. Unless retrieved; records transferred to a storage facility shall be dispositioned after expiration of their retention requirements."

Within the Department of Veterans Affairs – Records Control Schedule 10-1, dated January 2021. It provides a brief description of the records and states the retention period and disposition requirements. It also provides the NARA disposition authorities or the GRS authorities, whichever is appropriate for the records, in addition to program and service sections.

Upon expiration of the data retention period, records are destroyed in accordance with VA (Handbook 6500.1 Electronic Media Sanitization Policy) and NIST (SP800-88r1 Guidelines for Media Sanitization) record retention and Media Sanitization procedures. Media in the VA environment are sanitized following VA 6500.1 Guidelines. Media in the Microsoft CRM and government cloud are sanitized in accordance with NIST SP800-88r1 as audited by FedRAMP).

For each case handled by non-ORMDI personnel (i.e., Administration and Staff Office EEO managers), correspondence is received instructing them to redact non-essential PII from documents being submitted as part of the EEO case file. They have also been instructed in separate training.

ORMDI staff are trained to review all documents included in the case file for unnecessary PII and to redact it. As a second check, case managers review all files before finalizing them. Hard copy records that are held in Central Office are sent to VACO's Office of Administration's Records Manager Officer for shredding. Other district offices use VA-provided shredding services, or they contract with local shredders who provide a receipt for the shredding.

**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.*

ORMDI does not use PII for research, testing or training. Data that EEOE uses from Dynamics 365 CRM (e2) is not used for research, testing, or training. The data contained in Microsoft

Dynamics 365 remains the intellectual property of the system owner (VA). VA may use the data for purposes as necessary to fulfill its mission.

### 3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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

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

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

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

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

Follow the format below:

**Privacy Risk:**
**1.**The biggest risk is unauthorized access to the files.
2.There is a risk that information could be stored longer than necessary.

**Mitigation:**
1.Hard copy records are kept for no longer than is absolutely necessary, pursuant to the Federal records retention schedule. Additionally, all notes taken by counselors are destroyed after the file goes formal, and by investigators after the investigation report is completed. The risk, however, is not mitigated for electronic files because they are currently held indefinitely. Once an ORMDI staff person with access to EEOE leaves ORMDI, the Division Lead or Human Resources will enter a ticket into the Help Desk System that notifies the system administrator to terminate access. Furthermore, if there is no activity in a EEOE account for 6 months, the account is terminated. Access by EEO program managers (who are not ORMDI staff) who have access to EEO files in their particular geographic regions, is monitored. Their access will be terminated by lack of activity, if Form 9957 is not renewed, or by the expiration of their PIV card.
2.EEOE follows VA Handbook 5975.1, General Records Schedule (GRS) Code 20. Upon expiration, all retained data will be carefully disposed, as described 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.

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

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

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

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

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

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

*Data Shared with **Internal Organizations**:*

| ***List the Program Office or IT System information is shared/received with*** | ***List the purpose of the information being shared /received with the specified program office or IT system*** | ***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system*** | ***Describe the method of transmittal*** |
|---|---|---|---|
| Veterans Benefits Administration | New Case Alert<br><br>Benefits eligibility and issue resolution | • Employee name,<br>• First Name,<br>• Last Name.<br>• Address,<br>• Email Address.<br>• Phone Number,<br>• DOB,<br>• Race,<br>• Ethnicity,<br>• National Origin,<br>• Sex, | SFTP/Email notification sent from E2/EEO, HPP, ECP, or for RAMS for each new case.<br><br>Direct input is request by stakeholders who then go into the CRM cloud-based system (E2) to |

