



Privacy Act of 1974; Systems of Records

AGENCY: Department of Veterans Affairs (VA).

ACTION: Notice of Amendment to System of Records.

SUMMARY: As required by the Privacy Act of 1974, notice is hereby given that the Department of Veterans Affairs is amending the system of records currently entitled “Veterans, Dependents of Veterans, and VA Beneficiary Survey Records (43VA008)” as set forth in the Federal Register. VA is amending the System Manager, Notification Procedure, organizational information, updating existing Routine Uses to use VA standard language and adding Handbook for Secure Connections 6513. VA is republishing the system notice in its entirety.

DATES: This amended system of record will be effective **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN FEDERAL REGISTER]**

ADDRESSES: Written comments concerning the proposed amended system of records may be submitted by: mail or hand-delivery to Director, Regulations Management (02REG), Department of Veterans Affairs, 810 Vermont Avenue, N.W., Room 1068, Washington, DC 20420; fax to (202) 273-9026; or email to <http://www.Regulations.gov>. All comments received will be available for public inspection in the Office of Regulation Policy and Management, Room 1063B, between the hours of 8:00 a.m. and 4:30 p.m., Monday through Friday (except holidays). Please call (202) 461-4902 (this is not a toll-free number) for an appointment.

FOR FURTHER INFORMATION CONTACT: Office of Enterprise Integration (OEI), Privacy Officer, U.S. Department of Veterans Affairs, 810 Vermont Ave., NW., Washington, DC 20420; telephone (202) 461-5800.

SUPPLEMENTARY INFORMATION:

In the Routine Use Section existing language has been updated using approved VA language. No new routine uses have been added. Update included disaggregating previous Routine Use Four (4) for research and separating out the provision for matching with other federal agencies. This federal matching provision is Routine Use Number Five (5). Other Routine Uses have been renumbered.

In the System Location Section, the office has been amended from the Data Development and Analysis Service to the Office of Data Governance and Analysis, (008B1). To incorporate other organizational changes the System Manager has been changed to the Executive Director for Data Governance and Analysis. Also, the name of the Austin storage location has changed from Austin Automation Center to Austin Information Technology Center. Finally, the last sentence in the System Location Section has been amended for clarity to “records necessary for a contractor to perform under a VA-approved contract are located at the respective contractor’s facility.”

In the Authority for Maintenance of the System Section, P.L. 108 – 454 of 2004 has been removed. This Public Law authorized survey research for reporting requirements in Sections 211 and 805 that have expired.

In the Record Source Categories, language has been updated to include Centers for Medicare and Medicaid Services (CMS) to the list of entities from which information may be obtained.

The Policies and Practices for Storage have been amended to include the complete name and address of the OEI server location to be used for data storage at the VA Austin Information Technology Center, 615 Woodward St., Austin, TX, 78772. Further, VA has replaced rescinded Directive 6504 with its replacements, *VA Handbook 6500, Information Security Program*, and added *Handbook 6513 Secure Connections*.

In paragraph One (1) of the Physical, Procedural and Administrative Safeguards Section, the Health Insurance Portability and Accountability Act has been clarified. In

the paragraph Two (2) a VA organizational change edit was made to the Office of Operations, Security, and Preparedness and this paragraph was updated to reflect the current practice of storing data in a protected server environment.

In the Safeguards Section language has been updated. In paragraph Four (4) Directive 6504 has been replaced with *VA Handbook 6500, Information Security Program* to update and clarify security policy. Data handling to include both health and non-health data has been clarified.

The Safeguards section has included additional updates. Specifically, in the Safeguards Section Paragraph Five (5) Memorandum of Understanding (MOU) has been added to the possible agreements' types used to protect information. In addition, in Safeguards Section Paragraph Seven (7) update has been made to clarify and update the practice of using secure servers for data handling and analysis. Finally, in Section (8) language is updated and clarified to address access to record level files and related statistical software code as underlying survey data and resources.

In the System Manager(s) and Address(es) and Notification Procedure Sections, the office name has been amended from the Office of Policy and Planning, to the successor organization named the Office of Enterprise Integration (008). Titles of responsible System Notice officials in the new organization have been updated. Additionally, minor edits have been made to the System Notice for clarity, grammar, punctuation, and style. These changes are not substantive, and consequently, are not further discussed or enumerated.

The Report of Intent to Amend a System of Records Notice and an advance copy of the System Notice have been sent to the appropriate congressional committees and to the Director of the Office of Management and Budget (OMB) as required by 5 U.S.C. 552a(r) (Privacy Act) and guidelines issued by OMB (65 FR 77677), December 12, 2000.

