a limited number of system administrators and database administrators. In addition, VTA has undergone certification and accreditation. Users of VTA access the system via AccessVA. Users must also register through VTA and obtain a VTA Account. Within the VTA system, users are designated a role which determines their access to specific data. Based on a risk assessment that followed National Institute of Standards and Technology Vulnerability and Threat Guidelines, the system is considered stable and operational. VTA has received a final Authority to Operate (ATO). The system was found to be operationally secure, with very few exceptions or recommendations for change.

RECORD ACCESS PROCEDURES:

(See notification procedure below.)

CONTESTING RECORD PROCEDURES:

(See notification procedure below.)

NOTIFICATION PROCEDURES:

Individuals seeking information on the existence and content of a record pertaining to them should contact the system manager, in writing, at the above address. Requests should contain the full name, address and telephone number of the individual making the inquiry.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

Not Applicable.

HISTORY:

This SORN was originally published in the **Federal Register** on April 19, 2012, 77 FR 23543. The SORN was subsequently amended in the **Federal Register** on April 15, 2014, 79 FR 21352.

[FR Doc. 2021–09084 Filed 4–29–21; 8:45 am]

BILLING CODE P

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 amending the system of records entitled, ''Ionizing Radiation Registry-VA'' (69VA131). VA is amending the system of records by revising the System Number; System Location; System Manager; Authority for Maintenance of the System; Routine Uses of Records Maintained in the System; Policies and Practices for Storage of Records; Policies and Practices for Retention and Disposal of Records; Physical, Procedural and Administrative Safeguards; Record Access Procedures; and Notification Procedure. VA is republishing the system notice in its entirety.

DATES: Comments on this amended system of records must be received no later than June 1, 2021. If no public comment is received during the period allowed for comment or unless otherwise published in the **Federal Register** by the VA, the modified system will become effective June 1, 2021. 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 ''Ionizing Radiation Registry-VA (69VA131)''. Comments received will be available at regulations.gov for public viewing, inspection or copies.

FOR FURTHER INFORMATION CONTACT: Stephania 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 69VA131 to 69VA10 to reflect the current VHA organizational routing symbol.

The System Location is being updated to replace Austin Automation Center (AAC) with Austin Information Technology Center (AITC). Environmental Agents Service (131) is being replaced with Post Deployment Health Services (10P4Q). Also, since optic readers, paper, or disk copies are no longer used or maintained, this section is being updated to remove, ''The secure web-based data entry system is maintained by the AAC and provides retrievable images to users. The optical disk system is currently being utilized where there is no access to the secure web-based system. However, the optical disk system is scheduled to be discontinued in 2004 and all access to the Ionizing Radiation Registry (IRR) system will be through the secure web-based data entry system.''

The System Manager, Record Access Procedures, and Notification Procedure are being updated to replace, ''Program Chief for Clinical Matters, Office of Public Health and Environmental Hazards (13) (for clinical issues) and Management/Program Analyst, Environmental Agents Service (131) (for administrative issues)'' with Deputy Chief Consultant, Post Deployment Health Services (10P4Q). Telephone number (202) 266–4511 (Note: this is not a toll-free number).

Authority for Maintenance of the System is being amended to include Title 38, United States Code 527, 1116, Public Law 102–585 Section 703, and Public Law 100–687.

The Routine Uses of Records Maintained in the System is being updated to replace Joint Commission for Accreditation of Healthcare Organizations (JCAHO) to The Joint Commission in Routine use #10.

The language in Routine Use #11 is being amended which states that disclosure of the records to the U.S. 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 #13 has been updated 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 is 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 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 Storage of Records is updated to remove ''In 2003, the data collection process moved to a secure web-based system. Data previously recorded manually and converted to electronic format is now input through the secure VA Intranet system. Data is stored on a web server hosted by the AAC and is retrievable by the facility. Three levels of access are provided for the data that is input, using password security linked to the AAC Top Secret Security system, with mandated changes every 90 days. Data from individual facilities is uploaded nightly and stored on Direct Access Storage Devices at the AAC, Austin, Texas, and on optical disks at VA Central Office, Washington, DC. AAC stores registry tapes for disaster back up at an off-site location. VA Central Office also has back-up optical disks stored off-site. In addition to electronic data, registry reports are maintained on paper documents and microfiche. The optical disk system is currently being utilized where there is no access to the secure web- based system. The optical disk system is scheduled to be discontinued in 2004 and all access to the IRR system will be through the secure web-based data entry system. Records will be maintained and disposed of in accordance with records disposition authority approved by the Archivist of the United States.'' This section is updated to state that all registry data is stored electronically in the registry database.

Policies and Practices for Retention and Disposal of Records is being updated to remove Records will be maintained and disposed of in accordance with records disposition authority approved by the Archivist of the United States. This section is updated to state that currently these records are maintained as a permanent record, pending approval of a new records schedule by the National Archives and Records Administration (NARA). These permanent records will transfer to NARA in 5-year blocks, until scheduled.

