DEPARTMI

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, notice is hereby given that the Department of Veterans Affairs (VA) is amending the system of records entitled, ‘‘The Revenue Program-Billing and Collections Records-VA” (114VA10D). VA is amending the system of records by revising the System Number; System Location; Purpose of the System; Categories of Individuals Covered by the System; Record Source Categories; Routine Uses of Records Maintained in the System; Policies and Practices for Storage of Records; and 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 the VA, the new system will become effective **[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**.

ADDRESSES: Written comments may be submitted through www.Regulations.gov; by mail or hand-delivery to Director, Regulation Policy and Management (00REG), Department of Veterans Affairs, 810 Vermont Avenue, NW, Room 1064, Washington, DC 20420; or by fax to (202) 273-9026 (Note: not a toll-free number). Comments should indicate they are submitted in response to ‘‘The Revenue Program-Billing and Collections Records-VA”. Copies of comments received will be available for public

inspection in the Office of Regulation Policy and Management, Room 1063B, between the hours of 8:00 a.m. and 4:30 p.m., Monday through Friday (except holidays). Please call (202) 461-4902 for an appointment (Note: not a toll-free number). In addition, comments may be viewed online at www.Regulations.gov.

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 is being updated from 114VA10D to 114VA10 to reflect the current VHA organizational routing symbol.

The System Location is being updated to reflect electronic records being located at contractor facilities, 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. Amazon Web Services, LLC, 13461 Sunrise Valley Drive, Herndon, VA 20171–3283.

The Purpose of the System is being amended to remove participation in pilot test of NPI enumeration system by the Centers for Medicare and Medicaid Services (CMS). This section will add, CMS National Plan and Provider Enumeration System (NPPES).

Categories of Individuals Covered by the System is being amended to add “including those receiving or eligible to receive VA health care” to item 2. Also, item 10, Caregivers, is being added.

The Record Source Categories is being amended to add Social Security Administration and Patient Medical Records-VA (24VA10A7). Also, 77VA10A4 is being changed to 77VA10E2E and 79VA10P2 is being changed to 79VA10A7.

The Routine Uses of Records Maintained in the System is amending Routine Use 10 to remove universal personal identification number.

Routine Use 13 is being amended to include 7332-protected information.

Routine Use 17 is being amended to replace “CMS to test the enumeration system for the NPI and once the system is operational” with National Plan and Provider Enumeration System (NPPES).

Routine Use 20 has been amended by removing the language which states, this routine use permits disclosures by VA 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.

a. Effective Response. A Federal agency’s ability to respond quickly and effectively in the event of a breach of Federal data is critical to its efforts to prevent or minimize any consequent harm. An effective response necessitates disclosure of information regarding the breach to those individuals affected by it, as well as to persons and entities in a position to cooperate, either by assisting in notification to affected individuals or playing a role in preventing or minimizing harms from the breach.

b. Disclosure of Information. Often, the information to be disclosed to such persons and entities is maintained by Federal agencies and is subject to the Privacy Act (5 U.S.C 552a). The Privacy Act prohibits the disclosure of any record in a system of records by any means of communication to any person or agency absent the written consent of the subject individual, unless the disclosure falls within one of twelve statutory exceptions. In order to ensure an agency is in the best position to respond in a timely and effective manner, in accordance with 5 U.S.C 552a(b)(3) of the Privacy Act, agencies should publish a routine use for

appropriate systems specifically applying to the disclosure of information in connection with response and remedial efforts in the event of a data breach.

The language in Routine Use 21 is being amended. It previously stated 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 release of the records to the DoJ is limited to circumstances where relevant and necessary to the litigation. VA may disclose records in this system of records in legal proceedings before a court or administrative body after determining that release of the records to the court or administrative body is limited to circumstances where relevant and necessary to the litigation.

Policies and Practices for Storage of Records is being amended to include Records within this system is also hosted in Amazon Web Services (AWS) Government Cloud (GovCloud) infrastructure as a service cloud-computing environment that has been authorized at the high-impact level under the Federal Risk and Authorization Management Program (FedRAMP).

