Refinancing Loan Worksheet

Activity: Interest Rate Reduction

Agency Information Collection

Veterans Benefits Administration, Department of Veterans Affairs.

ACTION: Notice.

SUMMARY: Veterans Benefits Administration, Department of Veterans Affairs (VA), is announcing an opportunity for public comment on the proposed collection of certain information by the agency. Under the Paperwork Reduction Act (PRA) of 1995, federal agencies are required to publish notice in the Federal Register concerning each proposed collection of information, including each proposed extension of a currently approved collection, and allow 60 days for public comment in response to the notice.

DATES: Written comments and proposed collection of information should be received on or before October 18, 2021.

ADDRESS: Submit written comments on the collection of information through Federal Docket Management System (FDMS) at www.Regulations.gov or to Nancy J. Kessinger, Veterans Benefits Administration (20M33), Department of Veterans Affairs, 810 Vermont Avenue NW, Washington, DC 20420 or email to nancy.kessinger@va.gov. Please refer to “OMB Control No. 2900–0386” in any correspondence. During the comment period, comments may be viewed online through FDMS.

FOR FURTHER INFORMATION CONTACT: Maribel Aponte, Office of Enterprise and Integration, Data Governance Analytics (008), 1717 H Street NW, Washington, DC 20006, (202) 266–4688 or email maribel.aponte@va.gov. Please refer to “OMB Control No. 2900–0386” in any correspondence.

SUPPLEMENTARY INFORMATION: Under the PRA of 1995, federal agencies must obtain approval from the Office of Management and Budget (OMB) for each collection of information they conduct or sponsor. This request for comment is being made pursuant to Section 3506(c)(2)(A) of the PRA.

With respect to the following collection of information, VBA invites comments on: (1) Whether the proposed collection of information is necessary for the proper performance of VBA’s functions, including whether the information will have practical utility; (2) the accuracy of VBA’s estimate of the burden of the proposed collection of information; (3) ways to enhance the quality, utility, and clarity of the information to be collected; and (4) ways to minimize the burden of the collection of information on respondents, including through the use of automated collection techniques or the use of other forms of information technology.

Title: Interest Rate Reduction Refinancing Loan Worksheet (VA 26–923).
OMB Control Number: 2900–0386.
Type of Review: Revision.
Abstract: VA is revising this information collection to incorporate regulatory collection requirements previously captured under OMB control number 2900–0601. The purpose is to consolidate information collection requirements applicable only for interest rate reduction refinancing loans (IRRRLs) under one information collection package.

Affected Public: Individuals and households.
Estimated Annual Burden on Respondent: 30 minutes.
Frequency of Response: Response is generally one time per IRRRL.
Estimated Number of Respondents: 662,165.

By direction of the Secretary.

Maribel Aponte,
VA PRA Clearance Officer, Office of Enterprise and Integration/Data Governance Analytics, Department of Veterans Affairs.

DEPARTMENT OF VETERANS AFFAIRS

Privacy Act of 1974; System of Records

AGENCY: Veterans Health Administration, 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 the Department of Veterans Affairs (VA) is modifying the system of records entitled “Enrollment and Eligibility Records-VA” (147VA10NF1) as set forth in the Federal Register. This system of records notice is removing all elements of the Program of Comprehensive Assistance for Family Caregivers and the Program of General Caregiver Support Services established by the Caregivers and Veterans Omnibus Health Services Act of 2010, signed into law on May 5, 2010. Information pertaining to caregivers is now located within a new system of records entitled, “Caregiver Support Program-Caregiver Record Management Application (CARMa)-VA” (197VA10). VA is amending the system by revising the System Number; System Location; Categories of Individuals Covered by the System; System Manager; Record Source Categories; Routine Uses of Records Maintained in the System; Policies and Practices for Retrieval of Records; Policies and Practices for Retention and Disposal of Records; and Physical, Procedural, and Administrative Safeguards. VA is republishing the system notice in its entirety.

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.

DEPARTMENT OF VETERANS AFFAIRS

[OMB Control No. 2900–0386]

Agency Information Collection Activity: Interest Rate Reduction Refinancing Loan Worksheet

AGENCY: Veterans Benefits Administration, Department of Veterans Affairs.

