Privacy Impact Assessment for the VA IT System called:

VSignals Assessing

Office of Information and Technology (OI&T) Veterans Affairs Central Office (VACO)

Date PIA submitted for review:

12/20/2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Tonya Facemire	Tonya.Facemire@va.gov	202-632-8423
Information System Security Officer (ISSO)	Denise Engolia	Denise.Engolia@va.gov	504-619-4443
Information System Owner	Stefano Masi	Stefano.Masi@va.gov	860-681-9927

Abstract

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

VSignals is a FedRAMP approved Software as a Service (SaaS) that provides its clients with the ability to operationalize their customer experience management by aggregating customer feedback and experiences into a single interface location. VSignals uses a Software as a Service (SaaS) based solution called Medallia to help customers constantly improve the experience they deliver to their clients. VSignals provides this functionality with an interface for client feedback through the use and implementation of their VSignals VA Instance. VSignals is a customer experience management solution. VSignals will help the customer organizations who use it to understand their client's feedback and react in an appropriate manner. VSignals gathers client feedback through various mediums, analyzes the data gathered, and presents it to the organization. VSignals gathers data via email-based surveys, text-based 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 surveys around an organization, product, or service.

Overview

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

1 General Description

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

Veterans Signals (VSignals); Office of Information and Technology (OI&T)

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

VSignals is a customer experience management solution. VSignals will help the customer organizations who use it to understand their client's feedback and react in an appropriate manner. VSignals gathers client feedback through various mediums, analyzes the data gathered, and presents it to the organization. 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.

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

Office of Information and Technology (OI&T)

2. Information Collection and Sharing

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

VSignals is a solution designed to facilitate collection of Veteran feedback through the use of a COTS application known as the Medallia tool Customer Engagement Management (CEM) system, implemented as a software-as-a-service (SaaS) and hosted externally, for anonymous survey and case management. VSignals is hosted within the AWS GovCloud SaaS and utilizes Virtual Private Cloud (VPCs) to separate the different environments. The AWS VPCs are completed segregated from other VPCs hosted on the AWS SaaS with no way to move from VPC to VPC. 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's network via 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. VSignals has separated the front-end customer components into their own VPC and management and security components are hosted in a separate Management VPC. The only communication between the two VPCs is through the use of VPC peering used to perform vulnerability scanning and system logging and monitoring requirements.

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

VSignals is a customer experience management solution. VSignals will help the customer organizations who use it to understand their client's feedback and react in an appropriate manner. VSignals gathers client feedback through various mediums, analyzes the data gathered, and presents it to the organization. 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.

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

VSignals is a SaaS solution powered by the Medallia Customer Experience Management product. 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.

G. Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.

VSignals is a SaaS solution powered by the Medallia Customer Experience Management product. 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.

3. Legal Authority and SORN

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

Veterans, Dependents of Veterans, and VA Beneficiary Survey Record (43VA008/ 86 FR 6992). To the extent that records contained in the system include information protected by Title 45, Code of Federal Regulations (CFR), Parts 160 and 164 (i.e., individually identifiable health information), and 38 U.S.C. 7332 (i.e., medical treatment information related to drug abuse, alcoholism, or alcohol abuse, sickle cell anemia, or infection with the human immunodeficiency virus, that information cannot be disclosed under a routine use unless there is also specific statutory authority in 38 U.S.C. 7332 and regulatory authority in 45 CFR parts 160 and 164 permitting disclosure).

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?

Veterans, Dependents of Veterans, and VA Beneficiary Survey Records— VA is being amended to include the addition of VSignals.

D. System Changes

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

No changes are necessary.

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

No changes are necessary

VSignals is a customer experience management solution. VSignals will help the customer organizations who use it to understand their client's feedback and react in an appropriate manner. VSignals gathers client feedback through various mediums, analyzes the data gathered, and presents it to the organization. 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.

VSignals utilizes the tool from Medallia. The Medallia tool provides real-time anonymous survey, comment card development & management, online reporting, real-time alerts, case management, occurrence management, analytics, and performance metric reporting (presented as dashboards) to generate a unified view of the customer to support continuous improvements in Veteran Customer Experience (VCE). At present, insights on customer experiences are gained through the collection of data from numerous anonymous surveys and forms administered by a decentralized and uncoordinated approach. In addition, there is no unified communication channel from whereVA can listen directly to our customers.

