



## Privacy Act of 1974; System of Records

**AGENCY:** Department of Veterans Affairs (VA).

**ACTION:** Notice of a Modified System of Records.

**SUMMARY:** As required by the Privacy Act of 1974 (5 U.S.C. 552a(e)(4)), notice is hereby given that the Department of Veterans Affairs (VA) is amending the system of records entitled “Veterans Health Information Systems and Technology Architecture (VistA) Records-VA” (79VA10P2) as set forth in 77 FR 65939. VA is amending the system by revising the System Number, System Location, System Manager, Records Source Categories, Routine Uses of Records Maintained in the System, Policies and Practices for Retention and Disposal of Records, Physical, Procedural and Administrative Safeguards. VA is republishing the system notice in its entirety.

**DATES:** Comments on this amended system of records must be received no later than **[Insert date 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 new system will become effective **[Insert date 30 days after date of publication in the Federal Register]**.

**ADDRESSES:** Comments may be submitted through [www.Regulations.gov](http://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 “Veterans Health Information Systems and Technology Architecture (VistA) Records-VA (79VA10P2)”. Comments received will be available at [regulations.gov](https://www.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).

**SUPPLEMENTAL INFORMATION:** The system number is being updated from 79VA10P2 to 79VA10 to reflect the current VHA organizational routing symbol. The System Manager is being updated to reflect organization changes.

The System Location is being updated to reflect electronic records being located at VA Enterprise Cloud Data Centers/Amazon Web Services and contracted data repository sites, such as the Cerner Technology Centers (CTC): Primary Data Center in Kansas City, MO and Continuity of Operations/Disaster Recovery (COOP/DR) Data Center in Lee Summit, MO.

The Records Source Categories is being updated to include other VA information technology (IT) systems, including but not limited to, Master Person Index and Enrollment.

Routine Use twenty-nine (29) is being added to state, "VA may disclose health care information to DoD for the purpose of VHA health care operations as defined in the HIPAA Privacy Rule, 45 CFR Parts 160 and 164 and to the Defense Health Agency (DHA), as a health care provider, for the purpose of DHA health care operations." VHA, as a health care provider, must be able to share health care information with other entities and health care providers for VA to perform certain health care operations, such as quality assessment and improvement activities and medical reviews.

Routine Use thirty (30) 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. VA needs this routine use for the data breach response and remedial efforts with another Federal agency.

Routine Use thirty-one (31) is being added to state, "VA may disclose relevant health care information to (a) a Federal agency or non-VA health care provider or institution when VA refers a patient for hospital or nursing home care or medical services, or authorizes a patient to obtain non-VA medical services, and the information is needed by the Federal agency or non-VA institution or provider to perform the services, or (b) a Federal agency or a non-VA hospital (Federal, State and local, public, or private) or other medical institution having hospital facilities, blood banks, or similar institutions, medical schools or clinics, or other groups or individuals that have contracted or agreed to provide medical services or share the use of medical resources under the provisions of 38 U.S.C. 513, 7409, 8111, or 8153, when treatment is rendered by VA under the terms of such contract or agreement, or the issuance of an authorization, and the information is needed for purposes of medical treatment and/or follow-up, determining entitlement to a benefit, or recovery of the costs of the medical care.

Policies and Practices for Retention and Disposal of Records is being updated to remove, "Paper records and information stored on electronic storage media are maintained and disposed of in accordance with records disposition authority approved by

the Archivist of the United States.” This section will state, Record Control Schedule (RCS) 10-1, Item 2000.2 Information Technology Operations and Maintenance Records destroy 3 years after agreement, control measures, procedures, project, activity, or when transaction is obsolete, completed, terminated or superseded, but longer retention is authorized if required for business use (DAA-GRS-2013-0005-0004, item 020). RCS 10-1, Item 2100.3 2100.3, System Access Records destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use (DAA-GRS-2013-0006-0004, item 31).

The Physical, Procedural and Administrative Safeguards section is being amended to add, “Access to Cerner Technology Centers is generally restricted to Cerner employees, contractors or associates with a Cerner issued ID badge and other security personnel cleared for access to the data center. Access to computer rooms housing Federal data, hence Federal enclave, is restricted to persons Federally cleared for Federal enclave access through electronic badge entry devices. All other persons, such as custodians, gaining access to Federal enclave are escorted.”

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 November 10, 2020 for publication.

Dated: December 18, 2020.

**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:** Veterans Health Information Systems and Technology Architecture (VistA) Records-VA (79VA10).