ACTION: Notice.

SUMMARY: Veterans Benefits Administration, Department of Veterans Affairs (VA), is announcing an opportunity for public comment on the proposed collection of certain information by the agency. Under the Paperwork Reduction Act (PRA) of 1995, federal agencies are required to publish notice in the Federal Register concerning each proposed collection of information, including each proposed extension of a currently approved collection, and allow 60 days for public comment in response to the notice.

DATES: Written comments and proposed collection of information should be received on or before October 18, 2021.

Estimated Average Burden per Respondent: 30 minutes.
Frequency of Response: Frequency of response is generally one time per IRRRL.
Estimated Number of Respondents: 662,165.

By direction of the Secretary.

Maribel Aponte,
VA PRA Clearance Officer, Office of Enterprise and Integration/Data Governance Analytics, Department of Veterans Affairs.

[FR Doc. 2021–17530 Filed 8–16–21; 8:45 am]
BILLING CODE 8320–01–P
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, (005R1A), Washington, DC 20420. Comments should indicate that they are submitted in response to “Enrollment and Eligibility Records-VA (147VA10NF1)”. Comments received will be available at regulations.gov for public viewing, inspection or copies.

FOR FURTHER INFORMATION CONTACT: Stephanie Griffin, Veterans Health Administration (VHA) Privacy Officer, Department of Veterans Affairs, 810 Vermont Avenue NW, Washington, DC 20420; telephone (704) 245-2492 (Note: not a toll-free number).

SUPPLEMENTARY INFORMATION: The System Number will be changed from 147VA10NF1 to 147VA10 to reflect the current VHA organizational routing symbol.

The System Location and Record Source Categories are being updated to change 24VA10P2 to 24VA10A7 and 79VA10P2 to 79VA10.

Categories of Individuals Covered by the System is being amended to include non-Veteran, survivors, and VA Fourth Mission.

The System Manager is being amended to replace Chief Business Officer, 1722 I Street, with Deputy Under Secretary for Health and Operations, VHA Member Services 810 Vermont Avenue NW, Washington, DC 20420.

The Routine Uses of Records Maintained in the System has been amended by modifying the language in Routine Use #6 which states that disclosure of the records to the Department of Justice (DoJ) is a use of the information contained in the records that is compatible with the purpose for which VA collected the records. VA 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. This routine use will now state that VA may disclose information 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:

(a) VA or any component thereof;
(b) Any VA employee in his or her official capacity;
(c) Any VA employee in his or her official 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, provided, however, that in each case VA determines the disclosure is compatible with the purpose for which the records were collected. If the disclosure is in response to a subpoena, summons, investigative demand, or similar legal process, the request must meet the requirements for a qualifying law enforcement request under the Privacy Act, 5 U.S.C. 552a(b)(7), or an order from a court of competent jurisdiction under 552a(b)(11).

Routine Use #7 is being amended to remove General Services Administration.

Routine Use #13 has been amended by clarifying the language to state, “VA may disclose any information or records to appropriate agencies, entities, and persons when (1) VA suspects or has confirmed that there has been a breach of the system of records; (2) VA has determined that as a result of the suspected or confirmed breach there is a risk to individuals, VA (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, or persons reasonably necessary to assist in connection with VA efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.”

Routine Use #14 is being amended to include non-Veterans receiving VA medical care under VA’s Fourth Mission.

Routine Use #16 is being added to state, “VA may disclose information from this system of records 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 (1) responding to a suspected or confirmed breach or (2) 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.”

Policies and Practices for Retrievability of Records is being amended to include Electronic Data Interchange Personal Identifier (EDIPI).

Policies and Practices for Retention and Disposal of Records is being amended to remove HEC Records, Optical Disks or Other Electronic Medium will be temporarily deleted when all phases of the Veteran’s appeal rights have ended (ten years after the income year for which the means test verification was conducted) (N1–15–98–3, item 2). All Ad-Hoc reports created as part of this system shall be managed per NARA approved GRS 3.2 Items 030, Ad-Hoc reports. This section will include sections 1250.1 and 1250.2 and 1250.3; 1250.1 destroy 7 years after the income year for which the means test verification was conducted, when all phases of Veteran’s appeal rights have ended. If an appeal is filed, retain record until all phases of the appeal have ended; 1250.2, destroy 30 days after the data has been validated as being a true copy of the original data; and 1250.3, destroy when no longer needed.