VSignals plans to consolidate these existing anonymous surveys and become the sole tool of choice for any and all anonymous survey generation and feedback it will be creating a seamless touch-point between a Veteran and or eligible dependent and the VA. This capability is aimed at improving the Veterans Experience by connecting Veterans in real time with VA. Specifically this tool will provide the ability to ask Veterans and eligible dependents of veterans closedended questions and submit open text feedback. Additionally, in some occasion’s veterans might want to add additional feedback on a section where comments can be written.

VSignals is a solution designed to facilitate collection of Veteran feedback through the use of a COTS

application known as the Medallia tool Customer Engagement Management (CEM) system, implemented as a software-as-a-service (SaaS) and hosted externally, for anonymous survey and case management. VSignals is hosted within the AWS GovCloud SaaS and utilizes Virtual Private Cloud (VPCs) to separate the different environments. The AWS VPCs are completed segregated from other VPCs hosted on the AWS SaaS with noway to move from VPC to VPC. 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's network via 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. VSignals has separated the front-end customer components into their own VPC and management and security components are hosted in a separate Management VPC. The only communication between the two VPCs is through the use of VPC peering used to perform vulnerabilityscanning and system logging and monitoring requirements.

VSignals shall leverage multiple layers of security, including security groups and network access control lists, to help control access to the Amazon EC2 instances in each subnet.

Veterans completing anonymous survey will be directed to a separate Virtual Private Cloud (VPC) where they will have access to the VSignals anonymous surveys via HTTPS. VSignals deployments on the AWS GovCloud are documented in Federal Risk and Authorization Management Program (FedRAMP). The VSignals program does have a VA Agency ATO.

Information security is vital to our critical infrastructure and its effective performance and protection of importantmission data. Proper management of information technology systems is essential to ensure the confidentiality, integrity and availability of the data transmitted, processed or stored by the VA within the VSignals system.

Currently, we have acquired a VA Agency ATO. The Medallia Software maintains a FedRAMP ATO, but prior to obtaining a FedRAMP ATO we obtained a VA Agency ATO.

The security safeguards implemented for VSignals meet the policy and control requirements set forth in VSignalsSystem Security Plan (SSP), entitled FedRAMP-6500 Customer Security Plan – AWS GovCloud, and related electronically maintained System Security Plan found in the VSignals project VA eMASS repository.

The authorizing official has made a risk managed decision whether or not to authorize VSignals for operation basedon review of all security controls for VSignals, as documented in eMASS (also in the SSP), the Security Assessment (SAR), and Plan of Action and Milestones (POA&M). Upon receipt, the ATO Letter provides authorization to operate the information system leveraging the documented baseline security controls. VSignals is subject to ongoing monitoring consistent with applicable laws, regulations, agency policies, procedures and practices, throughout its lifecycle. VSignals shall operate at the enterprise level, in support of the Veterans Health Administration (VHA), Veterans Benefits Administration (VBA), and National Cemetery Administration (NCA).

The Initial Operational Standup Capacity for the VSignals system is as follows:
- Anonymous survey Creators / Modifiers (VA Internal): ≤ 300 users
- Dashboard / Reporting Consumers (VA Internal): ~ 350,000
- Respondents (Veterans and VA Employees) ≤ 5,000,000
- Case Management Users (VA Internal) ≤ 150,000

The following is a full list of related laws, regulations and policies and the 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

Section 1. Characterization of the Information

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

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

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

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

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

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

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

☐ Military History/Service Connection
☐ Next of Kin

☐ Other Data Elements (list below)

While surveys process out of the system, they're collected with the survey recipients: full name, email address, location, phone number, age/DOB, gender, and race.

PII Mapping of Components (Servers/Database)

VSignals consists of 3 key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by VSignals and the reasons for the collection of the PII are in the table below.

