)E: 8320-01

DEPARTMENT OF VETERANS AFFAIRS

Privacy Act of 1974; Systems of Records

AGENCY: Office of Enterprise Integration (OEI), Department of Veterans Affairs (VA).

ACTION: Notice of a modified system of records.

SUMMARY: As required by the Privacy Act of 1974, notice is hereby given that VA is amending the system of records titled “Veterans, Dependents of Veterans, and VA Beneficiary Survey Records - VA” (43VA008) as set forth in the Federal Register. This system is used to collect data regarding the characteristics of America’s Veteran, Service member, family member, and beneficiary populations through surveys that may be augmented with information from several existing VA systems of records and with information from non-VA sources.

DATES: Comments on this modified system of records must be received no later than 30 days after date of publication in the Federal Register. If no public comment is received during the period allowed for comment or unless otherwise published in the Federal Register by VA, the modified system of records will become effective a minimum of 30 days after date of publication in the Federal Register. If VA receives public comments, VA shall review the comments to determine whether any changes to the notice are necessary.

ADDRESSES: Comments may be submitted through www.Regulations.gov or mailed to VA Privacy Service, 810 Vermont Avenue, NW, (005X6F), Washington, DC 20420. Comments should indicate that they are submitted in response to “Veterans, Dependents of Veterans, and VA Beneficiary Survey Records” (43VA008). Comments received will be available at regulations.gov for public viewing, inspection or copies.

FOR FURTHER INFORMATION CONTACT: OEI, Privacy Officer, VA, 810 Vermont Ave, NW, Washington, DC 20420; telephone 202-461-5800.

SUPPLEMENTARY INFORMATION:

VA is amending the System Location; Policies and Practices for Storage of Records; Policies and Practices for Retrieval of Records; Policies and Practices for Retention and Disposal of Records; Safeguards; System Manager; Record Access Procedures; Contesting Records Procedures; Notification Procedures; and Routine Uses.

System Location has been updated to add “Electronic records for “Veterans Signals” are stored within the Medallia FedRAMP High Rated AWS GovCloud. Cloud service hosting within the Amazon Web Service GovCloud primary sits in US-Gov-West-1 with duplication in US-Gov-West-2.”

Policies and Practices for Storage of Records is being updated to include “VSignals is implemented on Medallia GovCloud that is hosted on AWS GovCloud, though the physical segregation cannot be specified as it is a cloud implementation. VA sensitive information that includes health information is stored logically segregated and secured. All Medallia implemented VA programs are hosted within its own logically segregated VPC (virtual private cloud) and not shared with any other agency customer. The VSignals instance is implemented with its dedicated embedded database and that is only accessible via a specific application interface. Requestors of stored health and non-health information within VA, or from external individuals, contractors, organizations, and/or agencies with whom VA has a contract or agreement, must provide an equivalent level of security protection and comply with current VA policies and procedures for storage and transmission as codified in VA directives such as but not limited to VA Handbook 6500, *Information Security Program and* Handbook 6513 *Secured Connections.*”

Policies and Practices for Retrieval of Records is being updated to state “Records in this system are retrieved by name, address, social security number, date of

birth, military service number, claim or file number, Department of Defense identification numbers, or other personal identifiers.

Policies and Practices for Retention and Disposal of Records is being updated to state “Records are maintained and disposed of in accordance with the records disposition authority DAA-GRS-2016-0003-0002 approved by the Archivist of the United States, Records Control Schedule 10-1, Item number 150.”

Safeguards has been updated to include “VSignals does not allow physical and direct access to databases and storage devices. All access to data is via VA Single Sign On configuration on a web interface by authorized, certified VA employees who have been granted access through product owner approval.”

System Manager has been updated to state “OEI’s System Manager is Executive Director, Lisa Rosenmerkel, Lisa.Rosenmerkel@va.gov. Office of Enterprise Integration, Data Governance and Analytics (008B1), VA Central Office, 810 Vermont Avenue, NW. Washington, DC 20420.”

For Further Information Contact has been updated to include “Ronell.Smith@va.gov.”

Record Access Procedures has been updated to state “Individuals seeking information on the existence and content of records in this system pertaining to them should contact the system manager in writing as indicated above or may write or visit the VA facility location where they normally receive their care. A request for access to records must contain the requester’s full name, address, telephone number, and signature, and describe the records sought in sufficient detail to enable VA personnel to locate them with a reasonable amount of effort.”

Contesting Records Procedures has been updated to state “Individuals seeking to contest or amend records in this system pertaining to them should contact the system manager in writing as indicated above or may write or visit the VA facility location where

they normally receive their care. A request to contest or amend records must state clearly and concisely what record is being contested, the reasons for contesting it, and the proposed amendment to the record."