Physical, Procedural, and Administrative Safeguards (Access) is being amended to replace the HEC Legacy system with Administrative Data Repository. Item 2 will include that employees are required to have completed “VA Privacy and Information Security Awareness and Rules of Behavior (VA 10176)” training, and “Privacy and HIPAA Focused Training (VA 10203)” to request and be granted access to the Enrollment Systems. There is also a user agreement notification that all users must attest.

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. Dominic A. Cussatt, Acting Assistant Secretary of Information and Technology and Chief Information Officer, approved this document on July 2, 2021 for publication.
Dated: August 11, 2021.

Amy L. Rose,
Program Analyst, VA Privacy Service, Office of Information Security, Office of Information and Technology, Department of Veterans Affairs.

SYSTEM NAME AND NUMBER:
Enrollment and Eligibility Records-VA (147VA10)

SECURITY CLASSIFICATION:
Unclassified.

SYSTEM LOCATION:
Records are maintained at the Health Eligibility Center (HEC) in Atlanta, Georgia; the Austin Information Technology Center (AITC) in Austin, Texas; at each VA health care facility as described in the VA system of records entitled “Patient Medical Records-VA” (24VA10A7); and at the Veteran Health Identification Card (VHIC) located at the AITC and 3M Cogent, Inc. Electronic and magnetic records are also stored at contracted facilities for storage and back-up purposes.

SYSTEM MANAGER(S):
Official responsible for policies and procedures: Deputy Under Secretary for Health and Operations, VHA Member Services (10NF), VA Central Office, 810 Vermont NW, Washington, DC 20420.

Official maintaining the system:
Director, Health Eligibility Center, 2957 Clairmont Road, Atlanta, GA 30329.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:
Title 28, United States Code, title 38, U.S.C., sections 501(a), 1705, 1710, 1722, and 5317.

PURPOSE(S) OF THE SYSTEM:
Information in this system of records is used to establish and maintain applicants’ records necessary to support the delivery of health care benefits; establish applicants’ eligibility for VA health care benefits; operate an annual enrollment system; provide eligible Veterans with an identification card; collect from an applicant’s health insurance provider for care of their non-service-connected conditions; provide educational materials related to VA health care benefits, respond to Veteran and non-Veteran inquiries related to VA health care benefits, and compile management reports.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:
The records contain information on individuals who have applied for or who have received VA health care benefits under Title 38 United States Code (U.S.C.), Chapter 17, the records also include Veterans, non-Veterans, caregivers, their spouses, dependents, and survivors as provided for in other provisions of Title 38, U.S.C or VA’s Fourth Mission.

CATEGORIES OF RECORDS IN THE SYSTEM:
The categories of records in this system may include: Medical benefit applications; eligibility and enrollment information, to include information obtained from Veterans Benefits Administration’s automated records, such as the “Compensation, Pension, Education and Rehabilitation Records-VA” (58VA21/22), and VHIC information including applicant’s name, address(es), date of birth, Member ID number—which is Department of Defense’s Electronic Data Interchange Personal Identifier (EDIP), Plan ID, special awards and Branch of Service, Internal Control Number (ICN), applicant’s image, preferred facility and facility requesting a VHIC, names, addresses and phone numbers of persons to contact in the event of a medical emergency, family information including spouse and dependent(s) name(s), address(es) and Social Security Number; applicant and spouse’s employment information, including occupation, employer(s) name(s) and address(es); financial information concerning the applicant and the applicant’s spouse including family income, assets, expenses, debts; third party health plan contract information, including health insurance carrier name and address, policy number and time period covered by policy; facility location(s) where treatment is provided; type of treatment provided (i.e., inpatient or outpatient); information about the applicant’s military service (e.g., dates of active duty service, dates and branch of service, and character of discharge, combat service dates and locations, military decorations, POW status and military service experience including exposures to toxic substances); information about the applicant’s eligibility for VA compensation or pension benefits, and the applicant’s enrollment status and enrollment priority group. These records also include, but are not limited to, individual correspondence provided to the HEC by Veterans, their family members and Veterans’ representatives, such as Veteran Service Officers (VSO); copies of death certificates; DD Form 214, “Certificate of Release or Discharge from Active Duty”; disability award letters; VA and other pension applications; VA Form 10–10EZ, “Application for Health Benefits”; VA Form 10–10EZR, “Health Benefits Renewal”; VA Form 10–10EC, “Application for Extended Care Services”; and workers compensation forms.