The Physical, Procedural and Administrative Safeguards section is being updated to remove, ''Data is securely located behind the VA firewall and only accessible from the VA Local Area Network (LAN) through the VA Intranet. Read access to the data is granted through a telecommunications network to authorized VA Central Office personnel. AAC reports are also accessible through a telecommunications network on a read-only basis to the owner (VA facility) of the data. Access is limited to authorized employees by individually unique access codes which are changed periodically. Physical access to the AAC is generally restricted to AAC staff, VA Central Office, custodial personnel, Federal Protective Service and authorized operational personnel through electronic locking devices. All other persons gaining access to the computer rooms are escorted. Backup records stored off-site for both the AAC and VA Central Office are safeguarded in secured storage areas. A disaster recovery plan is in place and system recovery is tested at an off-site facility in accordance with established schedules. This section is updated to state that there are multiple levels of security to ensure the confidentiality of all data stored within the IRR. The registry is stored on a password protected system located in a locked room. Registry application is web-based and accessible behind the VA firewall. Access to the facility is limited by Personal Identity Verification (PIV) access, security card, metal scanners at the entrance, and security guards.

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 March 26, 2021 for publication.

Dated: April 27, 2021.

Amy L. Rose,

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

SYSTEM NAME:

Ionizing Radiation Registry-VA (69VA10).

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

Character-based data from Ionizing Radiation Code Sheets are maintained in a registry data set at the Austin Information Technology Center (AITC), 1615 Woodward Street, Austin, Texas 78772. Since the data set at the AITC is not all-inclusive, *i.e.,* narratives, signatures, etc., noted on the code sheets are not entered into this system, images of the code sheets are maintained at the Department of Veterans Affairs, Post Deployment Health Services (10P4Q), 810 Vermont Avenue NW, Washington, DC 20420. These are electronic images of paper records, *i.e.,* code sheets, medical records, questionnaires and correspondence.

SYSTEM MANAGER(S):

Deputy Chief Consultant, Post Deployment Health Services (10P4Q). VA Central Office, 810 Vermont Avenue NW., Washington, DC 20420. Telephone number (202) 266–4511 (Note: this is not a toll-free number).

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Title 38, United States Code (U.S.C.) 527, 1116, 1710(e)(1)(B) and 1720E, Public Law 102–585 Section 703, and Public Law 100–687.

PURPOSE(S) OF THE SYSTEM:

The records will be used for the purpose of providing information about Veterans who have had an IRR examination at a VA facility; assisting in generating hypotheses for research studies; providing management with the capability to track patient demographics, and radiogenic related diseases; and planning and delivery of health care services and associated costs. The records are used to assist in generating hypotheses for research studies. Because of the self-selected nature of the registry participants, *i.e.,* the individuals decide themselves to be part of the registry rather than being ''chosen'' in a scientific manner, this group cannot be used for scientific research. However, the IRR may assist researchers by providing clues or suggestions of specific health problems that then form the basis for the design and conduct of specific scientific studies.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Veterans who may have been exposed to ionizing radiation while on active military duty and have had an IRR examination at a VA medical facility under conditions described in Title 38 United States Code (U.S.C.) 1710(e)(1)(B) and 1720E. These conditions include:

1. On-site participation in a test involving the atmospheric detonation of a nuclear device at a nuclear device testing site-the Pacific Island, *e.g.,* Bikini, New Mexico, Nevada, etc. (whether or not the testing nation was the United States);

2. Participation in the occupation of Hiroshima or Nagasaki, Japan, from August 6, 1945, through July 1, 1946;

(a) Internment as a prisoner of war (POW) in Japan during World War II which the Secretary of VA determines resulted in an opportunity for exposure to ionizing radiation comparable to that of Veterans involved in the occupation of Hiroshima or Nagasaki, Japan;

3. Treatment with nasopharyngeal (NP) radium irradiation while in the active military, naval or air service; and

4. Participated in radiation-risk activities at the:

(a) Department of Energy gaseous diffusion plants at Paducah, KY, Portsmouth, OH, or K25 area at Oak Ridge, TN, for at least 250 days before February 1, 1992;

(b) Underground nuclear tests at Amchitka Island, AK, before January 1, 1974.

CATEGORIES OF RECORDS IN THE SYSTEM:

These records consist of code sheet records containing VA facility code identifier where the Veteran was examined or treated; Veteran's name; address; Social Security number; military service serial number; claim number; date of birth; telephone number; sex; report of birth defects among Veteran's children or grandchildren; dates of medical examinations; consultations; radiogenic related diseases; and name and signature of examiner/physician coordinator.

In addition, there may be medical records with information relating to the examination and/or treatment, including laboratory findings on vision, hearing, blood tests, electrocardiograms, chest x-rays, urinalysis, laboratory report displays, medical certificates to support diagnosis; progress notes; military unit assignments; questionnaires; correspondence relating to Veteran's exposure history; personal history, *e.g.,* education, marital status, occupational history, family history, complaints/symptoms; personal medical history, habits, recreation, reproductive and family history, physical measurements; military discharge records; and VA claims for compensation.