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 July 24, 2020 for publication.

Dated: January 19, 2021.

Amy L. Rose,

Program Analyst,

VA Privacy Service,

Office of Information Security,

Office of Information and Technology,

Department of Veterans Affairs.

SYSTEM NAME: The Revenue Program-Billing and Collections Records-VA (114VA10)

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: Records are maintained at each Department of Veterans Affairs (VA) health care facility. In most cases, backup computer tape information is stored at off-site locations. Address locations for VA facilities are listed in VA Appendix 1 of the biennial publication of VA Privacy Act Issuances. In addition, information from these records or copies of records may be maintained at, 810 Vermont Avenue, NW,

Washington, DC; the VA Austin Automation Center (AAC), Austin, Texas; Veterans Integrated Service Network (VISN) Offices; VA Allocation Resource Center (ARC), Boston, Massachusetts; and contractor facilities, such as the Cerner Technology Centers (CTC); Primary Data Center in Kansas City, Missouri; and Continuity of Operations/Disaster Recovery (COOP/DR) Data Center in Lees Summit, Missouri. Records are also maintained at Amazon Web Services, LLC, 13461 Sunrise Valley Drive, Herndon, VA 20171–3283.

SYSTEM MANAGER(S): The official responsible for policies and procedures is the Deputy Under Secretary for Health, Office for Community Care (10D), Department of Veterans Affairs, 810 Vermont Avenue, NW, Washington, DC 20420. The local officials responsible for maintaining the system are the Director of the facility where the individual is or was associated.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 38, United States Code (U.S.C.), sections 1710 and 1729.

PURPOSE(S) OF THE SYSTEM: The records and information are used for the billing of, and collections from a third-party payer, including insurance companies, other Federal agencies, or foreign governments, for medical care or services received by a Veteran for a non-service-connected condition or from a first party Veteran required to make copayments. The records and information are also used for the billing of and collections from other Federal agencies for medical care or services received by an eligible beneficiary. The data may be used to identify and/or verify insurance coverage of a Veteran or Veteran's spouse prior to submitting claims for medical care or services. The data may be used to support appeals for non-reimbursement of claims for medical care or services provided to a Veteran. Data may be used in the Payer Compliance Tool to determine if third party payer information meets the requirement to reimburse VA. The data may be used to enroll health care providers with health plans and VA's

health care clearinghouse in order to electronically file third party claims. For the purposes of health care billing and payment activities to and from third party payers, VA will disclose information in accordance with the legislatively-mandated transaction standard and code sets promulgated by the United States Department of Health and Human Services (HHS) under the Health Insurance Portability and Accountability Act (HIPAA). The data may be used to make application for a National Provider Identifier (NPI), as required by the HIPAA Administrative Simplification Rule on Standard Unique Health Identifier for Healthcare Providers, 45 CFR Part 162, for all health care professionals providing examination or treatment within VA health care facilities, including the Centers for Medicare and Medicaid Services (CMS) National Plan and Provider Enumeration System (NPPES). The records and information may be used for statistical analyses to produce various management, tracking and follow-up reports, to track and trend the reimbursement practices of insurance carriers, and to track billing and collection information. The data may be used to support, or in anticipation of supporting, reimbursement claims from community health care providers or their agents. The data may be used to support, or in anticipation of supporting, reimbursement claims from academic affiliates with which VA maintains a business relationship.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

1. Veterans who have applied for health care services under Title 38, United States Code, Chapter 17, and in certain cases members of their immediate families.
2. Beneficiaries of other Federal agencies, including those receiving or eligible to receive VA health care.
3. Individuals examined or treated under contract or resource sharing agreements.
4. Individuals examined or treated for research or donor purposes.
5. Individuals who have applied for Title 38 benefits, but who do not meet the requirements under Title 38 to receive such benefits.