| *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* |
|---|---|---|---|
| | | • Age,<br>• Position,<br>• Facility,<br>• Facility address,<br>• Facility phone number,<br>• Date of Request,<br>• Information concerning, issue/claim,<br>• Specifics of the complaint (harassment, discrimination, etc.),<br>• Legal Agreements,<br>• Witness POC Information,<br>• Witness testimony,<br>• Health information if necessary (e.g., disability related) RAMS does collect data that is HIPPA protected,<br>• Any record relevant to the allegations,<br>• Recommendation for future harassment prevention or determinations/decisions,<br>• Human Resources,<br>• Employee Recruitment and Credit Card application and supporting documents,<br>• Facility/Administration Space Requirements | provide additional information (e.g., witness statements) |
| Veterans Health Administration | New Case Alert<br><br>Benefits eligibility and issue resolution | • Employee name,<br>• First Name,<br>• Last Name.<br>• Address,<br>• Email Address.<br>• Phone Number,<br>• DOB,<br>• Race,<br>• Ethnicity,<br>• National Origin,<br>• Sex, | SFTP/Email notification sent from E2/EEO, HPP, ECP or for RAMS for each new case.<br><br>Direct input by stakeholders into the CRM cloud-based system |

| *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* |
|---|---|---|---|
| | | • Age,<br>• Position,<br>• Facility,<br>• Facility address,<br>• Facility phone number,<br>• Date of Request,<br>• Information concerning, issue/claim,<br>• Specifics of the complaint (harassment, discrimination, etc.),<br>• Legal Agreements,<br>• Witness POC Information,<br>• Witness testimony,<br>• Health information if necessary (e.g., disability related) RAMS does collect data that is HIPPA protected,<br>• Any record relevant to the allegations,<br>• Recommendation for future harassment prevention or determinations/decisions,<br>• Human Resources,<br>• Employee Recruitment and Credit Card application and supporting documents,<br>• Facility/Administration Space Requirements | |
| The Department of Veterans Affairs Central Office (VACO) | New Case Alert<br><br>Benefits eligibility and issue resolution | • Employee name,<br>• First Name,<br>• Last Name.<br>• Address,<br>• Email Address.<br>• Phone Number,<br>• DOB,<br>• Race,<br>• Ethnicity,<br>• National Origin,<br>• Sex, | SFTP/Email notification sent from E2/EEO, HPP, ECP, or for RAMS for each new case.<br><br>Direct input by stakeholders into the CRM cloud-based system |

| *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* |
|---|---|---|---|
| | | • Age,<br>• Position,<br>• Facility,<br>• Facility address,<br>• Facility phone number,<br>• Date of Request,<br>• Information concerning, issue/claim,<br>• Specifics of the complaint (harassment, discrimination, etc.),<br>• Legal Agreements,<br>• Witness POC Information,<br>• Witness testimony,<br>• Health information if necessary (e.g., disability related) RAMS does collect data that is HIPPA protected,<br>• Any record relevant to the allegations,<br>• Recommendation for future harassment prevention or determinations/decisions,<br>• Human Resources,<br>• Employee Recruitment and Credit Card application and supporting documents,<br>• Facility/Administration Space Requirements | |
| National Cemetery Administration | New Case Alert<br><br>Benefits eligibility and issue resolution | • Employee name,<br>• First Name,<br>• Last Name.<br>• Address,<br>• Email Address.<br>• Phone Number,<br>• DOB,<br>• Race,<br>• Ethnicity,<br>• National Origin,<br>• Sex, | SFTP/Email notification sent from E2/EEO, HPP, ECP, or for RAMS for each new case.<br><br>Direct input by stakeholders into the CRM cloud-based system |

| *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* |
|---|---|---|---|
| | | • Age,<br>• Position,<br>• Facility,<br>• Facility address,<br>• Facility phone number,<br>• Date of Request,<br>• Information concerning, issue/claim,<br>• Specifics of the complaint (harassment, discrimination, etc.),<br>• Legal Agreements,<br>• Witness POC Information,<br>• Witness testimony,<br>• Health information if necessary (e.g., disability related) RAMS does collect data that is HIPPA protected,<br>• Any record relevant to the allegations,<br>• Recommendation for future harassment prevention or determinations/decisions,<br>• Human Resources,<br>• Employee Recruitment and Credit Card application and supporting documents,<br>• Facility/Administration Space Requirements | |
| Office of Information Technology | New Case Alert<br><br>Benefits eligibility and issue resolution | • Employee name,<br>• First Name,<br>• Last Name.<br>• Address,<br>• Email Address.<br>• Phone Number,<br>• DOB,<br>• Race,<br>• Ethnicity,<br>• National Origin,<br>• Sex, | SFTP/Email notification sent from E2/EEO, HPP, ECP, or for RAMS for each new case.<br><br>Direct input by stakeholders into the CRM cloud-based system |