RECORD SOURCE CATEGORIES:
Information in the systems of records may be provided by the applicant; applicant’s spouse or other family members or accredited representatives or friends; Veterans, health insurance carriers; other Federal agencies; “Patient Medical Records-VA” (24VA10A7) system of records; “Veterans Health Information System and Technology Architecture (VistA) Records-VA” (29VA10); “Income Verification Records-VA” (89VA10NB); and Veterans Benefits Administration automated record systems, including “Veterans and Beneficiaries Identification and Records Location Subsystem-VA” (38VA23) and the “Compensation, Pension, Education and Rehabilitation Records-VA” (58VA21/22).

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:
To the extent that records contained in the system include information protected by 45 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 may not 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. VA may disclose information relevant to a claim of a Veteran or beneficiary, such as the name, address, the basis and nature of a claim, amount of benefit payment information, medical information, and military service and active duty separation information, only at the request of the claimant to accredited service organizations, VA-approved claim agents, and attorneys acting under a declaration of representation, so that these individuals can aid claimants in the preparation, presentation, and prosecution of claims under the laws administered by VA.

2. VA may disclose information that, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, to a Federal, state, local, territorial, tribal, or foreign law enforcement authority or other appropriate entity charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing such law. 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.

3. VA may disclose information in the course of presenting evidence to a court, magistrate, or administrative tribunal; in matters of guardianship, inquests, and commitments; to private attorneys representing Veterans rated incompetent in conjunction with issuance of Certificates of Incompetency; and to probation and parole officers in connection with court-required duties.

4. VA may disclose information to a fiduciary or guardian ad litem in relation to his or her representation of a claimant in any legal proceeding as relevant and necessary to fulfill the duties of the fiduciary or guardian ad litem.

5. VA may disclose information to attorneys, insurance companies, employers, third parties liable or potentially liable under health plan contracts, and courts, boards, or commissions as relevant and necessary to aid VA in the preparation, presentation, and prosecution of claims authorized by law.

6. VA may disclose information 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:
   (e) VA or any component thereof;
   (f) Any VA employee in his or her official capacity;
   (g) Any VA employee in his or her official capacity where DoJ has agreed to represent the employee;
   (h) 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.

7. VA may disclose information to 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.

8. VA may disclose name(s) and address(es) of present or former members of the armed services or their beneficiaries: (1) To a nonprofit organization if the release is directly connected with the conduct of programs and the utilization of benefits under Title 38, or (2) to any criminal or civil law enforcement governmental agency or any agency charged under applicable law with the protection of the public health or safety, if a qualified representative of such organization, agency, or instrumentality has made a written request for such name(s) or address(es) be provided for a purpose authorized by law, provided that the records will not be used for any purpose other than that stated in the request and that the organization, agency, or instrumentality is aware of the penalty provision of 38 U.S.C. 5701(f).

9. VA may disclose information as is reasonably necessary to identify such individual or concerning that individual’s indebtedness to the United States by virtue of the person’s participation in a benefits program administered by the Department, to a consumer reporting agency for the purpose of locating the individual, obtaining a consumer report to determine the ability of the individual to repay an indebtedness to the United States, or assisting in the collection of such indebtedness, provided that the provisions of 38 U.S.C. 57019(g)(2) and (4) have been met.

10. VA may disclose information 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.

11. VA may disclose information 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.

12. Disclosure to other Federal agencies may be made to assist such agencies in preventing and detecting possible fraud or abuse by individuals in their operations and programs.