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. James P. Gfrerer, Assistant Secretary of Information and Technology and Chief Information Officer, approved this document on April 30, 2020 for publication.

Dated: January 19, 2021.

Amy L. Rose,

Program Analyst,

VA Privacy Service,

Office of Information Security,

Office of Information and Technology,

Department of Veterans Affairs.

43VA008

SYSTEM NAME: “VETERANS, DEPENDENTS OF VETERANS, AND VA BENEFICIARY SURVEY RECORDS – VA”

SYSTEM LOCATION:

Location for electronic records are stored on the Department of Veterans Affairs’ secured servers housed at VA’s Austin Information Technology Center, 1615 Woodward St., Austin, TX, 78772. Records necessary for a contractor to perform under a VA-approved contract are located at the respective contractor’s facility.

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

PURPOSE(S): The purpose of this system of records is to collect data about the characteristics of America’s Veteran, Servicemember, 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 the 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 Servicemembers,
- (4) Family members of Servicemembers, and
- (5) Other VA beneficiaries.

RECORD SOURCE CATEGORIES:

The categories of records in the system may include:

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 (DEERS));

7. The records may include information on Medicare beneficiaries from Centers for Medicare and Medicaid Services (CMS), and its predecessor, the Health Care Financing Administration (HCFA), 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).

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 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).

1. NARA & GSA. VA may disclose information from this system to the National Archives and Records Administration (NARA) and General Services Administration (GSA) in records management inspections conducted under title 44, U.S.C.
2. Contractors. VA may disclose information from this system of records to individuals, organizations, private or public agencies, or other entities or individuals with whom VA has a contract or agreement to perform such services as VA may deem practicable for the purposes of laws administered by VA, in order for the contractor, subcontractor, public or private agency, or other entity or individual with whom VA has a contract or agreement to perform services under the contract or agreement.

3. Law Enforcement. VA may, on its own initiative, disclose information in this system, except the names and home addresses of veterans and their dependents, which is relevant to a suspected or reasonably imminent violation of law, whether civil, criminal or regulatory in nature and whether arising by general or program statute or by regulation, rule or order issued pursuant thereto, to a Federal, state, local, tribal, or foreign agency charged with the responsibility of investigating or prosecuting such violation, or charged with enforcing or implementing the statute, regulation, rule or order. On its own initiative, VA may also disclose the names and addresses of veterans and their dependents to a Federal agency charged with the responsibility of investigating or prosecuting civil, criminal or regulatory violations of law, or charged with enforcing or implementing the statute, regulation, rule or order issued pursuant thereto.
4. Research. VA may disclose information from this system to a Federal agency for the conduct of research and data analysis to perform a statutory purpose of that agency upon the prior written request of that agency, provided that there is legal authority under all applicable confidentiality statutes and regulations to provide the data and VA has determined prior to the disclosure that VA data handling requirements are satisfied.
5. Federal Agencies for Computer Matches. VA may disclose limited individual identification information to another Federal agency from this system for the purpose of matching and acquiring information held by that agency for VA to use for the purposes stated for this system of records.
6. Congress. VA may disclose information from the record of an individual in response to an inquiry from the congressional office made at the request of that individual.

7. Litigation. VA may disclose information from this system of records to the Department of Justice (DoJ), either on VA's initiative or in response to DoJ's request for the information, after either VA or DoJ determines that such information is relevant to DoJ's representation of the United States or any of its components in legal proceedings before a court or adjudicative body, provided that, in each case, the agency also determines prior to disclosure that release of the records to the DoJ is a use of the information contained in the records that is compatible with the purpose for which VA collected the records. VA, on its own initiative, may disclose records in this system of records in legal proceedings before a court or administrative body after determining that the disclosure of the records to the court or administrative body is a use of the information contained in the records that is compatible with the purpose for which VA collected the records.

To determine whether to disclose records under this routine use, VA will comply with the guidance promulgated by the Office of Management and Budget in a May 24, 1985, memorandum entitled "Privacy Act Guidance—Update," currently posted at <http://www.whitehouse.gov/omb/inforeg/guidance1985.pdf>.