| *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* |
|---|---|---|---|
| | | • Age,<br>• Position,<br>• Facility,<br>• Facility address,<br>• Facility phone number,<br>• Date of Request,<br>• Information concerning, issue/claim,<br>• Specifics of the complaint (harassment, discrimination, etc.),<br>• Legal Agreements,<br>• Witness POC Information,<br>• Witness testimony,<br>• Health information if necessary (e.g., disability related) RAMS does collect data that is HIPPA protected,<br>• Any record relevant to the allegations,<br>• Recommendation for future harassment prevention or determinations/decisions,<br>• Human Resources,<br>• Employee Recruitment and Credit Card application and supporting documents,<br>• Facility/Administration Space Requirements | |
| VA Office of General Counsel | Case Information | • Employee name,<br>• First Name,<br>• Last Name.<br>• Address,<br>• Email Address.<br>• Phone Number,<br>• DOB,<br>• Race,<br>• Ethnicity,<br>• National Origin,<br>• Sex, | SFTP/Email notification sent from EEO |

| *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* |
|---|---|---|---|
| | | • Age,<br>• Position,<br>• Facility,<br>• Facility address,<br>• Facility phone number,<br>• Date of Request,<br>• Information concerning issue/claim,<br>• Specifics of the complaint (harassment, discrimination, etc.),<br>• Legal Agreements,<br>• Witness POC information<br>• Witness testimony<br>• Health information if necessary (e.g., disability related),<br>• Any record relevant to the allegations,<br>• Recommendation for future harassment prevention or determinations/decisions. | |

**4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure**

*Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).*

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

Follow the format below:

**Privacy Risk:**

1.Inadvertent disclosure.
2.Wrongful Access; and,
3.Information system breakdown/intrusion/penetration

**Mitigation:**

1.Awareness training and monthly privacy updates/reminders from the ORMDI privacy officer
2.Access controls - The type of access is determined and based on job, discipline or business need. Individuals' access to casefiles is captured in logs. Password refresh is forced 90 days, all non ORMDI employees or staff must submit signed or approved VA form 9957.
3.ORMDI operates redundant systems for failover or disaster recovery/COOP.

## Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

*Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.*
*This question is related to privacy control UL-2, Information Sharing 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*** | ***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*** | ***List the method of transmission and the measures in place to secure data*** |
|---|---|---|---|---|

| | ***with the specified program office or IT system*** | | ***external sharing (can be more than one)*** | |
|---|---|---|---|---|
| Equal Employment Opportunity Office (EEOC) | Case Information for hearings and resolution | • Employee name<br>• First Name,<br>• Last Name.<br>• Address,<br>• Email Address.<br>• Phone Number,<br>• DOB,<br>• Race,<br>• Ethnicity,<br>• National Origin,<br>• Sex,<br>• Age,<br>• Position,<br>• Facility,<br>• Facility address,<br>• Facility phone number,<br>• Date of Request,<br>• Information concerning issue/claim,<br>• Specifics of the complaint (harassment, discrimination, etc.),<br>• Legal Agreements,<br>• Witness testimony,<br>• Any record relevant to the allegations. | Routine use<br><br>SORN 203VA08,<br><br>EEOC/GOVT - 1 – Equal Employment Opportunity in the Federal Government Complaint and Appeals Records | Encrypted Email Notification |

**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:**

1. Emails are intercepted.
2. An email is sent to the wrong party

**Mitigation:**

1. Emails are encrypted so they cannot be opened by the wrong party.

## 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.*

In regard to medical information, VA provides a Notice of Privacy Practice which details how medical information of Veterans, other beneficiaries who receive health care benefits from VHA, and non-Veteran patients who receive benefits from the VHA.