The Notification Procedure Section is being modified to state "Individuals who wish to be notified if a record in this system of records pertains to them should submit the request following the procedures described in "Record Access Procedures," above."

Routine uses are being modified to reflect current accepted language.

VA is republishing the system notice in its entirety.

SIGNING AUTHORITY

The Senior Agency Official for Privacy, or designee, approved this document and authorized the undersigned to sign and submit the document to the Office of the Federal Register for publication electronically as an official document of the Department of Veterans Affairs. Eddie Pool, Deputy Chief Information Officer, Connectivity and Collaboration Services, Performing the Delegable Duties of the Assistant Secretary for Information and Technology and Chief Information Officer, approved this document on July 1, 2025, for publication.

Dated: January 8, 2026.

Saurav Devkota,

Government Information Specialist,

VA Privacy Service,

Office of Compliance, Risk and Remediation,

Office of Information and Technology,

Department of Veterans Affairs.

SYSTEM NAME AND NUMBER: “Veterans, Dependents of Veterans, and VA Beneficiary Survey Records-VA” (43VA008)

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: Electronic records for this system are stored on VA’s servers, secured via the AWS GovCloud and physical servers housed at VA’s Austin Information Technology Center, 1615 Woodward St., Austin, Texas 78772. Electronic records for “Veterans Signals” are stored within the Medallia FedRAMP High Rated AWS GovCloud. Cloud service hosting within the Amazon Web Service GovCloud primary sits in US-Gov-West-1 with duplication in US-Gov-West-2. Records necessary for a contractor to perform under a VA-approved contract are located at the respective contractor’s facility.

SYSTEM MANAGER(S): OEI’s System Manager is Executive Director, Lisa Rosenmerkel, Lisa.Rosenmerkel@va.gov. Office of Enterprise Integration, Data Governance and Analytics (008B1), VA Central Office, 810 Vermont Avenue, NW, Washington, DC 20420.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 5 U.S.C. 306, 38 U.S.C. 527.

PURPOSE(S) OF THE SYSTEM: The purpose of this system of records is to collect data about the characteristics of America’s Veteran, Service member, family member, and beneficiary populations through surveys that may be augmented with information from several existing VA systems of records and with information from non-VA sources to:

1. Conduct statistical studies and analyses relevant to VA programs and services;
2. Plan and improve services provided;
3. Decide about VA policies, programs, and services;
4. Study VA’s role in the use of VA and non-VA benefits and services; and

5. Study the relationship between the use of VA benefits and services and the use of related benefits and services from non-VA sources. These types of studies are needed for VA to forecast future demand for VA benefits and services.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

1. Veterans;
2. Family members of veterans;
3. Military Service members;
4. Family members of Service members; and
5. Other VA beneficiaries.

CATEGORIES OF RECORDS IN THE SYSTEM:

The categories of records in the system contain information provided by veterans as well as their families, advocates, and dependents. Information is also obtained from other VA components, systems of records, and supplemented with information purchased from data brokers including:

1. Personal identifiers (e.g., respondents' names, addresses, phone numbers, social security numbers, employer identification numbers);
2. Demographic and socioeconomic characteristics (e.g., date of birth, sex, race/ethnicity, education, marital status, employment and earnings, financial information, business ownership information);
3. Military service information (e.g., military occupational specialties, periods of active duty, branch of service including National Guard or Reserves, date of separation, rank);
4. Health status information (e.g., diagnostic, health care utilization, cost, and third-party health plan information);
5. Benefit and service information (e.g., data on transition assistance services, VA medical and other benefit eligibility, awareness, knowledge,

understanding, and use; data on access and barriers to VA benefits or services; data about satisfaction with VA outreach, benefits, or services);

6. The records may also include information about Department of Defense (DoD) military personnel from DoD files (e.g., utilization files that contain inpatient and outpatient medical records, and eligibility files from the Defense Eligibility Enrollment Reporting System; and
7. The records may include information on Medicare beneficiaries from Centers for Medicare and Medicaid Services, and its predecessor, the Health Care Financing Administration, that are contained in databases (e.g., Denominator file identifies the population being studied; Standard Analytical files on inpatient, outpatient, physician supplier, nursing home, hospice, home care, durable medical equipment; and Group and other Health Plans).

RECORD SOURCE CATEGORIES: Information provided by veterans as well as their families, advocates, and dependents. Information is also obtained from other VA components, systems of records, and supplemented with information purchased from data brokers.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSE OF SUCH USES:

To the extent that records contained in the system include information protected by 45 C.F.R. 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 C.F.R. Parts 160, 161, and 164 permitting disclosure).