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

Internal Database Connections

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
CDW	Yes	Yes	Name, email, date of birth, mailing address and zip, race, gender, and phone	Veteran identifiers	Encrypted and travels via TIC
AWS GovCloud	Yes	Yes	Name, email, date of birth, mailing address and zip, race, gender, and phone. In additions unsolicited PII/PHI through open text fields.	Veteran identifiers. Unsolicited PII/PHI through open text fields.	Encrypted and travels via TIC

CxDW	Yes	Yes	Name, email, date of birth, mailing address and zip, race, gender, and phone. In additions unsolicited PII/PHI through open text fields.	Veteran identifiers	Encrypted and travels via TIC

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. The VSignals platform supports unique email anonymous survey invitations and web anonymous survey templates (HTML) including brand logo, coloring, fonts, and other styling elements or images that can be personalized and customized as required by VA. VSignals's email invitations are device sensitive, automatically adjusting to the viewing format based on device type (PC, tablet, mobile).Through VSignals eDelivery functionality provides full sample and quota management, reminder rules, and monitoring of delivery status. Feedless Web-Based: VSignals enables deployment for online anonymous survey taking, including untargeted "feedless" and "static link" approaches to conducting online anonymous surveys, including URL on receipt or artifact, QR code, and a URL at the end of an online chat session. These feedless methods are a common method for enabling Veterans to provide feedback. Social Media Feedback: Leveraging the VSignals technology, VSignals Social Media solution gathers content from location-based social media properties including Yelp, Google+ Local, Facebook, and Twitter. Local managers have the same filtering, reporting, visualization capabilities and similar closed-loop workflow functionality available for solicited feedback, making the platform the "one-stop-shop" for VA engagement with Veterans.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: VSignals system does not retrieve records by personal identifier. Any information in identifiable form or PII is not collected directly from individual. It is extracted from the CDW. The notices have already been provided at the point of collection before being stored in the CDW.

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 data that will support VSignals originates from the VA's Corporate Data Warehouse (CDW), a central data warehouse of VA clinical data for all VistA instances. CDW data extracts are loaded into VSignals where the data is grouped and sampled via rules created by the VA Veterans Experience Office.

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 veteran 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.

Feedback Collection: Given the many methods in which Veterans engage with VA, it is important that VA has the ability to distribute anonymous surveys via different modes in support of their numerous channels and touchpoints in addition to various device enablement. VSignals anonymous surveys comply to all mandated VA security requirements and are compatible for desktop, tablet, and mobile with kiosks. The data collection mode utilized shall at the time of requirements definition for each anonymous survey delivered based on factors such as the anonymous survey's target audience, desired response rates, anonymous survey length, and the measures and metrics required to achieve the VA's desired outcome.

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

Yes, VSignals creates reports based on services and benefits experience 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 in VA, deliver actionable intelligence to design service delivery, and respond quickly to concerns and recommendations and are sent to all 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 anonymous survey response data in VSignals will be collected by electronic modalities, open text/free-form feedback, closed-ended questions, social listening, short message service (SMS), and web intercepts. The frequency of how often a Veteran receives an anonymous survey is a combination of multiple factors: Opt Out, Last Time Anonymous survey Received, Anonymous survey Type.

Methods for collecting anonymous survey responses include:

• Sending anonymous surveys automatically based on telephone call received and logged by the customer service call center.
• Support web intercepts that integrate surveys with VA affiliated websites.
• Develop a survey response interface that will be embedded in other VA Applications.

• Generate and distribute anonymous surveys based on interactions with the VA, such as VAMC appointment check-out, interaction with VBMS, or other personal interface with the VA.
• Generate and distribute anonymous surveys to subsets of customers' demographic characteristics determined by VA end users.
• Email anonymous surveys directly, including individualized links, to respondents based on any criteria defined by VA end users.
• Feedbacks might include an additional activity where a veteran can leave comments on a section. These comments could potentially contain PII. These comments are exported to an Excel style format for review and action.

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: VSignals system does not retrieve records by personal identifier. Any information in identifiable form or PII is not collected directly from individual. It is extracted from the CDW. The notices have already been provided at the point of collection before being stored in the CDW

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

Not applicable. No information is collected using paperwork.

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 integrity checks are performed by the CDW prior to VSignals ingesting invitation files.

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.

DI-02.1 Data Integrity And Data Integrity Board: Not Applicable - Handled by Agency. Please see VSignals Privacy Controls.

1.4b If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.

Not applicable. 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

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.
• VA Directive and Handbook 6502, Privacy Program
• Executive Order 9397, Numbering System for Federal Accounts Relating to the Individual Persons
• Memorandum of Understanding (MOU)/Interconnection Security Agreement (ISA) between VA and SAIC*
• 5 U.S.C. 552a, "Privacy Act," c. 1974
• 5 U.S.C. 552, "Freedom of Information Act," c. 1967
• Federal Information Security Management Act (FISMA) of 2002
*VA can export the data stored in VSignals and retain it locally in order to meet VA/NARA retention requirements.