13. VA may disclose any information or records to appropriate agencies, entities, and persons when (1) VA suspects or has confirmed that there has been a breach of the system of records; (2) VA has determined that as a result of the suspected or confirmed breach there is a risk to individuals, VA (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, or persons reasonably necessary to assist in connection with VA efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remediate such harm.

14. VA may disclose identifying information, including Social Security Number of Veterans, spouse(s) of Veterans, if married, children of Veterans, and non-Veterans may be disclosed to other Federal and/or State agencies for purposes of conducting computer matches, to obtain information to determine or verify eligibility of Veterans or non-Veterans who are receiving VA benefits or medical care under Title 38 U.S.C. or VA’s Fourth Mission.

15. VA may disclose the name and VHIC image of a missing patient from a VA health care facility to local law enforcement for the purpose of assisting in locating the missing patient.

16. VA may disclose information from this system 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 (1) responding to a suspected or confirmed breach or (2) 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.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records are maintained on magnetic tape, magnetic disk, optical disk and paper at the HEC, VHIC databases, VA medical centers, the 3M Cogent, Inc. databases, AITC, contract facilities, and at Federal Record Centers. In most cases, copies of back-up computer files are maintained at off-site locations and/or agencies with whom VA has a contract or agreement to perform such services, as VA may deem practicable.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records are retrieved by name, and/or Social Security Number, ICN, EDIPI, military service number, claim folder number, correspondence tracking number, internal record number, facility number, or other assigned identifiers of the individuals on whom they are maintained.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Per Records Control Schedule (RCS) 10–1 January 2020; use Health Eligibility Center disposition schedules 1250.1, 1250.2 and 1250.3. For 1250.1, destroy 7 years after the income year for which the means test verification was conducted, when all phases of Veteran’s appeal rights have expired. If an appeal is filed, retain record until all phases of the appeal have ended; 1250.2, destroy 30 days after the data has been validated and as a true copy of the original data; and 1250.3, destroy when no longer needed.
with an intrusion alarm system and a
security service vendor monitors the
system.
4. Contract employees are required to
sign a Business Associates Agreement as
required by the Health Insurance
Portability and Accountability Act
(HIPAA) Privacy Rule as
acknowledgement of mandatory
provisions regarding the use and
disclosure of protected health
information. Employee and contractor
access is deactivated when no longer
required for official duties or upon
termination of employment. Recurring
monitors are in place to ensure
compliance with nationally and locally
established security measures.
5. Beneficiary’s enrollment and
eligibility information is transmitted from
the Enrollment and Eligibility
information system to VA health care
facilities over the Department’s secure
computerized electronic
communications system.
6. Only specific key staff have
authorized access to the computer room.
Programmer access to the information
systems is restricted only to staff whose
official duties require that level of
access.
7. On-line data reside on magnetic
media in the HEC and AITC computer
rooms that are highly secured. Backup
media are stored in the computer room
within the same building and only
information system staff and designated
management staff have access to the
computer room. On a weekly basis,
backup media are stored in off-site
storage by a media storage vendor. The
vendor picks up and returns the media in
a locked storage container; vendor
personnel do not have key access to the
locked container. The AITC has
established a backup plan for the
Enrollment system as part of a required
Certification and Accreditation of the
information system.
8. Any sensitive information that may
be downloaded to personal computers
or printed to hard copy format is
provided the same level of security as
the electronic records. All paper
documents and informal notations
containing sensitive data are shredded
prior to disposal. All magnetic media
(primary computer system) and personal
computer disks are degauged prior to
disposal or release off-site for repair.
The VHIC contractor destroys all
Veteran identification data 30 days after
the VHIC card has been mailed to the
Veteran in accordance with contractual
requirements.
9. All new HEC employees receive
initial information security and privacy
training; refresher training is provided
to all employees on an annual basis. The
HEC’s Information Security Officer
performs an annual information security
audit and periodic reviews to ensure
security of the system. This annual
audit includes the primary computer
information system, the
telecommunication system, and local
area networks. Additionally, the
Internal Revenue Service performs
periodic on-site inspections to ensure
the appropriate level of security is
maintained for Federal tax data.
10. Identification codes and codes
used to access Enrollment and
Eligibility information systems and
records systems, as well as security
profiles and possible security violations,
are maintained on magnetic media in a
secure environment at the Center. For
contingency purposes, database backups
on removable magnetic media are stored
off-site by a licensed and bonded media
storage vendor.
11. Contractors, subcontractors, and
other users of the Enrollment and
Eligibility Records systems will adhere
to the same safeguards and security
requirements to which HEC staff must
comply.