8. Data breach response and remedial efforts. VA may, on its own initiative, disclose information from this system to appropriate agencies, entities, and persons when (1) VA suspects or has confirmed that the integrity or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of embarrassment or harm to the reputations of the record subjects, harm to economic or property interests, identity theft or fraud, or harm to the security, confidentiality, or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity)

that rely upon the potentially compromised information; and (3) the disclosure is to agencies, entities, or persons whom VA determines are reasonably necessary to assist or carry out the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

VA sensitive information that includes health information is 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 St., Austin, TX, 78772. Information that resides on a segregated server is kept inside a restricted network area behind cipher-locked doors with limited access. 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 RETRIEVABILITY OF RECORDS:

Health care information is kept separate from individual identifiers for survey data. Unique codes are assigned to individual health information. A codebook for decoding is stored on a secure server for name, social security number or other assigned identifiers of the individuals on whom they are maintained. These survey records may be 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 and the National Archives and Records Administration (NARA) and published in Agency Records Control Schedules. If the Archivist has not approved disposition authority for any records covered by the system notice, the System Manager will take immediate action to have the disposition of records in the system reviewed in accordance *with VA Handbook 6300.1, Records Management Procedures*. The records may not be destroyed until VA obtains an approved records disposition authority. See Records Control Schedule (RCS) 10-1 May 2016 for further detailed guidance. OEI destroys electronic files when no longer needed for administrative, legal, audit, or other operational purposes consistent with the Record Control Schedule. In accordance with 36 CFR 1234.34, *Destruction of Electronic Records*, “electronic records may be destroyed only in accordance with a records disposition schedule approved by the Archivist of the United States, including General Records Schedules.”

PHYSICAL, PROCEDURAL AND ADMINISTRATIVE SAFEGUARDS:

1. This list of safeguards furnished in this System of Record is not an exclusive list of measures that have been, or will be 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 in order to provide adequate safeguards. Further, VA policy directives that specify the standards that will be applied to protect health information will be reviewed by VA staff and contractors through mandatory data privacy and security training.

2. Access to data servers and storage areas is restricted to authorized VA employee or contract staffs who are cleared to work by the Office of Operations, Security, and Preparedness. Access to the OEI data servers used for storage is restricted and protected by access codes. Health information file areas are locked after normal duty hours. VA facilities are protected from outside access by the Federal Protective Service and/or other security personnel.
3. Access to health information provided by the Veterans Health Administration (VHA) 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 authorized by the System Manager. 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 kept encrypted at all times except when data is in immediate use. These methods are applied in accordance with HIPAA regulations [45 CFR 164.514] 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 (DUAs) or Memorandum of Understanding (MOU), Non-Disclosure Statements and Business Associates Agreement (BAA) to protect health information. Unless explicitly authorized in writing by the VA, 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. Direct access to the safe is controlled by select individuals who possess background security clearances. 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, TX, which are housed in a restricted access network area with appropriate locking devices. Access to such records are controlled by three measures: the application of a VA security identification card coded with special permissions network area’s key pad; 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 (ADP) 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 (PIV) card or other information.
9. Access to VA facilities where identification codes, passwords, security profiles and information on possible security violations are maintained is 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.

SYSTEM MANAGER(S) AND ADDRESS(ES):

OEI's System Manager is Kshemendra Paul, Executive Director, Office of Enterprise Integration, Data Governance and Analytics (008B1), VA Central Office, 810 Vermont Ave., NW. Washington, DC 20420, 202-461-1052, Kshemendra.Paul@va.gov.

RECORD ACCESS PROCEDURE:

An individual who wants to determine whether the Director, National Center for Veterans Analysis and Statistics (008B1) is maintaining a record under the individual's name or other personal identifier, or wants to determine the content of such records must submit a written request to the Director, National Center for Veterans Analysis and Statistics, Office of Enterprise Integration, (008B1), VA Central Office, 810 Vermont Ave., NW., Washington, DC 20420. The individual seeking this information must prove his or her identity and provide the name of the survey in question, approximate date of the survey, social security number, full name, and date of birth, telephone number, and return address. All inquiries must reasonably identify the health care information involved and the approximate date that medical care was provided.

CONTESTING RECORD PROCEDURES:

(See Records Access Procedures.)

NOTIFICATION PROCEDURE:

A Veteran who wishes to determine whether a record is being maintained by the Office of Enterprise Integration under his or her name or other personal identifier or wishes to determine the contents of such records should submit a written request or apply in person to: (1) Executive Director, Office of Enterprise Integration, (008B), VA Central Office, 810 Vermont Ave., NW., Washington, DC 20420. (2) Director, National Center for Veterans Analysis and Statistics, Office of Enterprise Integration, (008B1), VA Central Office, 810 Vermont Ave., NW. Washington, DC 20420. Inquiries should include the individual's full name and social security number.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

[FR Doc. 2021-01526 Filed: 1/22/2021 8:45 am; Publication Date: 1/25/2021]