All data upon completion or termination of a contract will be turned over to VA and disposed of as soon as notice of the termination or completion is given.

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

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

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

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

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:

- Sensitive Personal Information (SPI) including personal contact information, SSN and medicalinformation may be released to unauthorized individuals.
- Unsecured Sensitive Personal Information (SPI) including personal contact information, SSN andmedical information may be exposed.
- Data breach at the facilities level.
- Data breach at the network level.

Mitigation:

- VSignals does not house SSN data within their system. For all other data, profile based permissions will govern what access users have access to. The profiles will be reviewedon a regular basis to ensure that appropriate information is shared with appropriate users. All employees with access to Veteran's information is required to complete the VA Privacy, Information Security Awareness trainingand Rules of Behavior annually.
- To mitigate this risk, VSignals protects data by ensuring that only authorized users can access it. Data security rules are assigned that determine which data users can access. All data is encrypted in transfer. Access is governed by strict password security policies. All passwords are stored in Secure Hash algorithm (SHA) 256 one-way hash format.
- To ensure the utmost privacy and security at the facility level, authorized personnel must pass through multiple levels of biometric and/or badge scanning to reach the VSignals system rooms/cages. All buildings are completely anonymous, with bullet-resistant exterior walls and embassy-grade concrete posts and planters around the perimeter. All exterior entrances feature silent alarm systems that notify law enforcement in the event of a suspected intrusion. Data is backed up. Backups do not physically leave the data center.
- Multilevel security products from leading security vendors and proven security practices ensure network security. To prevent malicious attacks through unmonitored ports, external firewalls allow only https traffic on port 443, along with Internet Control Message Protocol (ICMP) traffic. Switches ensure that the networkcomplies with the Request for Comment (RFC) 1918 standard, and address translation technologies further enhance network security. IDS sensors protect all network segments. Internal software systems are protected by two-factor authentication, along with the extensive use of technology that controls point of entry.

Section 2. Uses of the Information

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

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

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

Any information in identifiable form or PII that is collected directly from individual is accompanied by a notice stating data is used for service recovery, additional information on experience, and process improvement based on feedback. Data that is extracted from the CDW for the purpose of invitation file is covered by the issued privacy notices have already been provided at thepoint of collection before being stored in the CDW. While anonymous surveys process out of the system, they're collected with the anonymous survey recipients: **full name, email address, location, age, gender, and race.**
Data from CDW is used to process and send anonymous surveys from VSignals. Once the anonymous survey reaches VSignals, the anonymous surveys remain anonymous.
The personal identifiable information is extracted from the CDW, this data is sent through the Trusted Internet Connection(TIC) to AWS to be used to send anonymous surveys to Veteran's to request anonymous responses on their anonymous surveys with the VA. It is not sent to any third parties.

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.

Data analytic capabilities will be inherent in the Customer Experience Management (CEM) to provide insights in both quantitative and qualitative data using common trend and statistical analysis in addition to sentiment and text analytics.

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.

Every response within the VSignals system creates a new record. Veteran recipients of the surveys are only contacted if service recovery is required based on feedback given. Access to PII will be based on user role permissions within

the Vsignals System. User roles are determined granted based on the Vsignals access policies and procedures outline within the AC controls documented and maintained in the Vsignals eMASS system.

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?

Controls are in place to ensure data is used and protected in accordance with legal requirements, VA policies, and VA's stated purpose for using the data. Controls include mandatory training completion for all employees, volunteers, and contractors. Additionally, audits are performed to ensure information is accessed and retrieved appropriately. VA and SAIC have implemented required security and privacy controls for Federal information systems and organizations according to NIST SP 800-53 and VA Handbook 6500, Risk Management Framework for VA Information Systems. Per the approval of the Acting Assistant Secretary for information Technology Employees such as patient advocates who are responding to the Veterans, eligible dependents, each have undergone an extensive background check and has taken the required annual privacy training, as well as signed off on a rule of behavior.

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

Not applicable. No SSN collected by VSignals

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

VSignals is hosted in the FedRAMP High rated AWS GovCloud. Medallia (VSignals SaaS provider) maintains a FedRAMP ATO and a VA F-package within eMASS that outlines all OMB Memorandum M-06-15 safeguards and security mechanisms.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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

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

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

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

2.4a How is access to the PII determined?