6. Individuals who were provided medical care under emergency conditions for humanitarian reasons.

7. Pensioned members of allied forces (Allied Beneficiaries) who are provided health care services under Title 38, United States Code, Chapter 1.

8. Health care professionals providing examination or treatment to any individuals within VA health care facilities.

9. Health care professionals providing examination or treatment to individuals under contract or resource sharing agreements or Community Care programs, such as Choice.

10. Caregivers.

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

1. The Social Security number and insurance policy number of the Veteran and/or Veteran's spouse. The record may include other identifying information (*e.g.*, name, date of birth, age, sex, marital status) and address information (*e.g.*, home and/or mailing address, home telephone number).

2. Insurance company information specific to coverage of the Veteran and/or spouse to include annual deductibles and benefits.

3. Diagnostic codes (ICD-10-CM, CPT– 4, and any other coding system) pertaining to the individual's medical, surgical, psychiatric, dental and/or psychological examination or treatment.

4. Charges claimed to a third-party payer, including insurance companies, other Federal agencies, or foreign governments, based on treatment/services provided to the patient.

5. Charges billed to those Veterans who are required to meet co-payment obligations for treatment/services rendered by VA.

6. The name, Social Security number, Drug Enforcement Administration (DEA) number, National Provider Identifier (NPI) and credentials including provider's degree, licensure, certification, registration or occupation of health care providers.

7. Records of charges related to patient care that are created in anticipation of litigation in which the United States is a party or has an interest in the litigation or potential litigation, including a third-party tortfeasor, workers compensation, or no-fault automobile insurance cases. Such records are not subject to disclosure under 5 U.S.C. 552a(d)(5).

RECORD SOURCE CATEGORIES: The patient, family members or guardian, and friends, employers or other third parties when otherwise unobtainable from the patient or family; health insurance carriers; private medical facilities and health care professionals; state and local agencies; other Federal agencies; Social Security Administration; VA regional offices; 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 (58VA21/22/28); and various automated systems providing clinical and facilities to include Health Care Provider Credentialing and Privileging Records-VA (77VA10E2E); Veterans Health Information Systems and Technology Architecture (VistA)-VA (79VA10A7) and Patient Medical Records-VA (24VA10A7).

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. VA may disclose information, except for the names and home address of Veterans and their dependents, to a Federal, State, local, tribal or foreign agency charged with the responsibility of investigating or prosecuting civil, criminal or regulatory violations of law, or charged with enforcing or implementing the statute, regulation, rule or order issued pursuant thereto. VA may also disclose the names and addresses of Veterans and their dependents to a Federal agency charged with the responsibility of investigating or prosecuting civil, criminal or regulatory violations of law, or charged with enforcing or implementing the statute, regulation, rule or order issued pursuant thereto.

2. 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 letting of a contract, 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. However, names and addresses of Veterans and their dependents will be released only to Federal entities.

3. 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.

4. Disclosure may be made to National Archives and Records Administration in records management inspections conducted under authority of Title 44 U.S.C.

5. 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.

6. Any information in this system of records, including personal information obtained from other Federal agencies through computer-matching programs, may be disclosed for the purposes identified below to any third party, except consumer reporting agencies, in connection with any proceeding for the collection of an amount owed to the United States by virtue of a person's participation in any benefit program administered by VA. Information may be disclosed under this routine use only to the extent that it is reasonably necessary for the following purposes: (a) to assist VA in collection of Title 38 overpayments, overdue indebtedness, and/or costs of services provided individuals not entitled to such services; and (b) to initiate civil or criminal legal actions for collecting amounts owed to the United States and/or for prosecuting individuals who willfully or fraudulently obtain Title 38 benefits without entitlement. This disclosure is consistent with 38 U.S.C. 5701(b)(6).

7. The name and address of a Veteran, other information as is reasonably necessary to identify such Veteran, including personal information obtained from other Federal agencies through computer matching programs, and any information concerning the Veteran's indebtedness to the United States by virtue of the person's participation in a benefits program administered by VA may be disclosed to a consumer reporting agency for purposes of assisting in the collection of such indebtedness, provided that the provisions of 38 U.S.C. 5701(g)(4) have been met.

8. The name of a Veteran, or other beneficiary, other information as is reasonably necessary to identify such individual, and any information concerning the individual's indebtedness by virtue of a person's participation in a medical care and treatment program administered by VA, may be disclosed to the Treasury Department, Internal Revenue Service, for the collection of indebtedness arising from such program by the withholding of all or a portion of the person's Federal income tax refund. These records

may be disclosed as part of a computer-matching program to accomplish these purposes.

9. Relevant information (excluding medical treatment information related to drug or alcohol abuse, infection with the human immunodeficiency virus or sickle cell anemia) may be disclosed to HHS for the purpose of identifying improper duplicate payments made by Medicare fiscal intermediaries where VA was authorized and was responsible for payment for medical services obtained at community health care facilities.

10. The Social Security number, NPI, credentials, and other identifying information of a health care provider may be disclosed to a third party where the third party requires the Department provide that information before it will pay for medical care provided by VA.

11. 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 and/or subcontractor to perform the services of the contract or agreement.

12. Relevant information from this system of records may be disclosed to the National Practitioner Data Bank and/or State Licensing Board in the State(s) in which a practitioner is licensed, in which the VA facility is located, and/or in which an act or omission occurred upon which a medical malpractice claim was based when VA reports information concerning: (a) any payment for the benefit of a physician, dentist, or other licensed health care practitioner which was made as the result of a settlement or judgment of a claim of medical malpractice if an appropriate determination is made in accordance with agency policy that payment was related to substandard care, professional incompetence or professional misconduct on the part of the individual; (b) a final decision which relates to possible incompetence or improper professional conduct that adversely affects the clinical privileges of a physician, dentist or other licensed

health care practitioner for a period longer than 30 days; or (c) the acceptance of the surrender of clinical privileges, or any restriction of such privileges by a physician, dentist, or other licensed health care practitioner either while under investigation by the health care entity relating to possible incompetence or improper professional conduct, or in return for not conducting such an investigation or proceeding. These records may also be disclosed as part of a computer-matching program to accomplish these purposes.

13. Relevant information, including 7332-protected information, may be disclosed from this system of records to any third party or Federal agency such as the Department of Defense, Office of Personnel Management, HHS and government-wide third-party insurers responsible for payment of the cost of medical care for the identified patients, in order for VA to seek recovery of the medical care costs. These records may also be disclosed as part of a computer matching program to accomplish these purposes.

14. Relevant information, including the nature and amount of a financial obligation, may be disclosed in order to assist VA in the collection of unpaid financial obligations owed VA, to a debtor's employing agency or commanding officer, so that the debtor employee may be counseled by his or her Federal employer or commanding officer. This purpose is consistent with 5 U.S.C. 5514, 4 CFR 102.5, and section 206 of Executive Order 11222 of May 8, 1965 (30 FR 6469).

15. 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 and/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.

16. Disclosure of individually identifiable health information including billing information for the payment of care may be made by appropriate VA personnel, to the extent necessary and on a need-to-know basis consistent with good medical-ethical practices, to family members and/or the person(s) with whom the patient has a meaningful relationship.

17. Provider identifying information may be disclosed from this system of records to the NPPES, to obtain an NPI for any eligible health care professional providing examination or treatment with VA health care facilities.

18. Relevant information may be disclosed to community health care providers or their agents where the community health care provider provides health care treatment to Veterans and requires the Department provide that information in order for that entity or its agent to submit, or in anticipation of submission of, a health care reimbursement claim or, in the case of the NPI, for permissible purposes specified in the HIPAA legislation (45 CFR Part 162).

19. Relevant information may be disclosed to an academic affiliate with which VA maintains a business relationship, where the VA provider also maintains an appointment to that academic affiliate's medical staff. This disclosure is to support, or in anticipation of supporting, a health care reimbursement claim(s) or, in the case of the NPI, for permissible purposes specified in the HIPAA legislation (45 CFR Part 162).

20. 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.

21. VA may disclose information in this system of records to the Department of Justice (DoJ), either on VA's initiative or in response to DoJ's request for the information, after either VA or DoJ determines that such information is relevant to DoJ's representation of the United States or any of its components in legal proceedings before a court or adjudicative body, provided that, in each case, the agency also determines prior to disclosure that release of the records to the DoJ is limited to circumstances where relevant and necessary to the litigation. VA may disclose records in this system of records in legal proceedings before a court or administrative body after determining that release of the records to the court or administrative body is limited to circumstances where relevant and necessary to the litigation.

22. 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.

23. 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.

24. VA may disclose relevant information to attorneys, insurance companies, employers, third parties liable or potentially liable under health plan contracts, and courts, boards, or commissions, to the extent necessary to aid VA in the preparation,

presentation, and prosecution of claims authorized under Federal, State, or local laws, and regulations promulgated thereunder.

25. VA may disclose relevant information to health plans, quality review and/or peer review organizations in connection with the audit of claims or other review activities to determine quality of care or compliance with professionally accepted claims processing standards.

DISCLOSURE TO CONSUMER REPORTING AGENCIES: Pursuant to 5 U.S.C. 552a(b)(12), VA may disclose records from this system to consumer reporting agencies as defined in the Fair Credit Reporting Act (15 U.S.C. 1681a(f)) or the Federal Claims Collection Act of 1966 (31 U.S.C. 3701(a)(3)).

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Records are maintained on paper or electronic media. Records within this system is also hosted in Amazon Web Services (AWS) Government Cloud (GovCloud) infrastructure as a service cloud-computing environment that has been authorized at the high-impact level under the Federal Risk and Authorization Management Program (FedRAMP).

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

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Follow the requirement of RCS 10-1 Chapter 4 Item 4000.1 a & b.

4000.1 Financial transaction records related to procuring goods and services, paying bills, collecting debts, and accounting.

a. Official record held in the office of record.

Temporary; destroy six (6) years after final payment or cancellation, but longer retention is authorized if required for business use. (GRS 1.1, Item 010) (DAA-GRS-2016-0001-0002)

b. All Other copies

Temporary; destroy or delete when six (6) years old, but longer retention is authorized if required for business use. (GRS 1.1 item 013) (DAA-GRS-2016-0001-0002)

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 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. Information in VistA may only be accessed by authorized VA personnel. Access to file information is controlled at two levels. The systems recognize authorized personnel by series of individually unique passwords/codes as a part of each data message, and personnel 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 personal computers 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 the VA Austin Information Technology Center (AITC) is generally restricted to AITC employees, custodial personnel, Federal Protective Service and other security personnel. Access to computer rooms is restricted to authorized operational personnel through electronic locking devices. All other persons gaining access to computer rooms are escorted. Information stored in the AITC databases may be accessed.

5. Access to records maintained at the VA Allocation Resource Center and the VISN Offices is restricted to VA employees who have a need for the information in the performance of their official duties. Access to information stored in electronic format is controlled by individually unique passwords/codes. Records are maintained in manned rooms during working hours. The facilities are protected from outside access during non-working hours by the Federal Protective Service or other security personnel.

6. 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 were treated.

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 health care facility where care was rendered. Addresses of VA health care facilities may be found in VA Appendix 1 of the biennial publication of VA Privacy Act Issuances. All inquiries must reasonably identify the place and approximate date that medical care was provided. Inquiries should include the patient's full name, Social Security number, insurance company information, policyholder and policy identification number as well as a return address.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

HISTORY: Last full publication provided in 83 FR 11303.

[FR Doc. 2021-01541 Filed: 1/22/2021 8:45 am; Publication Date: 1/25/2021]