**SECURITY CLASSIFICATION:** Unclassified.

**SYSTEM LOCATION:** Records are maintained at VA health care facilities, Regional Data Processing Centers and (in most cases), archival storage of the VistA data to back up tapes are maintained at off-site locations. Address locations for VA facilities are listed in VA Appendix 1. In addition, information from these records or copies of records may be maintained at the Department of Veterans Affairs, 810 Vermont Avenue, NW, Washington, DC; VA Data Processing Centers, VA Office of Information & Technology (OI&T) Field Offices; Veterans Integrated Service Network (VISN) Offices; Employee Education Systems and VA Enterprise Cloud Data Centers/Amazon Web Services, 1915 Terry Avenue, Seattle, WA 98101 and contracted data repository sites, such as the Cerner Technology Centers (CTC): Primary Data Center in Kansas City, MO and Continuity of Operations/Disaster Recovery (COOP/DR) Data Center in Lees Summit, MO.

**SYSTEM MANAGER(S):** The official responsible for policies and procedures is the Director, Health Information Governance (HIG), Department of Veterans Affairs, 810 Vermont Avenue, NW., Washington, DC 20420. Toll-free telephone number 1-877-461-5038.

**AUTHORITY FOR MAINTENANCE OF THE SYSTEM:** Title 38, United States Code, section 7301(a).

**PURPOSE(S) OF THE SYSTEM:** The records and information may be used for statistical analysis to produce various management, workload tracking and follow-up reports; to track and evaluate the ordering and delivery of equipment, services and patient care; the planning, distribution and utilization of resources; the possession and use of equipment or supplies; the performance of vendors, equipment, and employees; and to provide clinical and administrative support to patient medical care. The data may be used for research purposes. The data may be used also for such purposes as assisting in the scheduling of tours of duties and job assignments of employees; the scheduling of patient treatment services, including nursing care, clinic appointments, surgery, diagnostic and therapeutic procedures; the repair and maintenance of equipment and for follow-up activities to determine that the actions were accomplished and to evaluate the results; the registration of vehicles and the assignment and utilization of parking spaces; to plan, schedule, and maintain rosters of patients, employees and others attending or participating in sports, recreational or other events (e.g., National Wheelchair Games, concerts, picnics); for audits, reviews and investigations conducted by staff of the health care facility, the Network Directors Office, VA Central Office, and the VA Office of Inspector General (OIG); for quality assurance audits, reviews, investigations and inspections; for law enforcement investigations; and for personnel management, evaluation and employee ratings, and performance evaluations.

**CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:** The records include information concerning current and former employees, applicants for employment, trainees, contractors, sub-contractors, contract personnel, students, providers and consultants, patients and members of their immediate family, volunteers, maintenance personnel, as well as individuals working collaboratively with VA.

**CATEGORIES OF RECORDS IN THE SYSTEM:** The records may include information related to:

1. Workload such as orders entered, verified, and edited (e.g., engineering work orders, doctors' orders for patient care including nursing care, the scheduling and delivery of medications, consultations, radiology, laboratory and other diagnostic and therapeutic examinations); results entered; items checked out and items in use (e.g., library books, keys, x-rays, patient medical records, equipment, supplies, reference materials); work plans entered and the subsequent tracking (e.g., construction projects, engineering work orders and equipment maintenance and repairs assigned to employees and status, duty schedules, work assignments, work requirements); reports of contact with individuals or groups; employees' (including volunteers) work performance information (e.g., duties and responsibilities assigned and completed, amount of supplies used, time used, quantity and quality of output, productivity reports, schedules of patients assigned and treatment to be provided);
2. Administrative procedures, duties, and assignments of certain personnel;
3. Computer access authorizations, computer applications available and used, information access attempts, frequency and time of use; identification of the person responsible for, currently assigned, or otherwise engaged in various categories of patient care or support of health care delivery; vehicle registration (motor vehicles and bicycles) and parking space assignments; community and special project participants and attendees (e.g., sports events, concerts, National Wheelchair Games); employee work related accidents. The record may include identifying information (e.g., name, date of birth, age, sex, Social Security number, taxpayer identification number); address information (e.g., home and mailing address, home

telephone number, emergency contact information such as name, address, telephone number, and relationship); information related to training (e.g., security, safety, in-service), education and continuing education (e.g., name and address of schools and dates of attendance, courses attended and scheduled to attend, type of degree, certificate, grades etc.); information related to military service and status; qualifications for employment (e.g., license, degree, registration or certification, experience); vehicle information (e.g., type make, model, license and registration number); evaluation of clinical and technical skills; services or products purchased (e.g., vendor name and address, details about evaluation of service or product, price, fee, cost, dates purchased and delivered, employee workload and productivity data); employee work relate injuries (cause, severity, type of injury, body part affected);