Access to PII will be based on user role permissions within the VSignals System. User roles are determined granted based on the VSignals access policies and procedures outline within the AC controls documented and maintained in the VSignals eMASS system.

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

VSignals information system account types are limited to partner, and end user. The partner account requires Medallia configuration analyst training and certification prior to accessing the system and having configuration privileges. The end user requires a VSignals activated PIV card and results in the ability to view the data VSignals collects from Veterans. Once an end user is authorized to access VSignals additional role memberships must be requested through authorizing official and justification presented on why said role is needed. All access criteria, procedures, controls, and responsibilities are documented within the VSignals A&A (assessment and authorization) eMASS package.

2.4c Does access require manager approval?

VSignals information system account types are limited to partner, and end user. The partner account requires Medallia configuration analyst training and certification prior to accessing the system and having configuration privileges. The end user requires a VSignals activated PIV card and results in the ability to view the data VSignals collects from Veterans. Once an end user is authorized to access VSignals additional role memberships must be requested through authorizing official and justification presented on why said role is needed.

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

Access to the VSignals system is logged, reviewed, and audited by the Medallia FedRAMP authorized package and handled by the SaaS provider, Medallia. Frequency on which events are audited is also handled by the SaaS provider Medallia.

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

All safeguards for the VSignals system are established and maintained by the Medallia FedRAMP authorized package and handled by the SaaS provider, Medallia. Frequency on which safeguards are audited is also handled by the SaaS provider Medallia.

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

Any information in identifiable form or PII that is collected directly from individual is accompanied by a notice stating data is used for service recovery, additional information on experience, and process improvement based on feedback. Data that is extracted from the CDW for the purpose of invitation file is covered by the issued privacy notices have already been provided at thepoint of collection before being stored in the CDW. While anonymous surveys process out of the system, they're collected with the anonymous survey recipients: **full name, email address, physical address, date of birth, phone number gender, and race.**

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.*

Data is retained for 7 years as defined by the agency before being purged from the system. Any information in identifiable form or PII that is not collected directly from individual is extracted from the CDW. Information received from CDW is purged from the system after usage. Any issued privacy notices have already been provided at the point of collection before being stored in the CDW. Data is sent via Trusted Internet Connection to an S3 bucket within the VSignals system where it is then pulled into the system and processed. The data remains in the S3 bucket until the next round of data is pushed to the bucket at which point the deprecated data is removed. Data that is collected directly from the individual for use in service recovery will be retained for 7 years as defined by the agency before being purged from the system.

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

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

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

"The system complies with all VA retention and disposal procedures specified in VA Handbook 6300 and VA Directive 6500. Records contained in the system is retained for 7 years in accordance with NARA-approved retention schedule and Disposition Authority. https://www.archives.gov/files/records-mgmt/grs/grs04-2.pdf

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

"This system complies with all VA retention and disposal procedures specified in VA Handbook 6300 and VA Directive 6300. Records are retained according to Record Control Schedule 10-1 (reference: https://www.archives.gov/). Also see the General Record Schedule located here: https://www.archives.gov/files/records-mgmt/grs/grs04-2.pdf

3.4 What are the procedures for the elimination or transfer of SPI?

Explain how records are destroyed, eliminated or transferred to NARA at the end of their mandatory retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc.? This question is related to privacy control DM-2, Data Retention and Disposal.

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

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

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

Data is retained for 7 years as defined by the agency before being purged from the system. Any information in identifiable form or PII that is not collected directly from individual is extracted from the CDW. Information received from CDW is purged from the system after usage. Any issued privacy notices have already been provided at the point of collection before being stored in the CDW. Data is sent via Trusted Internet Connection to an S3 bucket within the VSignals system where it is then pulled into the system and processed. The data remains in the S3 bucket until the next round of data is pushed to the bucket at which point the deprecated data is removed. Data that is collected directly from the individual for use in service recovery will be retained for 7 years as defined by the agency before being purged from the system. Risk to privacy is minimized by limiting use of PII for service recovery only. PII is not used for testing or training and used in service recovery only by individuals that have the appropriate user access and ability to view PII are completing the proper VA trainings.