Additional notice is provided by the system's SORN 203VA08.

A third form of notice is provided by this Privacy Impact Assessment, which is available online as required by the eGovernment Act of 2002, Pub.L. 107–347§208(b)(1)(B)(iii).

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

Notice of Privacy Practices IB 10-163 – see Attachment #1

*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.*

When an aggrieved party (AP) contacts ORMDI with a possible discrimination complaint, ORMDI counselors reach out verbally to the AP to collect initial contact information and what the complaint is about. The counselor then conducts an initial interview verbally with the AP. No evidence is collected at this stage. The HIPAA Notice (Attachment 2) is sent to the AP during this stage. The HIPAA Notice clearly indicates that ORMDI will be collecting personally identifiable information and that it can only be disclosed upon the written consent of the individual. If and when the aggrieved party is ready to file a formal complaint, they are provided with VA Form 4939 to fill out which provides contact information and details the complaint(s) with which the AP wants to proceed. VA Form 4939 includes a Privacy Act Statement detailing how the information will be used and how it may be disclosed.

When the complaint goes formal, an investigation ensues, and evidence is collected. The following guidance is provided to the complainant regarding what evidence is needed: EEOC Guidelines for What it Takes to Prove Discrimination based on Sex, Race, National Origin, Color, Religion, Age, and Reprisal (Attachment 3); and EEOC Guidelines for What it Takes to Prove Discrimination based on Disability (Attachment 4).

Notice of Privacy Practices IB 10-163: VA Boston Health Care | Veterans Affairs

**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.*

EEO: In the EEO complaint process, we provide a "Notice of Rights and Responsibilities" (Attachment 5, pg. 2) to the AP in which a paragraph states: "You have the responsibility to cooperate with VA during the processing of your complaint. You must keep the VA informed of your current address; you must claim any mail sent to you, and you must cooperate with any individual assigned to the complaint. If you eventually file an appeal to the EEOC about the complaint, you must serve copies of the appeal papers on VA." APs can decline to provide information. ORMDI will process the claim, but without the necessary information, the claim will not proceed very far in the process.

RAMS: The RAMS portion of EEOE system is based by name as listed in the GAL. SSNs are not collected. If employees refuse to provide the requested medical information, their accommodation request will be administratively closed as outlined by VA Handbook 5975.1 Processing Requests for Reasonable Accommodation from Employees and Applicants with Disabilities.

HPP: The HPP portion of EEOE system is based by name as listed in the GAL or by a case already opened in EEO. SSNs are not collected. Allegers can decline to provide information. ORMDI will process the complaint, but without the necessary information, the case will not proceed very far in the process.

ECP: Form 10-0381 has a privacy notice at the top of the form: "The information requested on this form is solicited under authority of Title 38, Code of Federal Regulations, Chapter 1, Parts 15 and 18, and is used by patients and other VHA customers to file a formal complaint for alleged violations of their civil rights pertaining to race, color, sex, national origin, age, disability, or reprisal." Allegers can decline to provide information. ORMDI will process the claim, but without the necessary information, the claim will not proceed very far in the process.

MSD: The individual can refuse to provide the requested HR information; their employment can be impacted.

**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.*

EEO: In the Notice of Rights and Responsibilities (Attachment 5, pg. 2) provided to the AP, the AP is required to "limit any formal EEO complaint you may file to those matters discussed with ORMDI, or to like or related matters (that is, matters which are directly related to those matters or which are unmistakably derived from those matters). Additionally, if you wish to amend a previously filed complaint, only matters that are like or related to the claim(s) in the pending complaint may be added. To protect your rights, discuss all claims with ORMDI before you file a formal complaint."

RAMS: N/A - Individuals do not have rights to consent to particular uses of information.