4. Financial information, such as service line and clinic budgets, projected and actual costs;

5. Supply information, such as services, materials and equipment ordered; and

6. Abstract information (e.g., data warehouses, environmental and epidemiological registries, etc.) is maintained in auxiliary paper and automated records;

7. Electronic messages;

8. The Social Security number and universal personal identification number of health care providers;

9. Practitioner DEA registration numbers; and

10. The Integration Control Number or Veterans Administration Person Identifier.

**RECORD SOURCE CATEGORIES:** Information in this system of records is

provided by the individual, supervisors, other employees, personnel records, or obtained from their interaction with the system, and from other VA information technology (IT) systems, including but not limited to, Master Person Index and Enrollment.

**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 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 permitting disclosure. VA may disclose protected health information pursuant to the following routine uses where required by law or permitted by 45 CFR parts 160 and 164.

1. In the event that a record maintained by VA to carry out its functions indicates a violation or potential violation of law, whether civil, criminal or regulatory in nature, and whether arising by general statute or particular program statute, or by regulation, rule or order issued pursuant thereto, information may be disclosed to the appropriate agency whether Federal, state, local or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute or rule, regulation or order issued pursuant thereto.

2. Disclosure may be made to any source from which additional information is requested (to the extent necessary to identify the individual, inform the source of the purpose(s) of the request, and to identify the type of information requested),

when necessary to obtain information relevant to a Department decision concerning the hiring or retention of an employee, the issuance of a security clearance, the conducting of a security or suitability investigation of an individual, the letting of a contract, or the issuance of a license, grant, or other benefits.

3. Disclosure may be made to an agency in the executive, legislative, or judicial branch, or the District of Columbia government in response to its request or at the initiation of VA, in connection with the hiring of an employee, the issuance of a security clearance, the conducting of a security or suitability investigation of an individual, the letting of a contract, the issuance of a license, grant, or other benefits by the requesting agency, or the lawful statutory, administrative, or investigative purpose of the agency to the extent that the information is relevant and necessary to the requesting agency's decision.

4. Disclosure may be made to a Congressional office from the record of an individual in response to an inquiry from the Congressional office made at the request of that individual.

5. Disclosure may be made to National Archives and Records Administration (NARA) and the General Services Administration in records management inspections and other activities conducted under Title 44.

6. Disclosure may be made to the Department of Justice and United States Attorneys in defense or prosecution of litigation involving the United States, and to Federal agencies upon their request in connection with review of administrative tort claims filed under the Federal Tort Claims Act, 28 U.S.C. 2672.

7. Hiring, performance, or other personnel-related information may be disclosed to any facility with which there is or there is proposed to be an affiliation, sharing agreement, contract, or similar arrangement for purposes of establishing,

maintaining, or expanding any such relationship.

8. Disclosure may be made to a Federal, State or local government licensing board and to the Federation of State Medical Boards or a similar nongovernment entity which maintains records concerning individual employment histories or concerning the issuance, retention or revocation of licenses, certifications, or registration necessary to practice an occupation, profession or specialty; in order for the Department to obtain information relevant to a Department decision concerning the hiring, retention or termination of an employee; or to inform a Federal agency, licensing boards or the appropriate nongovernment entities about the health care practices of a terminated, resigned or retired health care employee whose professional health care activity so significantly failed to conform to generally accepted standards of professional medical practice as to raise reasonable concern for the health and safety of patients receiving medical care in the private sector or from another Federal agency. These records may also be disclosed as part of an ongoing computer matching program to accomplish these purposes.

9. For program review purposes, and the seeking of accreditation and/or certification, disclosure may be made to survey teams of The Joint Commission, College of American Pathologists, American Association of Blood Banks, and similar national accreditation agencies or boards with whom VA has a contract or agreement to conduct such reviews, but only to the extent that the information is necessary and relevant to the review.

10. Disclosure may be made to a State or local government entity or national certifying body which has the authority to make decisions concerning the issuance, retention or revocation of licenses, certifications or registrations required to practice a health care profession, when requested in writing by an investigator

or supervisory official of the licensing entity or national certifying body for the purpose of making a decision concerning the issuance, retention or revocation of the license, certification or registration of a named health care professional.

11. Any information which is relevant to a suspected violation 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, may be disclosed to a Federal, State, local or foreign agency charged with the responsibility of investigating or prosecuting such violation, rule or order issued pursuant thereto.