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: The VSignals systems' maintaining data within the VSignals longer than retention times require increases the risk that information can be compromised or breached. VSignals manages and retains data and information indefinitely and will only be removed from the system with authorization from the system owner. Data retained will include survey Configuration, survey Responses, survey Dimensions including the Organization Structure at the time of the survey, survey Users at the time of the survey, and the Invitations used to generate the survey. The breach or accidental release of VSignals data to inappropriate parties or the public will have Low impact on VA organizational operations, organizational assets, or individuals.

Mitigation: To mitigate the risk posed by information retention, any remaining data is pushed onto the S3 bucket in an automated process until the next round of data is pushed to the bucket at which point the deprecated data is removed.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

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

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

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

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

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

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

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

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
VA's Identity Access Management System VRM CRM AF	Provide the ability for personal with PIV card to gain access via Single Sign-on.	Name, email, date of birth, mailing address and zip, race, gender, phone, possible additional PII/PHI via open text boxes	HTTPS
VA Customer Experience Data Warehouse (CXDW)	This is the central repository for customer experience data.	Name, email, date of birth, mailing address and zip, race, gender, phone, possible additional PII/PHI via open text boxes	SFTP

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: The risk might include end users who do not log out of the VSignals tool when away from their computers or mobile devices. There is a risk that information may be shared with unauthorized VA personnel.

Mitigation: The tool 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, includingemployee 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, PersonalIdentification Numbers (PIN), encryption, and access authorization are all measures that are utilized for thesystem.

Section 5. External Sharing/Receiving and Disclosure

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

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

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

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

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

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

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

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

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are processed (shared/received/transmitted)with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
Amazon Web Services	VSignals is hosted in the AWS GovCloud	Full name, email address, location, phone number, age/DOB, gender, and race	ISA/MOU	Site to Site (S2S), IPSEC Tunnel, SecureFTP,
Microsoft Dynamics	Veteran Feedback generated from Survey, Call Center, or Social Media, VA Demographics, and Case updates	full name, email address, location, phone number, age/DOB, gender, and race.	ISA/MOU	VA Trusted Internet Connection

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

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

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

Follow the format below:

Privacy Risk: Data maintained outside of the Department and there is a risk that information may be accessed by an external organization or agency that does not have a need or legal authority to access VA data.

Mitigation: VA has contracted VSignals to deliver services that include maintaining VA data. A contract is in place that clearly articulates VSignals roles and responsibilities. Authorized personnel access user level data to provision and provide the VSignals service. Access is controlled by authentication and is restricted to authorized individuals. Security policies address the required security controls that must be followed in order to protect PII. The Interconnection Security Agreement (ISA) documentation is reviewed and updated annually to confirm that all security requirements are still being met and that no changes to the connections have occurred. The annual review can be done as part of the annual internal security assessment and third-party assessment. eMASS and other security documents must also be reviewed to ensure they accurately reflect the status of each item. VSignals utilizes VA onboarding processes to protect against unauthorized access to information within the system. All users must have an active PIV card and authenticate through IAM single-sign-on mechanisms.

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.

Veterans, Dependents of Veterans, and VA Beneficiary Survey Record (43VA008/ 86 FR 6992) https://www.oprm.va.gov/docs/SORN/Current_SORN_List_12_23_2022.pdf. Any information in identifiable form or PII that is collected directly from individual is accompanied by a notice stating data is used for service recovery, additional information on experience, and process improvement based on feedback. Data that is extracted from the CDW for the purpose of invitation file is covered by the issued privacy notices have already been provided at the point of collection before being stored in the CDW. A disclaimer warning will be displayed to all Veterans, and eligible dependents using VSignals requesting them not to provide PHI in open text comments. The surveys that do not solicit PII do not list where the information is going or why it is being collected since this info is provided already within an e-mail they receive which directs them to click a link that takes them to the survey web page.

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

Veterans, Dependents of Veterans, and VA Beneficiary Survey Record (43VA008/ 86 FR 6992). Veterans Signals (VSignals) follows the requirements of the Privacy Act (5 U.S.C. § 552a), which protects your personal information that the U.S. Department of Veterans Affairs (VA) maintains in systems of records. VSignals operates under the system of record outlined in 43VA008 Veterans, Dependents of Veterans, and Veteran Beneficiaries Survey Records. Any personally identifiable information that is collected from a survey respondent may be used for service recovery, additional information on experience, and process improvement based upon feedback. VSignals will not disclose your personal information to third parties outside of the VA without your consent, except to facilitate the transaction, to act on your behalf at your request, or as authorized by law.

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.