ACCESS:
1. In accordance with national and
locally established data security
procedures, access to enrollment
information databases (Administrative
Data Repository) is controlled by unique
entry codes (access and verification
codes). The user’s verification code is
automatically set to be changed every 90
days. User access to data is controlled
by role-based access as determined
necessary by supervisory and
information security staff as well as by
management of option menus available
to the employee. Determination of such
access is based upon the role or position
of the employee and functionality
necessary to perform the employee’s
assigned duties.
2. Employees are required to have
completed “VA Privacy and Information
Security Awareness and Rules of
Behavior (VA 10176)” training, and
“Privacy and HIPAA Focused Training
(VA 10203)” to request and be granted
access to the Enrollment Systems. There
is also a user agreement notification that
all users must attest to, acknowledging
understanding of privacy and
confidentiality requirements before
gaining access to the system. In
addition, all employees receive annual
privacy awareness and information
security training. Access to electronic
records is deactivated when no longer
required for official duties. Recurring
monitors are in place to ensure
compliance with nationally and locally
established security measures.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL
SAFEGUARDS:
1. Data transmissions between VA
health care facilities, the Health
Eligibility Center (HEC), the AITC, 3M
Cogent, Inc. databases are accomplished
using the Department’s secure wide area
network. The software programs
automatically flag records or events for
transmission based upon functional
requirements. Server jobs at each facility
run continuously to check for data to be
transmitted and/or incoming data which
needs to be parsed to files on the
receiving end. All messages containing
data transmissions include header
information that is used for validation
purposes. The recipients of the
messages are controlled and/or assigned
to the mail group based on their role or
position. Consistency checks in the
software are used to validate the
transmission and electronic
acknowledgment messages are returned
to the sending application. VA’s Office
of Cyber Security has oversight
responsibility for planning and
implementing computer security.
2. Working spaces and record storage
areas at HEC. Austin Information
Technology Center, and the Veteran
Health Identification Card (VHIC)
processing locations are secured during
all business hours, as well as during
non-business hours. All entrance doors
require an electronic pass card, for entry
when unlocked, and entry doors are
locked outside normal business hours.
Visitors to the HEC are required to
present identification, sign-in at a
specified location, and are issued a pass
card that restricts access to non-
sensitive areas. Visitors to the HEC are
escorted by staff through restricted
areas. At the end of the visit, visitors are
required to turn in their badge. The
building is equipped with an intrusion
alarm system, which is activated during
non-business hours. This alarm system
is monitored by a private security
service vendor. The office space
occupied by employees with access to
Veteran records is secured with an
electronic locking system, which
requires a card for entry and exit of that
office space. Access to the AITC is
generally restricted to AITC staff, VA
Central Office employees, custodial
personnel, Federal Protective Service
and authorized operational personnel
through electronic locking devices. All
other persons gaining access to the
computer rooms are escorted.
3. Access to the VHIC contractor
secured work areas is also controlled by
electronic entry devices, which require a
card and/or input for entry and exit of the
production space. The VHIC
contractor’s building is also equipped