1. **NARA:** To the National Archives and Records Administration (NARA) in records management inspections conducted under 44 U.S.C. 2904 and 2906, or other functions authorized by laws and policies governing NARA operations and VA records management responsibilities.
2. **Contractors:** To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for VA, when reasonably necessary to accomplish an agency function related to the records.
3. **Law Enforcement Authorities, for Reporting Violations of Law:** To a Federal, state, local, territorial, tribal, or foreign law enforcement authority or other appropriate entity charged with the responsibility of investigating or prosecuting a violation or potential violation of law, whether civil, criminal, or regulatory in nature, or charged with enforcing or implementing such law, provided that the disclosure is limited to information that, either alone or in conjunction with other information, indicates such a violation or potential violation. The disclosure of the names and addresses of veterans and their dependents from VA records under this routine use must also comply with the provisions of 38 U.S.C. 5701(f).
4. **Federal Agencies, for Research:** To a Federal agency for the purpose of conducting research and data analysis to perform a statutory purpose of that agency upon the prior written request of that agency.
5. **Federal Agencies, for Computer Matches:** To other Federal agencies for the purpose of conducting computer matches to obtain information to determine or verify eligibility of veterans receiving VA benefits or medical care under title 38.
6. **Congress:** To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

7. **DOJ, Litigation, Administrative Proceeding:** To the Department Of Justice (DOJ), or in a proceeding before a court, adjudicative body, or other administrative body before which VA is authorized to appear, when any of the following is a party to such proceedings or has an interest in such proceedings, and VA determines that use of such records is relevant and necessary to proceedings:

    (a) VA or any component thereof;

    (b) Any VA employee in his or her official capacity;

    (c) Any VA employee in his or her individual capacity where DOJ has agreed to represent the employee; or

    (d) The United States, where VA determines that litigation is likely to affect the agency or any of its components is a party to such proceedings or has an interest in such proceedings, and VA determines that use of such records is relevant and necessary to the proceedings.

8. **Data Breach Response and Remediation, for VA:** To appropriate agencies, entities, and persons when (a) VA suspects or has confirmed that there has been a breach of the system of records, (b) VA has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, VA (including its information systems, programs, and operations), the Federal Government, or national security; and (c) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with VA's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

9. **Data Breach Response and Remediation, for Another Federal Agency:** To another Federal Agency or Federal entity, when VA determines that information from this system of records is reasonably necessary to assist the recipient

agency or entity in (a) responding to a suspected or confirmed breach or (b) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

10. **EEOC:** To the Equal Employment Opportunity Commission (EEOC) in connection with investigations of alleged or possible discriminatory practices, examination of Federal affirmative employment programs, or other functions of the Commission as authorized by law.
11. **FLRA:** To the Federal Labor Relations Authority (FLRA) in connection with the investigation and resolution of allegations of unfair labor practices, the resolution of exceptions to arbitration awards when a question of material fact is raised, matters before the Federal Service Impasses Panel, and the investigation of representation petitions and the conduct or supervision of representation elections.
12. **MSPB:** To the Merit Systems Protection Board (MSPB) in connection with appeals, special studies of the civil service and other merit systems, review of rules and regulations, investigation of alleged or possible prohibited personnel practices, and such other functions promulgated in 5 U.S.C. 1205 and 1206, or as authorized by law.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records in this system are stored on a segregated secure server. For data match purposes and data storage, all databases are placed on secured servers located at the following location: VA's Austin Information Technology Center, 615 Woodward Street, Austin, Texas 78772. Requestors of stored health and non-health information within VA, or from external individuals, contractors, organizations, and/or agencies with whom VA

has a contract or agreement, must provide an equivalent level of security protection and comply with current VA policies and procedures for storage and transmission as codified in VA directives such as but not limited to VA Handbook 6500, *Information Security Program and* Handbook 6513, *Secured Connections.*

VSignals is implemented on Medallia GovCloud that is hosted on AWS GovCloud, though the physical segregation cannot be specified as it is a cloud implementation. VA sensitive information that includes health information is stored logically segregated and secured. All Medallia implemented VA programs are hosted within its own logically segregated VPC (virtual private cloud) and not shared with any other agency customer. The VSignals instance is implemented with its dedicated embedded database and that is only accessible via a specific application interface. Requestors of stored health and non-health information within VA, or from external individuals, contractors, organizations, and/or agencies with whom VA has a contract or agreement, must provide an equivalent level of security protection and comply with current VA policies and procedures for storage and transmission as codified in VA directives such as but not limited to VA Handbook 6500, *Information Security Program* and Handbook 6513, *Secured Connections.*

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records in this system are retrieved by name, address, social security number, date of birth, military service number, claim or file number, DoD identification numbers, or other personal identifiers.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records are maintained and disposed of in accordance with the records disposition authority approved by the Archivist of the United States, General Records Schedule 4.2, 150.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

