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 1–14–26; 8:45 am]

BILLING CODE 8320–01–P

DEPARTMENT OF VETERANS AFFAIRS

Privacy Act of 1974; System of Records

AGENCY: Department of Veterans Affairs (VA).

ACTION: Notice of modified system of records.

SUMMARY: In accordance with the Privacy Act of 1974, the Department of Veterans Affairs (VA) is modifying the systems of records listed in this notice to incorporate one routine use related to the disclosure of records to the U.S. Department of the Treasury pursuant to

the Office of Management and Budget's Memorandum 25–32. The new routine use permits disclosures of records to the U.S. Department of the Treasury when the information is relevant to review payment and award eligibility through the Do Not Pay Working System for the purposes of identifying, preventing, or recouping improper payments to an applicant for, or recipient of, Federal funds. For full descriptions of the systems of records, please see the chart below for a list of the System of Records Notices (SORNs) and their corresponding **Federal Register** citations.

DATES: Comments on these modified systems of records must be received no later than 30 days after the notice's 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 received will be available at *regulations.gov* for public viewing, inspection or copies.

FOR FURTHER INFORMATION CONTACT: Rita Grewal, Acting Director, VA Privacy Service, *Rita.Grewal@va.gov,* 202–870–1284.

SUPPLEMENTARY INFORMATION: On August 20, 2025, the Office of Management and Budget published Memorandum 25–32, Preventing Improper Payments and Protecting Privacy Through Do Not Pay, which established the routine use for the disclosure of information relevant to reviewing payment and award eligibility through the Do Not Pay Working System for the purposes of identifying, preventing, or recouping improper payments to an applicant for, or recipient of, Federal funds. The Department of Veterans Affairs is now modifying all the systems of records identified in this notice to include the routine use set forth in OMB Memorandum M–25–32.

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. Merissa Larson, Acting Deputy Chief Information Officer, Compliance, Risk, and Remediation, Office of Information and Technology, and Chief Privacy Officer, Department of Veterans Affairs approved this document on September 19, 2025, for publication.

Dated: January 12, 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:

The systems of records to be modified by including the routine use described below in this notice are set forth below. Any history prior to the last publication in the **Federal Register** is omitted for clarity.

SORN No.	SORN name	**Federal Register** citation
54VA10	Veterans and Beneficiaries Purchased Care	90 FR 44473
36VA29	Veterans and Uniformed Services Personnel Programs of U.S. Government Life Insurance—VA	83 FR 44407
37VA27	Beneficiary Fiduciary Field System (BFFS)—VA	79 FR 41744
23VA10	Non-VA Care (Fee) Records—VA	90 FR 39485
186VA10D	Community Care (CC) Provider Profile Management System (PPMS)	86 FR 6979
17VA26	Loan Guaranty Fee Personnel and Program Participant Records—VA	88 FR 44462
13VA047	Individuals Submitting Invoice Vouchers for Payment and Accounting Transactional Data—VA	88 FR 60269
138VA005Q	Veterans Affairs/Department of Defense Identity Repository (VADIR)—VA	89 FR 99335
89VA10	Income Verification Records—VA	88 FR 17639
58VA/21/22/28	Compensation, Pension, Education, and Vocational Rehabilitation and Employment Records—VA	90 FR 44464
73VA10	Health Professional Scholarship Program, and Visual Impairment and Orientation and Mobility	88 FR 38131
44VA01	Veterans Appellate Records System—VA	88 FR 44185
208VA0478C	Payroll Processing and Reporting—VA	88 FR 63684
55VA26	Loan Guaranty Home Condominium and Manufactured Home Loan Applicants Records, Specially Adapted Housing Applicant Records and Vendee Loan Applicant Records—VA.	88 FR 63686
194VA189	PayVA (QCR) Debt Management	85 FR 84123
168VA005	Health Information Exchange—VA	89 FR 83949
131VA047	Corporate Travel and Charge Cards—VA	88 FR 63674
88VA244	Centralized Accounts Receivable System/Centralized Accounts Receivable On-Line System (CAR/CAROLS, combined system referred to as CAO).	83 FR 40140
165VA05CCSP	VA Child Care Subsidy Program Records—VA	89 FR 83949
114VA10	The Revenue Program—Billing and Collections Records—VA	86 FR 6996
197VA10	Caregiver Support Program—Caregiver Record Management Application (CARMA)	89 FR 6568

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

The applicable individual or office is identified in each notice.

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

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in the systems identified above may be disclosed outside VA as a routine use pursuant to 5 U.S.C. 552(a)(b)(3) as follows:

To the U.S. Department of the Treasury when disclosure of the information is relevant to review payment and award eligibility through the Do Not Pay Working System for the purposes of identifying, preventing, or recouping improper payments to an applicant for, or recipient of, Federal

funds, including funds disbursed by a state (meaning a state of the United States, the District of Columbia, a territory or possession of the United States, or a federally recognized Indian tribe) in a state-administered, federally funded program.

HISTORY:

See System Name and Number above.

[FR Doc. 2026–00682 Filed 1–14–26; 8:45 am]

BILLING CODE 8320–01–P

DEPARTMENT OF VETERANS AFFAIRS

[Docket No. VA–2025–VACO–0001]

Privacy Act of 1974; System of Records

AGENCY: Office of Inspector General, Department of Veterans Affairs.

ACTION: Rescindment of a system of records.

SUMMARY: As required by the Privacy Act of 1974, notice is hereby given that the Department of Veterans Affairs (VA) is rescinding the system of records (SOR) known as ''The Office of Inspector General Management Information System (MIS)—VA'' (71VA53), which consists of records and information about the Office of Inspector General (OIG) employees for various management and human resources objectives. DATES: Comments on this rescinded SOR must be received no later than 30 days after 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 rescindment will become effective a minimum of 30 days after the 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* under docket number VA–2025–VACO–0001 or mailed to VA Privacy Service (005X6F), 810 Vermont Avenue NW, Washington, DC 20420. Comments must indicate that they are submitted in response to the SOR known as ''The Office of Inspector General Management Information System (MIS)—VA'' (71VA53). Comments received will be available at *www.regulations.gov* for public viewing, inspection, or copies.

FOR FURTHER INFORMATION CONTACT: Chris Wilbur, Counselor to the Inspector General (50C), Office of Inspector General, *Chris.Wilbur@va.gov.*

SUPPLEMENTARY INFORMATION: This publication is in accordance with the Privacy Act requirement that agencies publish their amended SOR in the **Federal Register** when there is revision, change, or addition. VA OIG has reviewed its SOR notices and has determined its record system, known as ''The Office of Inspector General Management Information System (MIS)—VA'' (71VA53), should be rescinded to reflect evolving technology and procedures, to conform to current practice, and to reflect current authorities. The SOR is being rescinded because the records are maintained as part of Governmentwide SORs, including Office of Personnel Management (OPM) GOVT–1- General Personnel Records, and OPM GOVT–2- Employee Performance.

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 November 14, 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:

The Office of Inspector General Management Information System (MIS)—VA (71VA53).

HISTORY:

73 FR 56633 (Sep. 29, 2008); 84 FR 16138 (Apr. 17, 2019).

[FR Doc. 2026–00725 Filed 1–14–26; 8:45 am]

BILLING CODE 8320–01–P