**6.4 <u>PRIVACY IMPACT ASSESSMENT: Notice</u>**

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

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

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

*<u>Principle of Use Limitation:</u> Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?*

*This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use.*

Follow the format below:

**Privacy Risk:**
**1.**Risk of an ORMDI employee using complainant information for purposes other than for processing the complaint.
2.Insufficient notice is provided to the Veteran.

**Mitigation:**
1. ORMDI employees sign the VA National Rules of Behavior.
2. Notice is given by the SORN #203VA08 in Section 6.1.

## Section 7. Access, Redress, and Correction

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

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

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

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

Individuals can request information from EEO, ECP, and HPP case files through the Freedom of Information Act. ORMDI's FOIA Officer can be reached at: ORMDIFOIA@va.gov. Requests can also be made through the Privacy Act; however, the entire case file is exempt from the access provisions of the Privacy Act, per the SORN 67 FR 49338 "EEOC/GOVT-1."

Records are maintained at VA field facilities and the Office of Resolution Management, Diversity and Inclusion (ORMDI), Department of Veterans Affairs, 810 Vermont Avenue NW, Washington, DC 20420. For addresses of VA field facilities, see *www.va.gov/find-locations.* Attachment 6 "EEO and HPP Fact Sheet 6 07 2023" is distributed to assist users in filing a FOIA request for EEO and HPP records.

Privacy Officer, Office of Resolution Management, Diversity and Inclusion (ORMDI), Department of Veterans Affairs, 810 Vermont Avenue NW, Washington, DC 20420, email: ormdiprivacy@va.gov.

An individual who seeks access to or wishes to contest records maintained under his or her name in this system must submit a written request to the Privacy Officer of the VA facility where the underlying incident or issue occurred.

Individuals seeking information concerning the existence and content of a record pertaining to themselves must submit a written request to or apply in person before the Privacy Officer of the VA facility where the underlying incident or issue occurred. Written requests should be signed and contain the individual's full name, mailing address, email address, telephone number, and the case number or case title.

*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).*

Requests can also be made through the Privacy Act; however, the entire case file is exempt from the access provisions of the Privacy Act, per the SORN 67 FR 49338 "EEOC/GOVT-1."

HPP has submitted for an exemption: Notice (WP 2023-010 Exemption of Harassment Prevention Program Records – VIEWS 09690147) until the comment period closes on Tuesday, August 8, 2023.

*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.*

Virtually all information gathered in an EEO complaint emanates from: (a) the aggrieved party - all information provided by the aggrieved party is voluntary; (b) witness testimony; and, (c) official documentation gathered by the local facility Human Resources manager that is verified as being true and accurate.

At the end of the formal stage of the complaint process, the complainant receives a copy of the complete investigative file – a compilation of all evidence, testimony, and correspondence during the counselling and investigative stages of the process.

Individuals can request information from EEO case files through the Freedom of Information Act. ORMDI's FOIA Officer can be reached at: ORMFOIA@va.gov. Requests can also be made through the Privacy Act; however, the entire case file is exempt from the access provisions of the Privacy Act, per the SORN 67 FR 49338 "EEOC/GOVT-1."

For RAMS the individual can request their Reasonable Accommodation File by contacting their RAC.

For MSD the individual can request their HR file by contracting their HR representative.

**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.*

Ongoing EEO case files are updated as information is received, either from the complainant or from requests to the local HR office (the type of information provided depends upon the allegation(s) that have been made). ORMDI maintains district offices around the country to process EEO complaints on a regional basis:
North Atlantic District One – Lyons, NJ (908) 604-5349
North Atlantic District Two – Washington, DC (202) 632-9599
Midwest District – Hines, IL (708) 202-7072
Southeast District – St. Petersburg, FL (727) 540-3971
Continental District – Houston, TX (713) 794-7756
Pacific District – Los Angeles, CA (713) 794-7756

For RAMS, the information is collected from individuals when they contact the RAC. If the individual discovers that incorrect information was provided during intake, they simply follow the same contact procedures as before, and state that the information they are now providing supersedes the information previously provided. The RAC would make appropriate changes to the system as requested and all entries are logged and tracked automatically be the system.

For MSD, HR information is collected for individuals when hired and from individuals and supervisors on an ongoing basis. Individuals can request a copy of their file. Budget and facility information is collected from government responsible parties.

**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.*

EEO/HPP/ECP: Witness testimony is taken verbally (and transcribed), or in writing. When transcribed, the testimony is given to the witness to review and verify and then sign. In the taking of testimony, witnesses are told there is no promise of confidentiality. It is up to the complainant to ensure that the information is complete and accurate, and to provide up-to-date contact information if it changes during the course of an investigation. If the contact information is incorrect, the complainant risks missing deadlines which are communicated in writing. By missing deadlines, the complainant risks closing the case prematurely.

For RAMS, this normally doesn't apply, since this information is pulled directly from the GAL. Unless the individual changes their information in the GAL or provides new medical documentation for requirements/needs, their information will not change.

**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.*

EEO: The complainant gets a copy of the complete investigative file at the completion of the investigation. If the complainant raises issues regarding accuracy or corrections, the complainant can request a hearing which opens up the process to discovery.

RAMS and MSD: The individual can request their information per the FOIA. VA Handbook 5975.1 Processing Requests for Reasonable Accommodation from Employees and Applicants with Disabilities.

HPP has submitted for an exemption: Notice (WP 2023-010 Exemption of Harassment Prevention Program Records – VIEWS 09690147) until the comment period closes on Tuesday, August 8, 2023.

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

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

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

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

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

Follow the format below:

**Privacy Risk:**

**1.**Redress for allegations against a responsible management official.

**2.**There is a risk that the information on file is incorrect and individuals are unaware of how to access, redress, or correct their information. EEO, RAMS, or MSD staff members may not adhere to information security requirements instituted by the VA OIT.

**Mitigation:**

1. EEO: If a complainant alleges discrimination against a supervisor (responsible management official-RMO), the RMO can only provide personal testimony against the allegations. They cannot see anyone else's testimony. If there is a finding of discrimination against the RMO, then the RMO can obtain pertinent witness testimony. If there is no finding of discrimination, all witness testimony will be withheld from the RMO. Access provisions of the Privacy Act are exempted, and FOIA protects the identities of witnesses.

**2.** EEO: The complainant gets a copy of the complete investigative file at the completion of the investigation. If the complainant raises issues regarding accuracy or corrections, the complainant can request a hearing which opens the process to discovery.

MSD and RAMS: Individuals are notified verbally as well as able to submit VA Form 10-5345a to access their information. They can also follow the steps in VA Handbook 1605.1 to amend their information. Both contractor and VA employees are required to take annual Privacy, HIPAA, and information security training. For further details, see Section 8: Technical Access and Security.

## 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.*

**End User Access:**
A request for application access form is filled out by the user and submitted to the Supervisor, once approved, next submitted to the Manager, then sent to the ORMDI Helpdesk, which is then forwarded to ORMDI System Administrator to validate the level or type of access to be granted. The process determines access on job, discipline or business need. Access to casefiles is captured in logs, and users submit signed or approved VA form 9957 when needed.

Specific user roles are defined for users on the EEO, RAMS and MSD applications system. Currently, user roles are defined by business leadership. The following steps are required before any user can use the system:

- Individuals must take and pass training on privacy, HIPAA, information security, and government ethics.
- Individuals must have a completed security investigation.
- Once training and the security investigation are complete, a request is submitted for access. Before access is granted; this request must be approved by the supervisor, the and the manager.
- The completed Access Request Form is verified by the System Administrator before providing access.

Access for End Users has various levels of permission from Read Only to partial to full access depending upon the need to know.