1. This list of safeguards furnished in this System of Record is not an exclusive list of measures that have been taken to protect individually identifiable information. The Health Insurance Portability and Accountability Act (HIPAA) provides guidelines for protecting health information that will be followed by adopting health care industry best practices and the reporting of breaches to provide adequate safeguards. Further, VA staff and contractors through mandatory data privacy and security training will review VA policy directives that specify the standards that will be applied to protect health information.
2. Access to data servers and storage areas is restricted to authorized VA employees or contract staff who the Office of Operations, Security, and Preparedness clears. Access codes are used to restrict and protect access to OEI data servers used for storage. Health information file areas are locked after normal duty hours and the Federal Protective Service and/or other security personnel protect VA facilities from outside access. VSignals does not allow physical and direct access to databases and storage devices. All access to data is via VA Single Sign On configuration on a web interface by authorized, certified VA employees that have been granted access through product owner approval.
3. Access to health information provided by the Veterans Health Administration pursuant to a Business Associate Agreement (BAA) is restricted to those OEI employees and contractors who have a business need for the information in the performance of their official duties. As a general rule, full sets of health care information are not provided for use unless the System Manager authorizes. File extracts provided for specific official uses will be limited to contain only the information fields needed for the analysis. Data used for analyses will have individual identifying characteristics removed whenever possible.

4. Security complies with applicable Federal Information Processing Standards (FIPS) issued by the National Institute of Standards and Technology (NIST). Health and non-health information files containing unique identifiers such as social security numbers are encrypted to NIST-verified FIPS 140-2 standard or higher for storage, transport, or transmission. Any health information files transmitted on laptops, workstations, data storage devices or media are encrypted. Record level files are always kept encrypted except when data is in immediate use. These methods are applied in accordance with HIPAA regulations and VA Handbook 6500, *Information Security Handbook.*
5. Contractors and their subcontractors are required to maintain the same level of security as VA staff for health care information that has been disclosed to them. Any data disclosed to a contractor, or use of a subcontractor to perform authorized analyses, requires use of Data Use Agreements or Memorandum of Understanding, Non-Disclosure Statements, and BAAs to protect health information. Unless VA explicitly authorizes in writing, sensitive or protected data made available to the contractor and subcontractors shall not be divulged or made known in any manner to any person. Other Federal or state agencies requesting health care information need to provide agreements to protect data.
6. The OEI work area is accessed for business-only needs. A limited amount of data is stored in a combination-protected safe which is secured inside a limited access room. Select individuals who possess background security clearances control direct access to the safe. Only a few employees with strict business needs or “need-to-know” access and completed background checks will ever handle the data once it is removed from the safe for data match purposes.
7. Data matches, analysis, and storage are conducted primarily on secured servers located in Austin, Texas, which are housed in a restricted access network area

with appropriate locking devices. Three measures control access to such records: the application of a VA security identification card coded with special permissions network area's keypad, the proper input of a series of individually unique passwords/codes by a recognized user, and the entrance of those select individuals for the performance of their official information technology-related duties.

8. Access to Automated Data Processing files, record level files, and related statistical software code is controlled by using an individually unique pin number or password entered in combination with a personally identifiable variable card or other information.
9. Access to VA facilities where identification codes, passwords, security profiles, and information on possible security violations are maintained and controlled at all hours by the Federal Protective Service, VA, or other security personnel and security access control devices.
10. Public use files prepared for purposes of research and analysis are purged of personal identifiers.
11. Paper records, when they exist, are maintained in a locked room at the Washington National Records Center or at designated locations identified in this System Notice. The Federal Protective Service protects paper records from unauthorized access.

RECORD ACCESS PROCEDURES: Individuals seeking information on the existence and content of records in this system pertaining to them should contact the system manager in writing as indicated above or may write or visit the VA facility location where they normally receive their care. A request for access to records must contain the requester's full name, address, telephone number, and signature, and describe the

records sought in sufficient detail to enable VA personnel to locate them with a reasonable amount of effort.

CONTESTING RECORD PROCEDURES: Individuals seeking to contest or amend records in this system pertaining to them should contact the system manager in writing as indicated above or may write or visit the VA facility location where they normally receive their care. A request to contest or amend records must state clearly and concisely what record is being contested, the reasons for contesting it, and the proposed amendment to the record.

NOTIFICATION PROCEDURES: Individuals who wish to be notified if a record in this system of records pertains to them should submit the request following the procedures described in “Record Access Procedures,” above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

HISTORY: 40 FR 38095 (August 26, 1975); 48 FR 52798 (November 22, 1983); 54 FR 20667 (May 12, 1989); 65 FR 61022 (October 13, 2000); 72 FR 17229 (April 6, 2007); 86 FR 6992 (January 25, 2021).

[FR Doc. 2026-00726 Filed: 1/14/2026 8:45 am; Publication Date: 1/15/2026]