12. Disclosure may be made to officials of labor organizations recognized under 5 U.S.C. chapter 71 when relevant and necessary to their duties of exclusive representation concerning personnel policies, practices, and matters affecting working conditions.

13. Disclosure may be made to the VA-appointed representative of an employee, including all notices, determinations, decisions, or other written communications issued to the employee in connection with an examination ordered by VA under medical evaluation (formerly fitness-for duty) examination procedures or Department-filed disability retirement procedures.

14. Disclosure may be made to officials of the Merit Systems Protection Board, including the Office of the Special Counsel, when requested in connection with appeals, special studies of the civil service and other merit systems, review of rules and regulations, investigation of alleged or possible prohibited personnel practices, and such other functions, promulgated in 5 U.S.C. 1205 and 1206, or as may be authorized by law.

15. Disclosure may be made to the Equal Employment Opportunity Commission

when requested in connection with investigations of alleged or possible discrimination practices, examination of Federal affirmative employment programs, compliance with the Uniform Guidelines of Employee Selection Procedures, or other functions vested in the Commission by the President's Reorganization Plan No. 1 of 1978.

16. Disclosure may be made to the Federal Labor Relations Authority, including its General Counsel, when requested in connection with investigation and resolution of allegations of unfair labor practices, in connection with the resolution of exceptions to arbitrator awards when a question of material fact is raised and matters before the Federal Service Impasses Panel.

17. Disclosure may be made in consideration and selection of employees for incentive awards and other honors and to publicize those granted. This may include disclosure to other public and private organizations, including news media, which grant or publicize employee awards or honors.

18. Disclosure may be made to consider employees for recognition through administrative and quality step increases and to publicize those granted. This may include disclosure to other public and private organizations, including news media, which grant or publicize employee recognition.

19. Identifying information such as name, address, Social Security number and other information as is reasonably necessary to identify such individual, may be disclosed to the National Practitioner Data Bank at the time of hiring or clinical privileging/re-privileging of health care practitioners, and at other times as deemed necessary by VA in order for VA to obtain information relevant to a Department decision concerning the hiring, privileging/re-privileging, retention or termination of the applicant or employee.

20. Disclosure of relevant information may be made to the National Practitioner Data Bank or to a State or local government licensing board which maintains records concerning the issuance, retention or revocation of licenses, certifications, or registrations necessary to practice an occupation, profession or specialty when under the following circumstances, through a peer review process that is undertaken pursuant to VA policy, negligence, professional incompetence, responsibility for improper care, or professional misconduct has been assigned to a physician or licensed or certified health care practitioner: (1) On any payment in settlement (or partial settlement) of, or in satisfaction of a judgment in a medical malpractice action or claim; or, (2) on any final decision that adversely affects the clinical privileges of a physician or practitioner for a period of more than 30 days. These records may also be disclosed as part of a computer matching program to accomplish these purposes.

21. Disclosure of medical record data, excluding name and address, unless name and address is furnished by the requester, may be made to epidemiological and other research facilities for research purposes determined to be necessary and proper and approved by the Under Secretary for Health.

22. Disclosure of names and addresses of present or former personnel of the Armed Services, and their dependents, may be made to: (a) A Federal department or agency, at the written request of the head or designee of that agency; or (b) directly to a contractor or subcontractor of a Federal department or agency, for the purpose of conducting Federal research necessary to accomplish a statutory purpose of an agency. When disclosure of this information is made directly to a contractor, VA may impose applicable conditions on the department, agency, or contractor to insure the appropriateness of the disclosure to the contractor.

23. The Social Security number, universal personal identification number and other identifying information of a health care provider may be disclosed to a third party where the third party requires the agency to provide that information before it will pay for medical care provided by VA.

24. Relevant information may be disclosed to individuals, organizations, private or public agencies, etc., with whom VA has a contract or agreement to perform such services as VA may deem practical for the purposes of laws administered by VA, in order for the contractor to perform the services of the contract or agreement.

25. Disclosure of relevant health care information may be made to individuals or organizations (private or public) with whom VA has a contract or sharing agreement for the provision of health care or administrative or financial services.

26. 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.

27. VA may, on its own initiative, disclose any information or records 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. This routine use permits disclosures by the Department to respond to a suspected or confirmed data breach, including the conduct of any risk analysis or provision of credit protection services as provided in 38 U.S.C. 5724, as the terms are defined in 38 U.S.C. 5727.

28. VA may disclose relevant provider information to a state prescription drug monitoring program, or similar program, for the purpose of submitting to or receiving from the program information regarding prescriptions to an individual for controlled substances, as required under the applicable state law.