**Developer Access**
Developers of the EEOE system are VA contractors. For details on VA contractor access, see Section 8.2.
All individuals requesting developer access are required to complete all VA trainings (VA Privacy and Information Security Awareness and Rules of Behavior Training, Privacy and HIPAA Focused Training and Information Security for IT Specialists Training) and must be authorized by a Contractor Supervisor and the VA Project Manager. To ensure that this requirement is met, the designated Veterans Centered Experience (VCE) project Point of Contact (POC) must submit a signed Access Request From for an individual or a group. At minimum, the following information should be provided for each VA Project Team member requesting access to the EEOE environments: First Name, Last Name, Primary E-mail, Main Phone, Manager, Current on VA Training, VA Employee or Contractor, VA Active Directory Username, Environment, Access Permissions, and Contract End date.

**Tester Access**
All individuals requesting Tester access are required to complete all VA trainings (VA Privacy and Information Security Awareness and Rules of Behavior Training, Privacy- and HIPAA-Focused Training and Information Security for IT Specialists Training) and must be authorized by a Supervisor and Manager. To ensure that this requirement is met, the designated VA Project POC must submit a signed Access Request Form for an individual or a group. At minimum, the following information should be provided for each VA Project Team member requesting access to the EEOE Environments: First Name, Last Name, Primary E-mail, Main Phone, Manager, Current date of completion annual required VA Training, VA Employee or Contractor, VA Active Directory Username, Environment, Access Permissions, and Contract End date.

Personnel accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training which all personnel must complete via the VA's Talent Management System (TMS). The rules state the terms and conditions that apply to personnel who are provided access to, or use of, information, including VA sensitive information, or VA information systems, such as no expectation of privacy, and acceptance of monitoring of actions while accessing the system. 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 obtained

through electronic acknowledgment is tracked through the TMS system. All VA employees must complete annual Privacy and Security training. EEOE users agree to comply with all terms and conditions of the VA National Rules of Behavior (ROB) by signing a certificate of training at the end of the training session.

*8.1b Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?*

Users from other agencies are not provided access to EEOE as this is an internal system.

*8.1c Describe the different roles in general terms that have been created to provide access to the system. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.*

**End User Access:**
A request for application access form is filled out by the user and submitted to the Supervisor, once approved, next submitted to the Manager, then sent to the ORMDI Helpdesk, which is then forwarded to ORMDI System Administrator to validate the level or type of access to be granted. The process determines access on job, discipline or business need. Access to casefiles is captured in logs, and users submit signed or approved VA form 9957 when needed.

Specific user roles are defined for users on the EEO, RAMS and MSD applications system. Currently, user roles are defined by business leadership. The following steps are required before any user can use the system:

- Individuals must take and pass training on privacy, HIPAA, information security, and government ethics.
- Individuals must have a completed security investigation.
- Once training and the security investigation are complete, a request is submitted for access. Before access is granted; this request must be approved by the supervisor, the and the manager.
- The completed Access Request Form is verified by the System Administrator before providing access.

Access for End Users has various levels of permission from Read Only to partial to full access depending upon the need to know.

**Developer Access**
Developers of the EEOE system are VA contractors. For details on VA contractor access, see Section 8.2.
All individuals requesting developer access are required to complete all VA trainings (VA Privacy and Information Security Awareness and Rules of Behavior Training, Privacy and HIPAA Focused Training and Information Security for IT Specialists Training) and must be authorized by a Contractor Supervisor and the VA Project Manager. To ensure that this requirement is met, the designated Veterans Centered Experience (VCE) project Point of Contact (POC) must submit a signed Access Request From for an individual or a group. At minimum, the following information should be provided for each VA Project Team member requesting access

to the EEOE environments: First Name, Last Name, Primary E-mail, Main Phone, Manager, Current on VA Training, VA Employee or Contractor, VA Active Directory Username, Environment, Access Permissions, and Contract End date.

**Tester Access**
All individuals requesting Tester access are required to complete all VA trainings (VA Privacy and Information Security Awareness and Rules of Behavior Training, Privacy- and HIPAA-Focused Training and Information Security for IT Specialists Training) and must be authorized by a Supervisor and Manager. To ensure that this requirement is met, the designated VA Project POC must submit a signed Access Request Form for an individual or a group. At minimum, the following information should be provided for each VA Project Team member requesting access to the EEOE Environments: First Name, Last Name, Primary E-mail, Main Phone, Manager, Current date of completion annual required VA Training, VA Employee or Contractor, VA Active Directory Username, Environment, Access Permissions, and Contract End date.