RECORD SOURCE CATEGORIES:

VA patient medical records, various automated record systems providing clinical and managerial support to VA health care facilities, Veteran, family members, and records from Veterans Benefits Administration, Department of Defense, Department of the Army, Department of the Air Force, Department of the Navy and other Federal agencies.

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 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. The record of an individual who is covered by this system may be disclosed to a member of Congress or staff person acting for the member when the member or staff person requests the record on behalf of, and at the written request of, that individual.

2. 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.

3. A record containing the name(s) and address(es) of present or former members of the armed services and/or their dependents may be released from this system of records under certain circumstances:

(a) To any nonprofit organization if the release is directly connected with the conduct of programs and the utilization of benefits under Title 38, and

(b) To any criminal or civil law enforcement governmental agency or instrumentality 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 standing written request that such name(s) or address(es) be provided for a purpose authorized by law; provided, further, that the record(s) 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).

4. Disclosure may be made to NARA in records management inspections conducted under authority of Title 44 U.S.C. 2904 and 2906, or other functions authorized by laws and policies governing NARA operations and VA records management responsibilities.

5. VA may disclose information from this system to epidemiological and other research facilities approved by the Under Secretary for Health for research purposes determined to be necessary and proper, provided that the names and addresses of veterans and their dependents will not be disclosed unless those names and addresses are first provided to VA by the facilities making the request.

6. In order to conduct Federal research necessary to accomplish a statutory purpose of an agency, at the written request of the head of the agency, or designee of the head of that agency, the name(s) and address(es) of present or former personnel or the Armed Services and/or their dependents may be disclosed

(a) To a Federal department or agency or

(b) Directly to a contractor of a Federal department or agency. When a disclosure of this information is to be made directly to the contractor, VA may impose applicable conditions on the department, agency, and/or contractor to insure the appropriateness of the disclosure to the contractor.

7. Any information in this system may be disclosed to a Federal grand jury, a Federal court or a party in litigation, or a Federal agency or party to an administrative proceeding being conducted by a Federal agency, in order for VA to respond to and comply with the issuance of a Federal subpoena.

8. Any information in this system may be disclosed to a state or municipal grand jury, a state or municipal court or a party in a litigation, or to a state or municipal administrative agency functioning in a quasi-judicial capacity or a party to a proceeding being conducted by such agency, in order for VA to respond to and comply with the issuance of a state or municipal subpoena; provided, that any disclosure or claimant information made under this routine use must comply with the provisions of 38 CFR 1.511.

9. 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. If the disclosure is in response to a request from a law enforcement entity, the request must meet the requirements for a qualifying law enforcement request under the Privacy Act, 5 U.S.C. 552a(b)(7).

10. VA may disclose information to survey teams of the Joint Commission on Accreditation of Healthcare Organizations, College of American Pathologists, American Association of Blood Banks, and similar national accreditation agencies or boards with which VA has a contract or agreement to conduct such reviews, as relevant and necessary for the purpose of program review or the seeking of accreditation or certification.

11. VA may disclose information to the 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; or

(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, 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).

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 is 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.

14. 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:

All registry data is stored electronically in the registry database.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Documents are retrieved by name of Veteran, Social Security number and service serial number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Currently these records are maintained as a permanent record, pending approval of a new records schedule by NARA. These permanent records will transfer to NARA in 5-year blocks, until scheduled.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Access to electronic and paper records at VA Central Office is only authorized to VA personnel on a ''need to know'' basis. Records are maintained in manned rooms during working hours. During non-working hours, there is limited access to the building with visitor control by security personnel. Registry data maintained at the AITC can only be updated by authorized AITC personnel.

There are multiple levels of security to ensure the confidentiality of all data stored within the IRR. The registry is stored on a password protected system located in a locked room. Registry application is web-based and accessible behind the VA firewall. Access to the facility is limited by Personal Identity Verification (PIV) access, security card, metal scanners at the entrance, and security guards.

RECORD ACCESS PROCEDURE:

An individual who seeks access to records maintained under his or her name may write or visit the nearest VA facility or write to the Deputy Chief Consultant, Post Deployment Health Services (10P4Q), VA Central Office, 810 Vermont Avenue NW, Washington, DC 20420.

CONTESTING RECORD PROCEDURES:

(See Record Access Procedures above.)

NOTIFICATION PROCEDURE:

An 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 last VA facility where medical care was provided or submit a written request to the Deputy Chief Consultant, Post Deployment

Health Services (10P4Q), VA Central Office, 810 Vermont Avenue NW, Washington, DC 20420. Inquiries should include the Veteran's name, Social Security number, service serial number, and return address.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

Last full publication provided in 68 FR 75028.

[FR Doc. 2021–09069 Filed 4–29–21; 8:45 am]

BILLING CODE P