4. Beneficiary’s enrollment and
eligibility information is transmitted from
the Enrollment and Eligibility
information system to VA health care
facilities over the Department’s secure
computerized electronic
communications system.
6. Only specific key staff have
authorized access to the computer room.
Programmer access to the information
systems is restricted only to staff whose
official duties require that level of
access.
7. On-line data reside on magnetic
media in the HEC and AITC computer
rooms that are highly secured. Backup
media are stored in the computer room
within the same building and only
information system staff and designated
management staff have access to the
computer room. On a weekly basis,
backup media are stored in off-site
storage by a media storage vendor. The
vendor picks up and returns the media in
a locked storage container; vendor
personnel do not have key access to the
locked container. The AITC has
established a backup plan for the
Enrollment system as part of a required
Certification and Accreditation of the
information system.
8. Any sensitive information that may
be downloaded to personal computers
or printed to hard copy format is
provided the same level of security as
the electronic records. All paper
documents and informal notations
containing sensitive data are shredded
prior to disposal. All magnetic media
(primary computer system) and personal
computer disks are degauged prior to
disposal or release off-site for repair.
The VHIC contractor destroys all
Veteran identification data 30 days after
the VHIC card has been mailed to the
Veteran in accordance with contractual
requirements.
9. All new HEC employees receive
initial information security and privacy
training; refresher training is provided
to all employees on an annual basis. The
HEC’s Information Security Officer
performs an annual information security
audit and periodic reviews to ensure
security of the system. This annual
audit includes the primary computer
information system, the
telecommunication system, and local
area networks. Additionally, the
Internal Revenue Service performs
periodic on-site inspections to ensure
the appropriate level of security is
maintained for Federal tax data.
10. Identification codes and codes
used to access Enrollment and
Eligibility information systems and
records systems, as well as security
profiles and possible security violations,
are maintained on magnetic media in a
secure environment at the Center. For
contingency purposes, database backups
on removable magnetic media are stored
off-site by a licensed and bonded media
storage vendor.
11. Contractors, subcontractors, and
other users of the Enrollment and
Eligibility Records systems will adhere
to the same safeguards and security
requirements to which HEC staff must
comply.

ACCESS:
1. In accordance with national and
locally established data security
procedures, access to enrollment
information databases (Administrative
Data Repository) is controlled by unique
entry codes (access and verification
codes). The user’s verification code is
automatically set to be changed every 90
days. User access to data is controlled
by role-based access as determined
necessary by supervisory and
information security staff as well as by
management of option menus available
to the employee. Determination of such
access is based upon the role or position
of the employee and functionality
necessary to perform the employee’s
assigned duties.
2. Employees are required to have
completed “VA Privacy and Information
Security Awareness and Rules of
Behavior (VA 10176)” training, and
“Privacy and HIPAA Focused Training
(VA 10203)” to request and be granted
access to the Enrollment Systems. There
is also a user agreement notification that
all users must attest to, acknowledging
understanding of privacy and
confidentiality requirements before
gaining access to the system. In
addition, all employees receive annual
privacy awareness and information
security training. Access to electronic
records is deactivated when no longer
required for official duties. Recurring
monitors are in place to ensure
compliance with nationally and locally
established security measures.
3. Users access to the VHIC database utilizes the national NT network authentication infrastructure. The external VHIC vendor utilizes the One-VA Virtual Private Network secured connection for access to VHIC records.

4. Strict control measures are enforced to ensure that access to and disclosure from all records is limited to VA and the contractor’s employees whose official duties warrant access to those files.

5. As required by the provisions of the HIPAA Privacy Rule, 45 CFR parts 160 and 164, access to records by HEC employees is classified under functional category “Eligibility and Enrollment Staff.”

RECORD ACCESS PROCEDURES:
Individuals seeking information regarding access to and contesting of Enrollment and Eligibility Records may write to the Director, Health Eligibility Center, 2957 Clairmont Road, Atlanta, GA 30329.

CONTESTING RECORD PROCEDURES:
(See Record Access Procedures above.)

NOTIFICATION PROCEDURES:
Any individual who wishes to determine whether a record is being maintained in this system under his or her name or other personal identifier, or wants to determine the contents of such record, should submit a written request or apply in person to the Health Eligibility Center. All inquiries must reasonably identify the records requested. Inquiries should include the individual’s full name, Social Security number, military service number, claim folder number and return address.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:
None.

HISTORY:
Last full publication provided in 81 FR 45597 dated July 14, 2016.

[FR Doc. 2021–17528 Filed 8–16–21; 8:45 am]

BILLING CODE 8320–01–P

DEPARTMENT OF VETERANS AFFAIRS

[OMB Control No. 2900–0740]

Agency Information Collection Activity: Application for Chapter 23 Burial Benefits

AGENCY: Veterans Benefits Administration, Department of Veterans Affairs.