Personnel accessing information systems must read and acknowledge their receipt and acceptance of the VA National Rules of Behavior (ROB) or VA Contractor's ROB prior to gaining access to any VA information system or sensitive information. The rules are included as part of the security awareness training which all personnel must complete via the VA's Talent Management System (TMS). The rules state the terms and conditions that apply to personnel who are provided access to, or use of, information, including VA sensitive information, or VA information systems, such as no expectation of privacy, and acceptance of monitoring of actions while accessing the system. 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 obtained through electronic acknowledgment is tracked through the TMS system. All VA employees must complete annual Privacy and Security training. EEOE users agree to comply with all terms and conditions of the VA National Rules of Behavior (ROB) by signing a certificate of training at the end of the training session.

**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.*

Contracts for EEOE-related contractors are renewed annually. Contracts include OIT contract language, including security clauses and requirements for Information Security Officers, Contracting Officers, and others.

All VA contractors that have access to the pre-production environments for development purposes sign Non-Disclosure Agreements (NDAs). Contractors will also have access to the live production system for maintenance and sustainment activities. The following steps are required before contractors can gain access to the system:

- Contractors must take and pass training on privacy, HIPAA, information security, and government ethics.
- Contractors must have a completed background investigation.
- Contractors accessing the EEOE system must complete relevant EPAS Training
- Once training and the background investigation are complete, an EPAS request form and a EEOE system access request form are submitted for access.
- Access Request Forms must be approved by the Contractors immediate supervisor and Government Manager.
- The EEOE System Administrator will only provide EEOE access upon full verification of the EEOE Access Request Form.
- The OIT System Administrator will only provide EEOE environment access upon full verification of the EPAS access request.

**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.*

Users of EEOE are required to take the annual Privacy Awareness training and to sign the VA Rules of Behavior. Personnel who will be accessing information systems must read and acknowledge their receipt and acceptance of the VA 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 EEOE user's initial acceptance of the Rules, the user must re-affirm their acceptance annually as part of the security awareness training. Acceptance obtained through electronic acknowledgment is tracked through the TMS system. All VA employees must complete annual Privacy and Security training. EEOE 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.

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

Yes

*8.4a If Yes, provide:*

1. *The Security Plan Status:* Approved
2. *The System Security Plan Status Date:* 10 Aug 2022
3. *The Authorization Status:* Authority to Operate
4. *The Authorization Date:* 1 Oct 2022
5. *The Authorization Termination Date:* 30 Sep 2023

6. *The Risk Review Completion Date:* 3 May 2021
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.***

## 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)"*

EEOE is hosted on Microsoft Dynamics 365 CRM, a SaaS cloud model which is housed on the FedRAMP approved FISMA High Microsoft Government Commercial Cloud environment.

**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.*

N/A

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

N/A

**9.4**

*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.*

N/A

**9.5 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.*

N/A

**9.6 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).*

N/A

## 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 provided in this Privacy Impact Assessment is true and accurate.**

ZULEMA BOLIVAR

Digitally signed by ZULEMA BOLIVAR
Date: 2023.10.11 13:32:57 -04'00'

**Privacy Officer, Zulema Bolivar**

LaToya N. Butler-Cleveland 204980

Digitally signed by LaToya N. Butler-Cleveland 204980
Date: 2023.10.11 09:21:44 -04'00'

**Information Systems Security Officer, LaToya Butler-Cleveland**

GLENN THOMAS

Digitally signed by GLENN THOMAS
Date: 2023.10.10 14:34:03 -04'00'

**Information Systems Owner, Glenn Thomas**

## 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).

**Please see attachments for Notices.**

The System of Record (SORN) 203VA08 – Department of Veteran Affairs (VA), Office of Resolution Management, Diversity and Inclusion (ORMDI)

NOPP IB 10-163

## 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