A disclaimer warning will be displayed to all Veterans, and eligible dependents using VSignals requesting them not to provide PHI in open text comments. The surveys that do not solicit PII do not list where the information is going or why it is being collected since this info is provided Any information in identifiable form or PII that is collected directly from individual is accompanied by a notice stating data is used for service recovery, additional information on experience, and process improvement based on feedback. Data that is extracted from the CDW for the purpose of invitation file is covered by the issued privacy notices have already been provided at thepoint of collection before being stored in the CDW.

A disclaimer warning will be displayed to all Veterans, and eligible dependents using VSignals requesting them not to provide PHI in open text comments. The surveys that do not solicit PII do not list where the information is going or why it is being collected since this info is provided already within an e-mail they receive which directs them to click a link that takes them to the survey web page.

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, the Veteran, and eligible dependents may elect to not provide feedback through VSignals. There is no penalty or denial of service, this is a voluntary service.

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.

VHA Handbook 1605.1 Appendix D 'Privacy and Release Information', section 5 lists the rights of the Veterans to request VHA to restrict the uses and/or disclosures of the individual's identifiable health information to carry out treatment, payment, or health care operations. The request must be in writing and adequately describe the specific information the individual believes to be inaccurate, incomplete, irrelevant, or untimely and the reason for this belief. The written request needs to be mailed or delivered to the VA health care facility that maintains the record.

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

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

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

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

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

<u>Privacy Risk:</u> There is a risk that members of the general public may not know that the VSignals

system exists within the Department of Veterans Affairs. This poses a low risk to the enterprise.

Mitigation: Upon login to VSignals web application and management console, all users will be presented with asystem notification banner which explicitly states that the user is entering a federal information system. This banner will inform the users that their actions are being monitored, recorded, and actively audited in accordancewith a system which is classified as FIPS 199 Moderate. Lastly, the banner will inform the user that only acceptable use, in accordance with the rules of behavior, is permitted. This banner shall be unconditionally displayed.

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.***

VHA Handbook 1605.1 Appendix D 'Privacy and Release Information', section 7(b) states the rights of the Veterans to request access to review their records. VA Form 10-5345a, Individual's Request For a Copy of Their Own Health Information, may be used as the written request requirement. All requests to review must be received by direct mail, fax, in person, or by mail referral from another agency or VA office. All requests for access must be delivered to, and reviewed by the System Manager for the concerned VHA system of records, the facility Privacy Officer, or their designee. Each request must be date stamped and reviewed to determine whether the request for access should be granted.

7.1b If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR).

N/A

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

N/A

7.2 What are the procedures for correcting inaccurate or erroneous information?

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed. If the correction procedures are the same as those given in question 7.1, state as much. This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

There is no facility in VSignals that enables an individual's responses to a survey to be changed once the survey responses are submitted. An individual may request to permanently opt-out of participating in surveys at any time as a capability within the survey generated by VSignals.

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.

No formal redress is provided to correcting information.

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

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

There is no facility in VSignals that enables an individual's responses to a survey to be changed once the survey responses are submitted. An individual may request to permanently opt-out of participating in surveys at any time as a capability within the survey generated by VSignals. Other data correction requests shall utilize the original system of record's standard data change/correction process depending on the original source of the invalid data.

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 VSignals system exists within the Department of Veterans Affairs. This poses a low risk to the enterprise. When VA collects personal datafrom 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 andposted on the VA Systems of Records website.

Mitigation: VA will collect only those personal data elements required to fulfill an official function or missiongrounded in law. Those collections will be conducted by lawful and fair means. VSignals shall follow the VA'sCode of Fair Information Principles. http://www.oprm.va.gov/docs/VA_Code_Of_Privacy_Principles.pdf

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.

VSignals information system account types are limited to partner, and end user. The partner account requires Medallia configuration analyst training and certification prior to accessing the system and having configuration privilege's. The end user requires a VSignals activated PIV card and results in the ability to

view the data VSignals collects from Veterans. All end user request are processed and approved by Ricardo Ruiz (VSignals Account manager.) Request process is done via sharepoint request form and information availability is based on user roles within the system.

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?

VSignals does not have any users from other agencies that have access to the system. The users with access have all completed the VA required privacy and HIPAA trainings as part of their onboarding process.

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.