ACTION: Notice.

SUMMARY: Veteran’s Benefits Administration (VBA), Department of Veterans Affairs (VA), is announcing an opportunity for public comment on the proposed collection of certain information by the agency. Under the Paperwork Reduction Act (PRA) of 1995, Federal agencies are required to publish notice in the Federal Register concerning each proposed collection of information, including each proposed currently approved collection, and allow 60 days for public comment in response to the notice.

DATES: Written comments and recommendations on the proposed collection of information should be received on or before October 18, 2021.

ADDRESS: Submit written comments on the collection of information through Federal Docket Management System (FDMS) at www.Regulations.gov or to Nancy J. Kessinger, Veterans Benefits Administration (20M33), Department of Veterans Affairs, 810 Vermont Avenue NW, Washington, DC 20420 or email nancy.kessinger@va.gov. Please refer to “OMB Control No. 2900–0740” in any correspondence. During the comment period, comments may be viewed online through FDMS.

FOR FURTHER INFORMATION CONTACT:
Maribel Aponte, Office of Enterprise and Integration/Data Governance Analytics (008), 1717 H Street NW, Washington, DC 20006, (202) 266–4688 or email maribel.aponte@va.gov. Please refer to “OMB Control No. 2900–0740” in any correspondence.

SUPPLEMENTARY INFORMATION: Under the PRA of 1995, Federal agencies must obtain approval from the Office of Management and Budget (OMB) for each collection of information they conduct or sponsor. This request for comment is being made pursuant to Section 3506(c)(2)(A) of the PRA.

With respect to the following collection of information, VBA invites comments on: (1) Whether the proposed collection of information is necessary for the proper performance of VBA’s functions, including whether the information will have practical utility; (2) the accuracy of VBA’s estimate of the burden of the proposed collection of information; (3) ways to enhance the quality, utility, and clarity of the information to be collected; and (4) ways to minimize the burden of the collection of information on respondents, including through the use of automated collection techniques or the use of other forms of information technology.

Authority: 38 U.S.C. 5121A.
Title: Request for Substitution of Claimant Upon Death of Claimant.

OMB Control Number: 2900–0740.
Type of Review: Extension Without Change of a Previously Approved Collection.

Abstract: VA Form 21P–0847 is used to allow claimants to request substitution for a claimant, who passed away, prior to VA processing a claim to completion. This is only allowed when a claimant dies while a claim or appeal for any benefit under a law administered by the VA is pending. The substitute claimant would be eligible to receive accrued benefits due a deceased claimant under Section 5121(a).

AFFECTED PUBLIC: Individuals and households.
Estimated Annual Burden: 1,667 hours.
Estimated Average Burden per Respondent: 5 minutes.
Frequency of Response: Once.
Estimated Number of Respondents: 20,000.

By direction of the Secretary.

Maribel Aponte,
VA PRA Clearance Officer, Office of Enterprise and Integration/Data Governance Analytics, Department of Veterans Affairs.

[FR Doc. 2021–17622 Filed 8–16–21; 8:45 am]

BILLING CODE 8320–01–P

DEPARTMENT OF VETERANS AFFAIRS

[OMB Control No. 2900–NEW]

Agency Information Collection Activity: Request for Substitution of Claimant Upon Death of Claimant (VA Form 21P–0847)

AGENCY: Veterans Benefits Administration, Department of Veterans Affairs.

ACTION: Notice.

SUMMARY: Veteran’s Benefits Administration (VBA), Department of Veterans Affairs (VA), is announcing an opportunity for public comment on the proposed collection of certain information by the agency. Under the Paperwork Reduction Act (PRA) of 1995, Federal agencies are required to publish notice in the Federal Register concerning each proposed collection of information, including each proposed currently approved collection, and allow 60 days for public comment in response to the notice.

DATES: Written comments and recommendations on the proposed collection of information should be received on or before October 18, 2021.

ADDRESS: Submit written comments on the collection of information through Federal Docket Management System (FDMS) at www.Regulations.gov or to