29. VA may disclose health care information to DoD for the purpose of VA health care operations as defined in the HIPAA Privacy Rule, 45 CFR Parts 160 and 164 and to the Defense Health Agency (DHA), as a health care provider, for the purpose of DHA health care operations.

30. 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.

31. VA may disclose relevant health care information to (a) a Federal agency or non-VA health care provider or institution when VA refers a patient for hospital or

nursing home care or medical services, or authorizes a patient to obtain non-VA medical services, and the information is needed by the Federal agency or non-VA institution or provider to perform the services, or (b) a Federal agency or a non-VA hospital (Federal, State and local, public, or private) or other medical institution having hospital facilities, blood banks, or similar institutions, medical schools or clinics, or other groups or individuals that have contracted or agreed to provide medical services or share the use of medical resources under the provisions of 38 U.S.C. 513, 7409, 8111, or 8153, when treatment is rendered by VA under the terms of such contract or agreement, or the issuance of an authorization, and the information is needed for purposes of medical treatment and/or follow-up, determining entitlement to a benefit, or recovery of the costs of the medical care.

**POLICIES AND PRACTICES FOR STORAGE OF RECORDS:** Records maintained on paper, microfilm, magnetic tape, disk, or laser optical media. In most cases, archival storage of the VistA data to backup tapes are maintained at off-site locations.

**POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:** Records are retrieved by name, Social Security number or other assigned identifiers of the individuals on whom they are maintained.

**POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:** RCS 10-1, Item 2000.2 Information Technology Operations and Maintenance Records destroy 3 years after agreement, control measures, procedures, project, activity, or when transaction is obsolete, completed, terminated or superseded, but longer retention is authorized if required for business use (DAA-GRS-2013-0005-0004, item 020). RCS10-1, Item 2100.3 2100.3, System Access Records destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use (DAA-GRS-2013-0006-0004, item 31).

**ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:**

1. Access to VA working and storage areas is restricted to VA employees on a “need- to-know” basis. Strict physical security control measures are enforced to ensure that disclosure to these individuals is also based on this same principle. Generally, VA file areas are locked after normal duty hours and the facilities are protected from outside access by the Federal Protective Service or other security personnel.
2. Access to computer rooms at health care facilities and regional data processing centers is generally limited by appropriate locking devices and restricted to authorized VA employees and vendor personnel. Automated Data Processing (ADP) peripheral devices are placed in secure areas (areas that are locked or have limited access) or are otherwise protected. Information in VistA may be accessed by authorized VA employees. Access to file information is controlled at two levels. The systems recognize authorized employees by series of individually unique passwords/codes as a part of each data message, and the employees are limited to only that information in the file which is needed in the performance of their official duties. Information that is downloaded from VistA and maintained on laptops and

other approved government equipment is afforded similar storage and access protections as the data that is maintained in the original files. Access to information stored on automated storage media at other VA locations is controlled by individually unique passwords/codes.

Access by Office of Inspector General (OIG) staff conducting an audit, investigation, or inspection at the health care facility, or an OIG office location remote from the health care facility, is controlled in the same manner.

3. Information downloaded from VistA and maintained by the OIG headquarters and Field Offices on automated storage media is secured in storage areas for facilities to which only OIG staff have access. Paper documents are similarly secured. Access to paper documents and information on automated storage media is limited to OIG employees who have a need for the information in the performance of their official duties. Access to information stored on automated storage media is controlled by individually unique passwords/codes.

4. Access to Cerner Technology Centers is generally restricted to Cerner employees, contractors or associates with a Cerner issued ID badge and other security personnel cleared for access to the data center. Access to computer rooms housing Federal data, hence Federal enclave, is restricted to persons Federally cleared for Federal enclave access through electronic badge entry devices. All other persons, such as custodians, gaining access to Federal enclave are escorted.

**RECORD ACCESS PROCEDURE:** Individuals seeking information regarding access to and contesting of records in this system may write, call or visit the VA facility location where they are or were employed or made contact.

**CONTESTING RECORD PROCEDURES:**

(See Record Access Procedures above.)

**NOTIFICATION PROCEDURE:** Individuals who wish to determine whether this system of records contains information about them should contact the VA facility location at which they are or were employed or made contact. Inquiries should include the person's full name, Social Security number, dates of employment, date(s) of contact, and return address.

**EXEMPTIONS PROMULGATED FOR THE SYSTEM:** None.

**HISTORY:** Last full publication provided in 69 FR 5667.

[FR Doc. 2020-28340 Filed: 12/22/2020 8:45 am; Publication Date: 12/23/2020]