VSignals information system account types are limited to partner, and end user. The partner account requires Medallia configuration analyst training and certification prior to accessing the system and having configuration privileges. The end user requires a VSignals activated PIV card and results in the ability to view the data VSignals collects from Veterans. All end user request are processed and approved by Ricardo Ruiz (VSignals Account manager.) Request process is done via SharePoint request form and information availability is based on user roles within the system

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.

System Administrator from Medallia and contractor for VA and maintains governing authority over all VSignals environments, where he maintains users, updates environments with system-level updates and new functionality, governs deployment activity and ensures user operability. The System Administrator is not a primary user of VSignals.VA product owner and COR approve all new or modified incoming or outgoing contracts involving VSignals. The contractors who provide support to the system are required to complete annual VA Privacy and Information Security and Rules of Behavior training via the VA's Talent Management System (TMS).

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.

VA Directive 6500 requires mandatory periodic training in computer security awareness and accepted computer security practices for all VA employees, contractors, and all other users of VA sensitive information and VA information systems. All members of the workforce are required to complete computer security training annually and must complete computer security awareness training before they can be authorized to access any VA computer system. Each site identifies personnel with significant information system security roles and responsibilities (i.e., management, system managers, system administrators, contracting staff, HR staff), documents those roles and responsibilities, and provides appropriate additional information system security training. Security training records will be monitored and maintained. The workforce will receive security awareness training annually as part of the Mandatory Training Program. In addition, the training for the tool will include awareness training regarding the possible existence of PII/PHI information submitted from the Veterans and eligible dependents. Each employee is asked to refresh their understanding of the appropriate way to handle the data.

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 Security Plan Status Date – 14 Feb 2022*
3. *The Authorization Status – Authority to Operate*
4. *The Authorization Date – 15 May 2022*
5. *The Authorization Termination Date – 14 May 2023*
6. *The Risk Review Completion Date – 09/14/2022*
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH) – Moderate*

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

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

N/A

Section 9 – Technology Usage

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

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

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

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

Veterans Signals is a Software as a Service (SaaS) application powered the Medallia customer experience management system. Medallia is a fully FedRAMP authorized system. Medallia is hosted externally in an AWS GovCloud.

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

Contract #: VA118-16-D-1002

Data delivered to Medallia or collected or accessed by Medallia on behalf of the VA in relation to the Program is owned by the Department of Veteran Affairs. Medallia (SaaS provider) has no ownership of Program Data contained within surveys and reports, including any modified versions of that data created through the use of the Medallia Solution contained within surveys and reports.

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.

Excluding all Program Data and all modified versions thereof, Medallia (CSP) owns surveys developed for the Program during the term of a Subscription, reports downloaded from the Medallia Solution during the term of a Subscription, and reports delivered by Medallia's customer experience management consulting organization, and Medallia grants SAIC (contractor) a non-exclusive, worldwide, sublicensable, assignable, and perpetual license to use, copy, and make derivative works based upon surveys and reports, in each instance for the limited purpose of supporting the Program.

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.
See contract language below:
The Contractor/Subcontractor must store, transport, or transmit VA sensitive information in an encrypted form, using VA-approved encryption tools that are, at a minimum, FIPS 140-2 validated. The Contractor/Subcontractor's firewall and Web services security controls, if applicable, shall meet or exceed VA's minimum requirements.

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).

There is no Robotics Process Automation in the Medallia GovCloud.

Section 10. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

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

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

Signature of Responsible Officials

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

Tonya L. Facemire 234776

Digitally signed by Tonya L. Facemire 234776
Date: 2023.01.12 12:58:25 -05'00'

Privacy Officer, Tonya Facemire

Faye D. Newman Engolia 150983

Digitally signed by Faye D. Newman Engolia 150983
Date: 2023.01.12 12:19:26 -06'00'

Information Systems Security Officer, Denise Engolia

Stefano Masi 474380

Digitally signed by Stefano Masi 474380
Date: 2023.01.17 11:23:46 -05'00'

Information Systems Owner, Stefano Masi

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).

Veterans, Dependents of Veterans, and VA Beneficiary Survey Record (43VA008/ 86 FR 6992)
https://www.oprm.va.gov/docs/SORN/Current_SORN_List_12_23_2022.pdf.

HELPFUL LINKS:

Record Control Schedules:

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

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

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

National Archives (Federal Records Management):

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

VHA Publications:

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

VA Privacy Service Privacy Hub:

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

Notice of Privacy Practice (NOPP):

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices