



Privacy Impact Assessment for the VA IT System called:

Medallia GovCloud -E  
VA Corporate  
Veterans Experience Office (VEO)  
eMASS ID 2254

Date PIA submitted for review:

5/21/2024

System Contacts:

	Name	E-mail	Phone Number
Privacy Officer	Julie Drake	Julie.drake@va.gov oitprivacy@va.gov	202-632-8431
Information System Security Officer (ISSO)	Roland Parten	roland.parten@va.gov	205-534-6179
Information System Owner	Henna Grover	henna.grover@va.gov	412-216-4566

## Abstract

*The abstract provides the simplest explanation for “what does the system do?”.*

Medallia GovCloud-E is an experience management Software as a Service (SaaS) product which contains data applicable to all administrations in the VA. This system provides users with a suite of tools for capturing and analyzing structured and unstructured feedback, which may be invited/solicited or anonymous/unsolicited. It captures customer feedback/responses and customer and employee experience information across email, text (SMS), web, social, mobile, and contact center channels, and analyzes it in real-time.

## 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. What is the IT system name and the name of the program office that owns the IT system?*

Medallia GovCloud -E SaaS system that falls under the purview of Veterans Experience Office.

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

To meet operational goals and become the federal leader in Customer Experience (CX), OI&T has a requirement for the Medallia Enterprise Customer Experience Suite Software-as-a-Service (SaaS) tool. Medallia SaaS allows VA to continue to collect CX and Employee Experience (EX) data. Centralizing the capture and analysis of CX and EX data allows VA to make better strategic decisions on impactful resourcing, ultimately improving Trust in VA. This acquisition allows VA to meet 38 CFR 0.603 Customer Experience Principles and VA Directive 0010 VA Customer Experience, as well as OMB Circular No. A-11, Section 280 Managing Customer Experience, and Improving Service Delivery. Medallia has several features that VA requires including the ability to capture experience feedback on calls, which VA has implemented in all enterprise contact centers using a variety of call center products. Medallia is Health Insurance Portability and Accountability Act of 1996 (HIPAA) compliant and is a Hospital Consumer Assessment of Healthcare Providers and Systems (HCAHPS) approved vendor. Medallia also offers packaged integrations to ease connecting with platforms such as Salesforce and ServiceNow, as well as using the RESTful API and custom API development. Medallia provides Sentiment Analysis via Athena AI and allows custom development functionality to tailor sentiment analysis. The mission of VEO is to enable VA to be the leading customer service organization in government and this SaaS product provides VA with capabilities to serve the varied needs of administrations and program offices in capturing and analyzing experience feedback to ultimately make decisions on resourcing that impacts how likely Veterans, their families, caregivers, and survivors are to Choose VA. This is an Enterprise request for the VA as a whole to utilize this system.

C. *Who is the owner or control of the IT system or project?*

Medallia GovCloud -E is SaaS system that is VA controlled/non-VA owned and operated by Veterans Experience Office (VEO).

2. *Information Collection and Sharing*

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

The typical client or affected individual may vary based on the survey/feedback being conducted. It is approximately 20,000,000 survey responses.

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

Medallia GovCloud -E is a Software as a Service (SaaS) product that captures the customer feedback/responses and customer experience information across email, text (SMS), web, social, mobile, and contact center channels, and analyzes it in real-time. VSignals gathers data via email-based anonymous surveys, text based anonymous surveys, social emails, phone calls, and web scraping. VSignals processes the text of the data into specific topics and performs sentiment analysis, then presents the information in an easy-to-use user interface. The interface allows users to review the feedback data and design new anonymous surveys around an organization, product, or service. ESignals gathers data via email-based anonymous surveys and processes the text of the data into specific topics and performs sentiment analysis, then presents the information in an easy-to-use user interface. VRCN Lab gathers information shared into the software for innovation and idea sharing.

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

- Veteran Signals (VSignals) – gathers customer feedback data via email-based surveys, text-based surveys, web/app surveys, social emails, phone calls and web scraping. VSignals processes the text of the data into specific topics and performs sentiment analysis, then presents the information in an easy-to-use user interface. VSignals is deployed in the FedRAMP High rated AWS GovCloud. Primary hosting location is the AWS West region with backup being the AWS East region.
- Employee Signals (ESignals) – gathers employee feedback data via email-based surveys. ESignals processes feedback data into specific topics and performs sentiment analysis, then presents the information in an easy-to-use user interface. ESignals is deployed in the FedRAMP High rated AWS GovCloud. Primary hosting location is the AWS West region with backup being the AWS East region.
- Veterans Community Resource Network (VCRN) Lab (Crowdicity) – is used to crowdsource ideas and innovations from trusted community partners.

G. *Is 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?*

The primary hosting location for Medallia GovCloud -E is AWS GovCloud. Backup region is the different availability zone in the same region as supported by AWS GovCloud.

3. *Legal Authority and SORN*

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

*Legal Authorities*

- Title 38, United States Code, Sections 501(a), 1705, 1710, 1722, and 5317

- 5 U.S.C. 552, "Freedom of Information Act," c. 1967
- 5 U.S.C. 552a, "Privacy Act," c. 1974
- OMB Circular A-130, Appendix III, "Security of Federal Automated Information Systems"
- Information Technology Management Reform Act of 1996 (also known as the Clinger-Cohen Act)
- Federal Information Security Management Act (FISMA) of 2002
- OMB M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002"
- VA Directive and Handbook 6502, Privacy Program
- Executive Order 14058 on Transforming the Customer Experience and Federal Service Deliver to Rebuild Trust in Government
- The President's Management Agenda, Priority 2
- 21<sup>st</sup> Century Integrated Digital Experience Act (IDEA)
- OMB Circular A-11; Section 280
- Executive Order 9397, Numbering System for Federal Accounts Relating to the Individual Persons
- National Archives and Records Administration (NARA) (44 U.S.C Chapter 21) c 2102 (a) (Pub. L. 98-497, § 103) (a)
- Records Management by the Archivist of the United States (44 U.S.C. Chapter 29) c 2901 .2 "Record Management; c 2605 (a) "Selective Retention of records; security measures."
- Contractual obligations of Master Agreement, Section 8 – Survey and Questionnaires, where the surveys are voluntary, and responses are confidential and respondent anonymity protected. In addition, other survey governance process that meets the Organizational Assessment Committee (OAC) criteria would also be reviewed with this governance board. Requirements included dissemination to greater than 20 sites or 10,000+ employees.

#### SORNS

- 43VA008/86 FR 6992 Veterans, Dependents of Veterans, and VA Beneficiary Survey Records-VA (1/21/2021) <https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01526.pdf>
- OPM/GOVT-1 General Personnel Records (12/22/2012, 77FR79694 modified as 20 FR 74815 on 11/30/2015) <https://www.gpo.gov/fdsys/pkg/FR-2012-12-11/pdf/2012-29777.pdf>
- 97VA10/85FR84119 Consolidated Data Information Systems – VA (12/23/2020) <https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28342.pdf>
- 155VA10/88FR63678 – Customer Relationship Management System (CRMS) – VA (9/15/2023) <https://www.govinfo.gov/content/pkg/FR-2023-09-15/pdf/2023-20044.pdf>
- 168VA005 / 86 FR 6975 – Health Information Exchange – VA (1/25/2021) <https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01516.pdf>
- 173VA005OP2 / 86 FR 61852 – VA Enterprise Cloud – Mobile Application Platform (Cloud) Assessing (VEAC-MAP) (11/8/2021) – <https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24368.pdf>

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

43VA008/86 FR 6992 Veterans, Dependents of Veterans, and VA Beneficiary Survey Records— VA is being amended to include the addition of VSignals. There are no additional SORNS that require amendment or revision and approval for this system. Yes, the SORN for the system does cover cloud usage and storage.

#### 4. System Changes

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

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

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

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

## Section 1. Characterization of the Information

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

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

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

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.

This question is related to privacy control AP-1, Authority To Collect, and AP-2, Purpose Specification.

*The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1. It must also match the information provided in question 3.4 of the PTA.*

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

- |  |   |   |
|--|---|---|
| <input checked="" type="checkbox"/> Name                     | <input type="checkbox"/> Emergency Contact                        | <input checked="" type="checkbox"/> Internet Protocol (IP)          |
| <input checked="" type="checkbox"/> Social Security Number   | Information (Name, Phone Number, etc. of a different individual)  | Address Numbers   |
| <input checked="" type="checkbox"/> Date of Birth            | <input checked="" type="checkbox"/> Financial Information         | <input checked="" type="checkbox"/> Medications                     |
| <input type="checkbox"/> Mother's Maiden Name                | <input checked="" type="checkbox"/> Health Insurance              | <input checked="" type="checkbox"/> Medical Records                 |
| <input checked="" type="checkbox"/> Personal Mailing Address | Beneficiary Numbers   | <input checked="" type="checkbox"/> Race/Ethnicity                  |
| <input checked="" type="checkbox"/> Personal Phone Number(s) | Account numbers   | <input type="checkbox"/> Tax Identification Number                  |
| <input type="checkbox"/> Personal Fax Number                 | <input type="checkbox"/> Certificate/License numbers <sup>1</sup> | <input type="checkbox"/> Medical Record Number                      |
| <input checked="" type="checkbox"/> Personal Email Address   | <input type="checkbox"/> Vehicle License Plate Number             | <input checked="" type="checkbox"/> Gender                          |
|  |   | <input checked="" type="checkbox"/> Integrated Control Number (ICN) |

<sup>1</sup> \*Specify type of Certificate or License Number (e.g., Occupational, Education, Medical)

- Military History/Service Connection
- Next of Kin

- Other Data Elements (list below)

Other PII/PHI data elements: Veteran ID Number, VA Email Address, Employee ID Number.

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

**Medallia GovCloud -E** consists of **3** key components (servers/databases/instances/applications/software/application programming interfaces (API). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **Medallia GovCloud -E** and the reasons for the collection of the PII are in the table below.

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

*Internal Components Table*

Component Name (Database, Instances, Application, Software, Application Program Interface (API) etc.) that contains PII/PHI	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
VSignals Assessing	Yes	Yes	Name, Address, Email Address, Phone Number, Race/Ethnicity, Gender, Date of Birth, Social Security Number, Medical Records, Medications, Military, History/ Service Connection, Integrated Control Number (ICN), Next of Kin, Insurance Beneficiary Information	Survey Sample, Quarantine file, sending survey, reminders, and retain/sort/filter Response data, Manage user roles to data access	User role access controls, Encryption, PII Masking
ESignals	Yes	Yes	Name, Birthdate, Email address	Survey Sample, Quarantine file, sending survey,	User role access controls,

			Gender, Race/Ethnicity Disability, Employee ID Number, Internet Protocol (IP) Address Number	reminders, and retain/sort/filter Response data, Manage user roles to data access	Encryption, PII Masking
Veterans Resource Community Network (VRCN) Lab	Yes	Yes	Name, Email, Address, Internet Protocol (IP) Address Number, Personal Phone Number	Registration for user account/ access and sign-in, submission of innovative ideas, experience, needs, comments, and votes.	User role access controls

**1.2 What are the sources of the information in the system?**

*These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.*

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

Email Invitation to Web Anonymous survey: The most common mode of feedback collection is via email invitation to an online anonymous survey. Any information in identifiable form or PII can be collected directly from individual, via survey or open text fields that allow individuals to disclose information. The data elements in 1.1 are extracted from various systems to identify who will receive the surveys, such as VA Customers and VA Employees. These systems include: Corporate Data Warehouse (CDW), Customer Experience Data Warehouse (CxDW), Enterprise Data Warehouse (EDW), Human Resources Information System (HRIS), Call Center Customer Relationship Management (CRM) database, Automated Monument Application System (AMAS), Burial Operations Support System (BOSS), VA Insurance program (VA administered insurance groups and Prudential Insurance Group), Readjustment Counseling Services (RCS) RCSNet, Member Services CRM database, Cisco for VEOCC Interactive Voice Response (IVR), Avaya for Enterprise Contact Center Council (ECCC) Caregiver and ECCC Women Veteran IVR, Caregiver Record Management Application (CARMA), Office of Small and Disadvantaged Business Utilization (OSDBU) CRM, Cisco WebEX (OSDBU), Salesforce, VBA National Call Center (NCC) CRM, VASS Dataset. The data elements and the source of information collected will vary based on the administration, business line, program and/or subject.

*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.*

The information is collected to determine who should be sent a survey based on the set standards for that specific feedback and to retain survey response data for analysis. Data extracts from sources such as CDW and EDW are loaded into the Medallia environment where the data is grouped and sampled. Information that is sent to VSignals via National Security Operations Center approved Trusted Internet Connection currently includes:

•Customer data - In the case of solicited feedback, VSignals requires anonymous survey invitation data — the customer information necessary to send anonymous surveys as well as for analysis. When a respondent is leaving feedback there is a section to allow for comments to be entered. These comments could potentially contain PII. •Organizational hierarchy data – The reporting units responsible for the records in the customer data. •User data - The employees who should have access to the VSignals platform and their levels of access

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

Yes, VSignals and ESignals create reports based on survey responses to gather near real-time feedback from Veterans, Eligible Dependents, Customers, Caregivers, Survivors, VA Employees, Veteran Service Organization and Community Leaders that is used to measure trust and experience/satisfaction in VA, deliver actionable intelligence to design/improve service delivery, and respond quickly to concerns and recommendations and are available via reports and dashboards to various levels of VA leadership and employees.

### **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?*

The response collection of data in Medallia GovCloud-E is collected by electronic modalities, open text/free-form feedback, closed-ended questions, social listening, short message service (SMS), and web intercepts as approved in the FEDRAMP package. The direct source of that information is based on the sampling requirements for the business line/survey topic. DI-01.1 Data Quality: VA policy requires PTAs, and as appropriate PIAs, to be updated annually in order to address any inaccurate or outdated collection, use, maintenance or sharing of PII.IP-01.1 Consent: Medallia GovCloud-E does not retrieve records by personal identifier. Any information in identifiable form or PII is not collected directly from an individual; It is extracted from the CDW and/or EDW. The notices have already been provided at the point of collection before being stored in the CDW and/or EDW

*1.3b If the information is collected on a form and is subject to the Paperwork Reduction Act, what is the form's OMB control number and the agency form number?*

VSignals: OMB 2900-0876 and OMB 2900-0770

ESignals: None

VRCN Lab: None

No information is collected using a form (vs electronic record) for any VA use of Medallia SaaS

### **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.*

Data is uploaded via invitation file transfer or uploaded directly into Medallia for the survey sample files. There are no system data checks as response information is submitted directly to the Medallia SaaS. Data integrity checks are performed by CDW and/or EDW prior to ingesting invitation files. Data engineering and/or data cleaning is performed by humans prior to data upload.

*1.4b Does the system check for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract?*

No commercial aggregation of information performed.

## **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*

### *Legal Authorities*

- Title 38, United States Code, Sections 501(a), 1705, 1710, 1722, and 5317
- 5 U.S.C. 552, "Freedom of Information Act," c. 1967
- 5 U.S.C. 552a, "Privacy Act," c. 1974
- OMB Circular A-130, Appendix III, "Security of Federal Automated Information Systems"
- Information Technology Management Reform Act of 1996 (also known as the Clinger-Cohen Act)
- Federal Information Security Management Act (FISMA) of 2002
- OMB M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002"
- VA Directive and Handbook 6502, Privacy Program
- Executive Order 14058 on Transforming the Customer Experience and Federal Service Deliver to Rebuild Trust in Government
- The President's Management Agenda, Priority 2
- 21<sup>st</sup> Century Integrated Digital Experience Act (IDEA)
- OMB Circular A-11; Section 280
- Executive Order 9397, Numbering System for Federal Accounts Relating to the Individual Persons
- National Archives and Records Administration (NARA) (44 U.S.C Chapter 21) c 2102 (a) (Pub. L. 98-497, § 103) (a)
- Records Management by the Archivist of the United States (44 U.S.C. Chapter 29) c 2901 .2 "Record Management; c 2605 (a) "Selective Retention of records; security measures."

Contractual obligations of Master Agreement, Section 8 – Survey and Questionnaires, where the surveys are voluntary, and responses are confidential and respondent anonymity protected. In

addition, other survey governance process that meets the Organizational Assessment Committee (OAC) criteria would also be reviewed with this governance board. Requirements included dissemination to greater than 20 sites or 10,000+ employees.

#### *SORNS*

- 43VA008/86 FR 6992 Veterans, Dependents of Veterans, and VA Beneficiary Survey Records- VA (1/21/2021) <https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01526.pdf>
- OPM/GOVT-1 General Personnel Records (12/22/2012, 77FR79694 modified as 20 FR 74815 on 11/30/2015) <https://www.gpo.gov/fdsys/pkg/FR-2012-12-11/pdf/2012-29777.pdf>
- 97VA10/85FR84119 Consolidated Data Information Systems – VA (12/23/2020) <https://www.govinfo.gov/content/pkg/FR-2020-12-23/pdf/2020-28342.pdf>
- 155VA10/88FR63678 – Customer Relationship Management System (CRMS) – VA (9/15/2023)  
POC: Official responsible for policies and procedures: Deputy Under Secretary for Health and Operations, VHA Member Services, VA Central Office, 810 Vermont Avenue NW, Washington, DC 20420. Telephone number 202–461– 4239 (this is not a toll-free number). Official maintaining the system: Director, VHA Member Services, 3401 SW 21st Street Bldg. 9, Topeka, Kansas 66604 <https://www.govinfo.gov/content/pkg/FR-2023-09-15/pdf/2023-20044.pdf>
- 168VA005 / 86 FR 6975 – Health Information Exchange – VA (1/25/2021) <https://www.govinfo.gov/content/pkg/FR-2021-01-25/pdf/2021-01516.pdf>
- 173VA005OP2 / 86 FR 61852 – VA Enterprise Cloud – Mobile Application Platform (Cloud) Assessing (VEAC-MAP) (11/8/2021) – <https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24368.pdf>

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

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

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

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

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

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

*Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?*

*This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.*

Follow the format below when entering your risk assessment:

**Privacy Risk:** Data is captured and pulled from other systems. If the data is not current, complete, or accurate, the survey could potentially be sent to an individual that is not relevant to the questions. The survey could also potentially be sent to the wrong email address.

**Mitigation:** If a discrepancy is discovered, the survey owner will direct the individual to submit a request to the Health Information Management System at the individual’s VA facility.

## Section 2. Uses of the Information

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

### 2.1 Describe how the information in the system that will be used in support of the program’s business purpose.

*Identify and list each use (both internal and external to VA) of the information collected or maintained. This question is related to privacy control AP-2, Purpose Specification.*

PII/PHI Data Element	Internal Use	External Use
Name	File Identification purposes Used to send personalized (feeded) survey invitations	Personalized survey invitations
Health Insurance Beneficiary Numbers Account Numbers	Used to identify appropriate survey recipient and to filter/sort survey responses to conduct data analysis	Not used
VA Email address	Used to identify appropriate survey recipient and to filter/sort survey responses to conduct data analysis	Not used
Address/Location	Used to identify appropriate survey recipient and to filter/sort survey responses to conduct data analysis	Not used
Email Address	Used to send personalized (feeded) survey invitations	Used to send personalized (feeded) survey invitations
Phone Number	May be used to send surveys to individual in the future-state	May be used to send surveys to individual in the future-state
Race/Ethnicity	Used to identify appropriate survey recipient and to filter/sort survey responses to conduct data analysis	Not used
Gender	Used to identify appropriate survey recipient and to filter/sort survey responses to conduct data analysis	Not used

Date of Birth	Used to identify appropriate survey recipient and to filter/sort survey responses to conduct data analysis	Not used
Social Security Number	Used to identify appropriate survey recipient	Not used
Veteran ID Number	Used to identify appropriate survey recipient	Not used
Medical Records	Used to identify appropriate survey recipient	Not used
Medications	Used to identify appropriate survey recipient and to filter/sort survey responses to conduct data analysis	Not used
Military History/Service Connection	Used to identify appropriate survey recipient and to filter/sort survey responses to conduct data analysis	Not used
Integrated Control Number (ICN)	Used to identify appropriate survey recipient	Not used
Internet Protocol (IP) Address Number	Used to identify unique respondents	Not used
Employee ID Number	Used to identify appropriate survey recipient	Not used
Next of Kin (NOK)	Used to identify appropriate survey recipient	Not used
Financial Information	Used to identify appropriate survey recipient	Not used

**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?*

Medallia SaaS provides real-time text analytics. Natural Language Processing (NLP) is used to analyze text, sort and group into emerging trends, patterns, and key insights. The system uses this data analysis to create alerts, categorization, and/or sentiments from unstructured data to assist with identifying changes/new trends, understanding customer needs and prioritizing action(s). Data analysis is displayed in reports and dashboards with visualizations.

*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.*

Medallia captures customer experience feedback submitted by an individual. VSignals responses for VHA surveys are interfaced with PATS-R to allow VHA employees to take follow-up action on addressing concerns or complaints, additionally, responses flagged as potential risk for homelessness or crisis alerts are share with the VA Homeless program and VA Crisis Hotline for review and follow-up, if deemed necessary

### **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?*

Medallia GovCloud -E is hosted in Medallia GovCloud FedRAMP High authorized environment that is hosted on AWS GovCloud. FedRAMP High authorization enforces the data in transit and at rest protection as documented within the Medallia GovCloud -E SSP package. AWS GovCloud (US) is an isolated AWS region designed to host sensitive data and regulated workloads in the cloud. This application is accessible from the VA network via TIC and Government-furnished equipment (GFE) or other controlled methods of accessing the VA Network including the Citrix-Access Gateway (CAG) services via two- factor PIV enabled access. Medallia GovCloud -E is separated from other Medallia GovCloud customers and implemented within its own VPC.

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

Medallia GovCloud -E does not require Social Security Numbers (SSN) for its operations. If SSNs are used to identify who will be surveyed, it would be protected with encryption controls in place at rest and in transit.

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

Medallia GovCloud -E requires the minimal collection of PII (e.g. first name, last name and email address) for its operations and it is protected by the encryption controls in place at rest and during transit. For some identified fields an additional field level encryption can be implemented at the application level.

Medallia GovCloud -E do not require PHI for its operations. But if a customer specific use case implementation requires the use of PHI it would be protected with encryption controls in place at rest and in transit. For some identified fields an additional field level encryption can be implemented at the application level.

### **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?*

User Roles are created and managed by the VA to limit PII access as needed. For Medallia GovCloud -E, only VA staff or designated contractors with a VA.Gov e-mail address may gain access to the system via SAML SSOi. When a new program is developed and configured, the program team asks the stakeholders to provide a list of “designated approvers” who are authorized to provide user access to all approved/authorized users in their network as per program office guidelines or standard operating procedures established by the stakeholder group or Administration in question. An initial list of approved users is provided to the program team by the stakeholder and any subsequent users requesting access are approved by the designated approvers via an electronic user access request process.

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

Medallia GovCloud -E level criteria, procedures, controls and overall access responsibilities will be defined by the specific VA teams implementing their program. Infrastructure level access controls are inherited by Medallia FedRAMP High authorized package. VA teams do not have any infrastructure level access to Medallia GovCloud -E.

*2.4c Does access require manager approval?*

Access to Medallia GovCloud-E is managed by VA federal employees through an approved process culminating in a review from the ISO. Once approval is granted, users are provisioned through VA’s Active Directory groups.

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

Medallia change logs record all activities, if specific fields are identified as PII they can be extracted (e.g., first name, last name, email address).

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

The VA Product Team, which is the Business Owner and IT Project Manager, is responsible for ensuring that minimal PII is required to be collected for specific programs, and assures the required procedures and policies are in place.

At the infrastructure level, Medallia GovCloud-E has implemented encryption controls at rest and during transit for the protection of PII.

For applications behind the VA TIC, it is shared responsibility between the Medallia team and VA Product Team to configure data in transit encryption.

## 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*

1. Name
2. Health Insurance Beneficiary Numbers Account Numbers
3. Social Security Number
4. Veteran ID Number
5. Personal Mailing Address
6. Personal Email Address
7. Phone Number
8. Race/Ethnicity
9. Gender
10. Date of Birth
11. Integrated Control Number (ICN)
12. Internet Protocol (IP) Address Number
13. Personal Phone Number
14. Medications
15. Medical Records
16. Military History/Service Connection
17. Employee ID Number
18. VA Email Address
19. Next of kin (NOK)
20. Financial Information

### 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.*

Yes, the system uses Cloud technology and will follow the NARA approved retention schedule.

GENERAL RECORDS SCHEDULE 6.5: Public Customer Service Records, Item 10: Public customer service operations records, Temporary. Destroy 1 year after resolved, or when no longer needed for business use, whichever is appropriate.

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

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

*This question is related to privacy control DM-2, Data Retention and Disposal.*

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

Yes, GENERAL RECORDS SCHEDULE 6.5: Public Customer Service Records, item 010 Public customer service operations records, DAA-GRS2017-0002- 0001.

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

GENERAL RECORDS SCHEDULE 6.5: Public Customer Service Records, item 010 Public customer service operations records, DAA-GRS2017-0002- 0001

### **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.*

Data utilized by Medallia GovCloud -E is pulled from the systems listed in Table 4.1 The data collected is deleted when the contract is terminated, and the instance needs to be decommissioned. Medallia GovCloud Team defaults 30 days (or as required by customer) for the instance decommission from the end of contract notification. This is to avoid any disruption in customer services or to meet additional customer requirements. As Medallia GovCloud -E is hosted on AWS GovCloud, physical data destruction and sanitization to be done by Medallia is not applicable to Medallia GovCloud -E, it is inherited from AWS GovCloud.

Medallia will coordinate with the Records Officer, complete the VA Form 7468 and then perform electronic media sanitation per the Standard Operating Procedure Media Sanitization and Disposition IAW Information and Technology Operations and Services (ITOPS) End User Operations.

### **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.*



Medallia provides agency specific sandbox environments for program specific testing (program specific dev / QA environment to test the business use case implementation) that does not involve the use of customer PII. If the specific use case implementation requires PII, then it is the customer's responsibility to approve the usage of minimized PII for testing.

Medallia GovCloud-E performs testing in the production environment Medallia GovCloud and are secured with the same control implementation as of the production environment. No live data is used when testing is performed.

Medallia GovCloud -E does not use their system for research.

Training is not provided outside the scope of new users, for new roles or new system features. Trainings will never be recorded if it includes PII and concerted efforts will be made not to share PII in trainings. Training is only provided with the proper ATO in place to utilize this system.

### **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:** Medallia manages and retains data for a diverse set of programs across VA. If a Medallia GovCloud -E must retain data beyond the approved retention schedule, the risk of information being breached increases.

**Mitigation:** Medallia coordinates with the ISO to ensure adherence to the VA provided retention schedule. On an annual basis, the systems team will review the retention schedule against each instance, identify data which requires deprecation, and schedule removal. Additionally, data collected, processed, and retained will be protected in accordance with VA Handbook 6500 and FIPS

Version date: October 1, 2023

Page 17 of 37

140-2 encryption and data in-transit protection standards. All systems and individuals with access to the system will be approved, authorized, and authenticated before access is granted. VA annual privacy and security training compliance will be enforced for all VA employees, contractors, and vendors.

## 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*

<i>List the Program Office or IT System information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</i>	<i>Describe the method of transmittal</i>
VA's Identity & Access Management (IAM) System	Manage and track employee access to Dashboards/Reports based on User Role(s) assigned	Name, VA Email address	Cloud interconnection
Veterans Relationship Management (VRM)	Survey sampling, filtering/sorting response data.	Name, email address, Medical Information, Address, Phone number, Race/Ethnicity,	Site-to-Site VPN Tunnel on port 443

<b>List the Program Office or IT System information is shared/received with</b>	<b>List the purpose of the information being shared /received with the specified program office or IT system</b>	<b>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</b>	<b>Describe the method of transmittal</b>
Customer Resource Management (CRM) Application Framework (AF)		Gender, Social Security Number, Veteran ID Number	
Clinical Resource Hub: Analytics and Business Intelligence LAN (ABI LAN) VSSC/Veteran Support Service Center)	Survey sampling, filtering/sorting response data.	Name, email address, Medical Information, Address, Phone Number, Race/Ethnicity, Gender, Social Security Number, Veteran ID Number	Business Partner Extranet (BPE) – secure and encrypted connection housed at AITC. FIPS 199
Patient Advocate Tracking system – Revised (PATS-R): Microsoft Dynamics	Share information with VHA PATS-R for patient advocates to track and respond to customer concerns, recommendations, and accolades.	Full Name, Date of Birth, email address, Medical Records, Address/Location, Phone Number, Integrated control number (ICN)	S3 Bucket Data Transfer
VA Customer Experience Data Warehouse (CxDW) – Azure Cloud Data Lake	Data sharing and analyze data across multiple data sources.	Full name, email address, Medical Record, Personal Address, Phone Number, Race/Ethnicity, Gender, Social Security Number, Veteran ID Number	Secure Gateway between AWS GovCloud and Azure GovCloud
Human Resources Information System (HRIS)	Employee Signals survey sampling and response management.	Employee ID, Birth Date, Race/Ethnicity, Name, VA email, Gender	Manual Process verified by VA employees
Veterans Health Administration (VHA) IE Salesforce	Internal VA project management of information submitted via survey response.	Name, Business Email	VA Secure File Transfer Protocol (SFTP)
Corporate Data Warehouse (CDW)	Survey sampling, filtering/sorting response data.	Name, email, date of birth, mailing address, race/ethnicity, gender and phone number	Encrypted via Trusted Internet Connection (TIC)
Enterprise Data Warehouse (EDW)	Survey sampling, filtering/sorting response data.	Name, DOB, Email address, phone number, SSN, Gender, mailing address, personal mailing address	S3 Bucket Transfer
Call Center Customer Relationship	Survey sampling, filtering/sorting response data.	Name, Email address, personal phone number	S3 Bucket Transfer

<i>List the Program Office or IT System information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</i>	<i>Describe the method of transmittal</i>
Management (CRM) database			
Automated Monument Application System (AMAS)	Survey sampling, filtering/sorting response data.	Name, gender, Date of Birth, Date of Death, Personal Mailing address, email address, phone number	Delimited file via SFTP
Burial Operations Support System (BOSS)	Survey sampling, filtering/sorting response data.	Name, birth date, death date, personal mailing address, phone number, email address, next of kin (NOK)	Delimited file via SFTP
VA Insurance program (VA administered insurance groups and Prudential Insurance Group)	Survey sampling, filtering/sorting response data.	Name, SSN, Date of Birth, Gender, Address, email	Delimited file via email and S3 Bucket Transfer
Member Services CRM database	Survey sampling, filtering/sorting response data.	Name, Date of Birth, Personal Phone number(s), gender, Integrated control number (ICN), military history/service connection	S3 Bucket Transfer
Cisco for VEOCC Interactive Voice Response (IVR)	Survey sampling, filtering/sorting response data.	Name, Phone Number, Email address	Spreadsheet via email and S3 Bucket Transfer
Avaya for Enterprise Contact Center Council (ECCC) Caregiver and ECCC Women Veteran IVR	Survey sampling, filtering/sorting response data.	Name, phone number, email address	Spreadsheet via email and S3 Bucket Transfer
Cisco WebEX (OSDBU)	Survey sampling, filtering/sorting response data.	Name, phone number, email address	S3 Bucket Transfer
Caregiver Record Management Application (CARMA)	Survey sampling, filtering/sorting response data.	Name, phone number, email address	Spreadsheet via email / Manual process verified by VA employees and S3 Bucket Transfer
Office of Small and Disadvantaged Business Utilization (OSDBU) CRM	Survey sampling, filtering/sorting response data.	Name, date of birth, gender, email address	S3 Bucket Transfer

<i>List the Program Office or IT System information is shared/received with</i>	<i>List the purpose of the information being shared /received with the specified program office or IT system</i>	<i>List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system</i>	<i>Describe the method of transmittal</i>
VBA National Call Center (NCC) CRM	Survey sampling, filtering/sorting response data.	Name, Phone number, financial information, gender, integrated control number (ICN), military history/service connection,	Spreadsheet via email and S3 Bucket Transfer
CommCare CRM Database	Survey sampling, filtering/sorting response data.	Name, SSN, Date of Birth, Personal Phone Number	Azure SQL database and S3 Bucket Transfer
Readjustment Counseling Services (RCS) RCSNet	Survey sampling, filtering/sorting response data.	Name, Date of Birth, phone number, medical records, race/ethnicity, gender, military history/service connection	PowerBI dashboard, manual employee review and S3 Bucket Transfer
Salesforce: Veteran Rapid Retraining Assistance Program (VRRAP) Tool	Survey sampling, filtering/sorting response data.	Name, Email address, phone number	SFTP
VA Solid Start (VASS) dataset	Survey sampling, filtering/sorting response data.	Name, Phone number, Military history, Date of Birth, email address, SSN	Spreadsheet via email and S3 Bucket Transfer

**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:** Risks may include end users who do not log out of Medallia GovCloud -E from their computers. As these risks cannot be completely eliminated, information could be shared with unauthorized personnel.

**Mitigation:** Medallia GovCloud -E has a “time-out” setting which will automatically log the user out after a period of inactivity. Safeguards are implemented to ensure data is not sent to unauthorized VA employees, including employee security and privacy training and required reporting of suspicious activity. Use of secure passwords, access for need-to-know basis, Personal Identification Verification (PIV) Cards,

Personal Identification Numbers (PIN), encryption, and access authorization are all measures that are utilized for the system.

## Section 5. External Sharing/Receiving and Disclosure

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

**5.1 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

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

Members of the Public-Consultants	Crowdsourcing innovations from community partners	Name, Email Address, IP Address	43VA008/8 6 FR 6992	https (web URL) and VA's dedicated TIC implementation with Medallia GovCloud
Members of the Public - Veterans-Persons Surveyed	Responding to Digital comment card surveys	Name , Email Address, Phone Number, Date of Birth, IP Address	43VA008/8 6 FR 6992	https (web URL) and VA's dedicated TIC implementation with Medallia GovCloud
Akamai Content Delivery Network (CDN)	Digital Survey data transfer (e.g. survey pop-up on VA.gov)	Internet Protocol (IP) Address	43VA008/8 6 FR 6992, MOUISA	https (web URL) and VA's dedicated TIC implementation with Medallia GovCloud
Mobile API	Survey sampling data files for upload to Medallia	Name, Personal mailing address, email address, age, date of birth, race, gender, phone number, Internet Protocol (IP) address	43VA008/8 6 FR 6992, MOUISA	https (web URL) and VA's dedicated TIC implementation with Medallia GovCloud
Amazon Web Service (AWS) S3 Bucket	Survey sampling data files for upload to Medallia	Name, Personal mailing address, email address, date of birth, race/ethnicity, gender, phone number, Internet Protocol (IP) address, ICN	43VA008/8 6 FR 6992, MOUISA	https (web URL) and VA's dedicated TIC implementation with Medallia GovCloud

## **5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure**

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

*If no External Sharing listed on the table above, (State there is no external sharing in both the risk and mitigation fields).*

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

*Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.*

*This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing*

Follow the format below:

**Privacy Risk:** Due to the sensitive nature of this user data, there is a risk that, if the data were accessed or received by unauthorized parties/recipients or otherwise breached, serious personal, professional and/or financial harm may result for the affected individuals.

**Mitigation:** Medallia GovCloud -E uses several security measures designed to ensure that the information is not inappropriately disclosed or released. Use of encryption to secure data during transmission and at rest. Users will have a “time-out” setting which will automatically log the user out after a period of inactivity. Safeguards are implemented to ensure data is not sent to unauthorized VA employees, including employee.

## Section 6. Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

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

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

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

Yes, each survey for VSignals states specifically in the body: We are asking for this information so that you can provide compliments, recommendations, or concerns to VA. By filling out this survey, you are authorizing VA database access to retrieve Veteran contact information to follow up with you accordingly for purposes of service recovery, potential crisis, or to learn more about feedback you have shared regarding your experience with VA. Your contact information and response may be referred to the Veterans Crisis Line if an automated review indicates your response may be concerning. The Veterans Crisis Line may contact you for follow up as a result of that referral. VA may utilize individual Veteran survey data from this survey or other sources to ensure the final scores truly and accurately represent the experiences of Veterans. This information is collected in accordance with section 3507 of the Paperwork Reduction Act of 1995. Title 38, United States Code, allows us to ask for this information. We estimate that you will need an average of 2 minutes to review the instructions and complete this survey. The results of this survey will be used to inform opportunities for program improvement in the quality of VA services. Participation in this survey is voluntary, and your decision not to respond will have no impact on VA benefits or services which you may currently be receiving. VA cannot conduct or sponsor a collection of information



unless a valid OMB control number is displayed. You are not required to respond to a collection of information if this number is not displayed. Valid OMB control numbers can be located on the OMB Internet Page at <https://www.reginfo.gov/public/do/PRAMain>. Information gathered will be kept private to the extent provided by law.

For ESignals, the Privacy statement is provided on the landing page of the ESignals dashboard, as well as a part of every survey disseminated. The last statement on each ESignals survey requires the individual to certify they understand and agree with this statement: I certify that I understand my responses to this survey are voluntary, confidential, and anonymous. I understand that in order to protect confidentiality, all comments provided are anonymized in reporting, making the survey collection team unable to directly respond to individuals' comments, or refer comments to any other review body, and I understand that concerns such as grievances, patient safety issues, discrimination, harassment, ethical concerns, or other time-sensitive issues should be directly reported to the appropriate responsible parties at my organization to ensure they receive prompt attention.

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

*6.1c Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection.*  
The notice is provided specifically on each form prior to individual's submission to VA.

## **6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?**

*This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress.*

Yes, they can choose to not respond to the survey. No penalty or denial of service will result in not completing it.

## **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.*

The users are notified on how their information will be used before beginning or before submitting the survey response. Additionally, Veterans are explicitly provided with the option of either allowing or disallowing VA staff from following up with them about their input/feedback. VSignals surveys state this at the footer: "Participation in this survey is voluntary, and your decision not to respond will have no impact on VA benefits or services which you may currently be receiving. VA cannot conduct or sponsor a collection of information unless a valid OMB control number is displayed. You are not required to respond to a collection of information if this number is not displayed." OMB guidelines that VEO operates under stipulate that VSignals

survey responses/data trends may only be used for internal quality and systems improvement efforts. Neither aggregate data trends nor individual respondent records may be shared or used externally in any form or fashion.

#### **6.4 PRIVACY IMPACT ASSESSMENT: Notice**

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

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

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

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

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

Follow the format below:

**Privacy Risk:** If a Privacy Act Statement was not clear or reviewed and did not reference the government's authority, an individual may enter PII in open text fields even when the open text field directions state to not include that type of data.

**Mitigation:** Medallia GovCloud -E will automatically mask information that may potentially be PII, such as SSN. If a pattern arises, the notices will be reviewed.

## **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.***

Users will not have access to their information unless they file a request under the Privacy Act of 1974 to the Office of Accountability and Whistleblower Protection (OAWP) or Freedom of Information Act (FOIA) to the VA FOIA Service. The business team can assist in directing members on how to submit these requests.

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)?

This system is not exempt from the Privacy Act.

7.1c If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information?

This system is subject to the Privacy Act.

## **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.*

Users will not have access to modify their survey responses once submitted to this system. This is a survey/feedback tool.

## **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.*

Users will not have access to modify their survey responses once submitted to this system. This is a survey/feedback tool.

## **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 ensure data accuracy.***

*This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.*

Users will not have a redress process. This is a survey/feedback tool.

## **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:** There is a risk that members of the general public may not know that the Medallia GovCloud -E exists within the Department of Veterans Affairs. This poses a low risk to the enterprise. When VA collects personal data from an individual, VA will inform him or her of the intended uses of the data, the disclosures that will be made, the authorities for the data's collection, and whether the collection is mandatory or voluntary. VA will collect no data subject to the Privacy Act unless a Privacy Act system notice has been published in the Federal Register and posted on the VA Systems of Records website.

**Mitigation:** OMB guidelines that VEO operates under stipulate that survey responses/data trends may only be used for internal quality and systems improvement efforts. Neither aggregate data trends nor individual respondent records may be shared or used externally in any form or fashion.

## 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?

For VSignals: Only VA staff or designated contractors with a VA.Gov e-mail address may gain access to the VSignals system. When a new survey is developed and configured, the Business Owner asks the stakeholders to provide a list of "designated approvers" who are designated and authorized to provide user access to all approved/authorized users in their network as per program office guidelines or standard operating procedures established by the stakeholder group or Administration in question. An initial list of approved users is provided to the Business Owner by the stakeholder and any subsequent users requesting access are approved by the designated approvers via an electronic user access request process.

For ESignals: To access the different roles within the dashboards, team members must have access within the VA network and established SAML SSOi process for access. There are unique roles where there are limited users, for those cases exception's list is created to only allow those on the exceptions list ability to access through same SSOi process.

For VRCN Lab: The user must submit an enrollment request that is reviewed and approved by a VA employee assigned with the Administrator Role for that site.

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

No users from other agencies have access to the system.

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

For VSignals: All user roles are read-only for VA end users except for an Ad Hoc (self-service) role that is exclusively used by VEO/EMD staff. There are multiple user roles to restrict access to various Dashboards. For ESignals: There are different roles for each ESignals dashboard (but there is no personal identifiable information) showing aggregate results of each survey program. If there are <5 responses recorded for any site, or unit, data will not be displayed when filtering in the dashboard to protect participant anonymity.

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

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

VA Contractors will have access to PII to assist VA in collecting and cleaning the data for survey sampling, uploading to Medallia, and filtering/sorting data for analysis. Those contractors are required to obtain certain levels of background investigation clearance and complete appropriate training before obtaining such access/information. A Business Associate Agreement (BAA) is being developed and will be signed before granting contractors access to the system.

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

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

Users must have completed VA 10176 VA Privacy and Information Security Awareness and Rules of Behavior training in order to obtain Single Sign-on access through a VA issued PIV.

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

8.4a If Yes, provide:

1. The Security Plan Status: Approved
2. The System Security Plan Status Date: 03/09/2023
3. The Authorization Status: FedRAMP Authorized
4. The Authorization Date: 04/09/2021
5. The Authorization Termination Date: 6/15/2024
6. The Risk Review Completion Date: 12/18/2023
7. The FIPS 199 classification of the system (LOW/MODERATE/HIGH): High

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

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

<<ADD ANSWER HERE>>

## 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 (ITMAaaS). 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)**

This system utilizes Medallia GovCloud, a Government only Cloud implementation of Medallia’s Software as a Service (SaaS) that is hosted on AWS GovCloud. Medallia GovCloud is currently FedRAMP High Authorized and active on the FedRAMP Marketplace under FedRAMP ID FR1711262842

### 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.

36C10A23D0004 states “The Contractor shall deliver to the Government all data first produced under this Contract/Order with unlimited rights as defined by FAR 52.227-14.”

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

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

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

CSP Collects the program specific data as described below for the specific feature implementation in the customer specific instance. This data is customer owned.

**Medallia Survey Engine** - Customer determined but at minimum email address, first name and last name. IP address of feedback respondent

**Medallia Reporting Application** - Customer determined but at minimum email address, first name and last name and IP address of feedback respondent.

**Medallia Digital** - Customer determined but at minimum, IP address of feedback respondent.

**Medallia Conversation** - Customer determined but at minimum Phone Number of feedback respondent.

**Medallia Speech** - Customer defined Audio Files that may potentially have PII information.

**Medallia Ideas** - Customer determined but at a minimum email address, first name, last name. Customer defined images (user can upload a picture to their profile)

**Application Specific Audit Logs** are stored within the Application database and accessible to customers.

Other than that, there is no customer specific ancillary data collected. There is environment specific infrastructure and network metadata that is generated, but it is not customer specific, and it is owned by Medallia GovCloud.

### **9.4 NIST 800-144 states, “Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf.” Is this principle described in contracts with customers? Why or why not?**

*What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.*

CSP Collects the program specific data as described below for the specific feature implementation in the customer specific instance. This data is customer owned.

**Medallia Survey Engine** - Customer determined but at minimum email address, first name and last name. IP address of feedback respondent

**Medallia Reporting Application** - Customer determined but at minimum email address, first name and last name and IP address of feedback respondent.

**Medallia Digital** - Customer determined but at minimum, IP address of feedback respondent.

**Medallia Conversation** - Customer determined but at minimum Phone Number of feedback respondent.

**Medallia Speech** - Customer defined Audio Files that may potentially have PII information.

**Medallia Ideas** - Customer determined but at a minimum email address, first name, last name. Customer defined images (user can upload a picture to their profile)

**Application Specific Audit Logs** are stored within the Application database and accessible to customers.

Other than that, there is no customer specific ancillary data collected. There is environment specific infrastructure and network metadata that is generated, but it is not customer specific and is owned by Medallia GovCloud.

**9.1 NIST 800-144 states, “Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf.” Is this principle described in contracts with customers? Why or why not?**

*What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met? This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.*

Yes. The SaaS contract (36C10A23D0004) states: “The information system solution selected by the Contractor shall comply with the Federal Information Security Management Act (FISMA) and have a current VA authorization.” And “All VA sensitive information shall be protected at all times in accordance with local security field office System Security Plans (SSP’s) and Authority to Operate (ATO)’s for all systems/LAN’s accessed while performing the tasks detailed in this Product Description.” And “Information systems that are designed or developed for or on behalf of VA at non-VA facilities shall comply with all VA directives developed in accordance with FISMA, HIPAA, NIST, and related VA security and privacy control requirements for Federal information systems. This includes standards for the protection of electronic PHI, outlined in 45 C.F.R. Part 164, Subpart C, information and system security categorization level designations in accordance with FIPS 199 and FIPS 200 with implementation of all baseline security controls commensurate with the FIPS 199 system security categorization (reference VA Handbook 6500, Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program, and the TIC Reference Architecture). During the development cycle a Privacy Impact Assessment (PIA) shall be completed, provided to the COR, and approved by the VA Privacy Service in



accordance with Directive 6508, Implementation of Privacy Threshold Analysis and Privacy Impact Assessment.” And “For Cloud Services hosting, the Contractor shall also ensure compliance with the Federal Risk and Authorization Management Program (FedRAMP).”

**9.5 If the system is utilizing Robotics Process Automation (RPA), please describe the role of the bots.**

*Robotic Process Automation is the use of software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. For example, will the automation move or touch PII/PHI information. RPA may also be referred to as “Bots” or Artificial Intelligence (AI).*

This system does not use RPA.

## Section 10. References

### Summary of Privacy Controls by Family

*Summary of Privacy Controls by Family*

<b>ID</b>	<b>Privacy Controls</b>
<b>AP</b>	<b>Authority and Purpose</b>
AP-1	Authority to Collect
AP-2	Purpose Specification
<b>AR</b>	<b>Accountability, Audit, and Risk Management</b>
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
<b>DI</b>	<b>Data Quality and Integrity</b>
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
<b>DM</b>	<b>Data Minimization and Retention</b>
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
<b>IP</b>	<b>Individual Participation and Redress</b>
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
<b>SE</b>	<b>Security</b>
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
<b>TR</b>	<b>Transparency</b>
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
<b>UL</b>	<b>Use Limitation</b>
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

**Signature of Responsible Officials**

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

---

**Privacy Officer, Julie Drake**

---

**Information System Security Officer, Roland Parten**

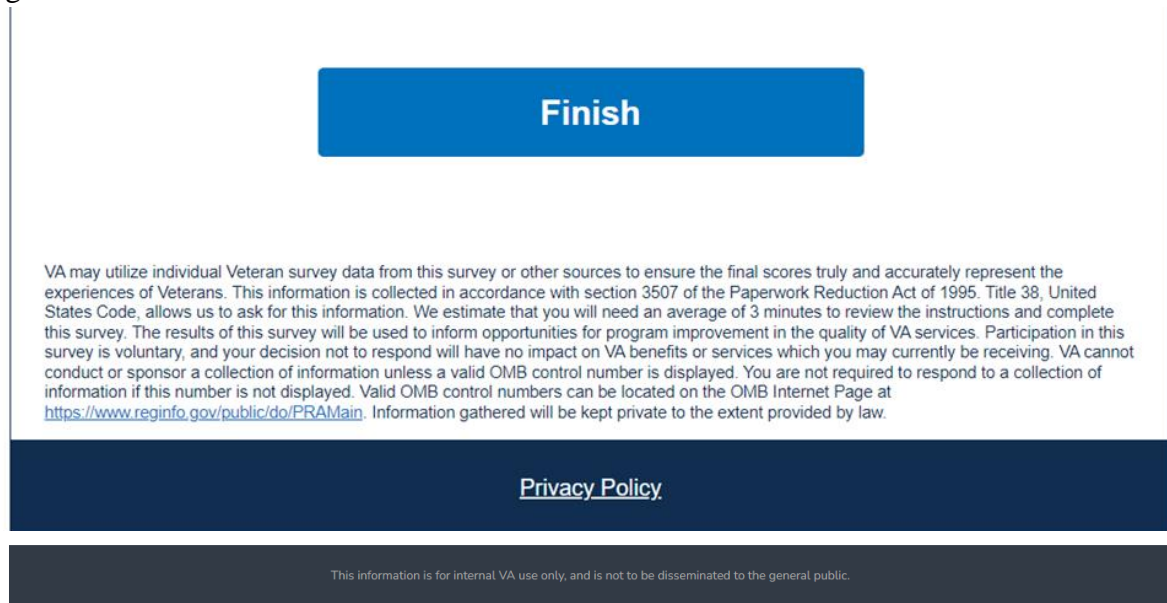
---

**Information System Owner, Henna Grover**

## APPENDIX A-6.1

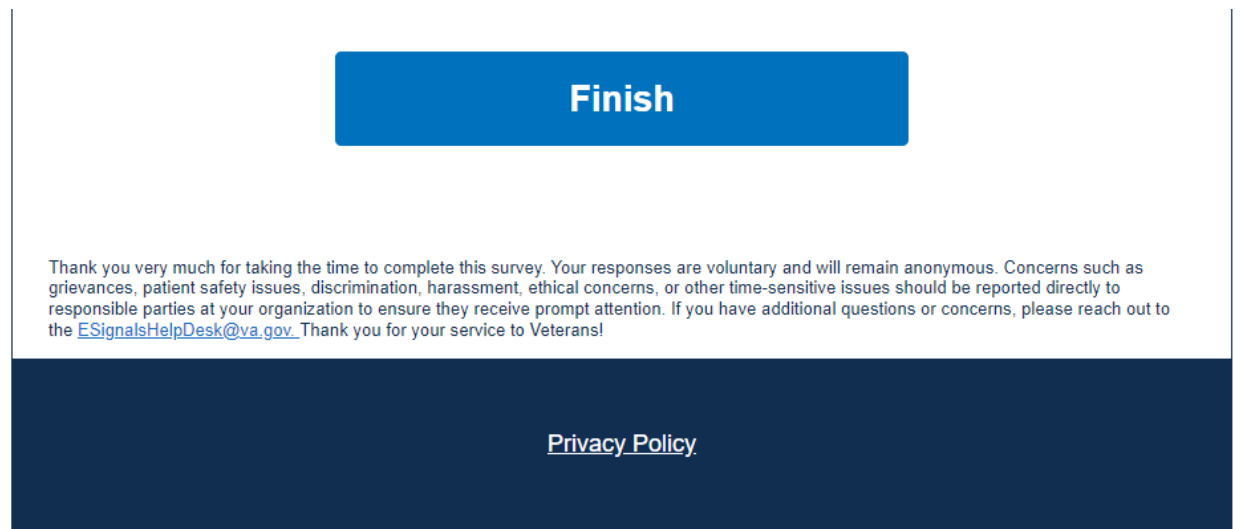
Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy; a Privacy Act notice on forms; screen shot of a website collection privacy notice).

VSignals Notice:



The screenshot shows a survey completion screen. At the top center is a blue button with the word "Finish" in white. Below the button is a paragraph of text explaining that VA may use individual Veteran survey data to ensure final scores accurately represent the experiences of Veterans. It mentions that the information is collected in accordance with section 3507 of the Paperwork Reduction Act of 1995, Title 38, United States Code. The text states that participation is voluntary and that the results will be used to inform opportunities for program improvement. It also includes a link to the OMB Internet Page at <https://www.reginfo.gov/public/do/PRAMain>. At the bottom of the screen is a dark blue bar with the text "Privacy Policy" in white, and a small grey bar at the very bottom with the text "This information is for internal VA use only, and is not to be disseminated to the general public."

ESignals Notice:



The screenshot shows a survey completion screen. At the top center is a blue button with the word "Finish" in white. Below the button is a paragraph of text thanking the user for taking the time to complete the survey. It states that responses are voluntary and will remain anonymous. It also mentions that concerns such as grievances, patient safety issues, discrimination, harassment, ethical concerns, or other time-sensitive issues should be reported directly to responsible parties at your organization. It includes a link to the [ESignalsHelpDesk@va.gov](mailto:ESignalsHelpDesk@va.gov). At the bottom of the screen is a dark blue bar with the text "Privacy Policy" in white.

## **HELPFUL LINKS:**

### **General Records Schedule**

<https://www.archives.gov/records-mgmt/grs.html>

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

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

### **VA Publications:**

<https://www.va.gov/vapubs/>

### **VA Privacy Service Privacy Hub:**

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

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

[VHA Notice of Privacy Practices](#)

[VHA Handbook 1605.04: Notice of Privacy Practices](#)