DEPARTMENT OF VETERANS AFFAIRS

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 ‘‘VHA Corporate Data Warehouse-VA’’ (172VA10P2) as set forth in 79 FR 4377. VA is amending the system of records by revising the System Number; System Manager; Purposes of the System; Categories of Records in the System; Routine Uses of Records Maintained in the System and Policies; Record Access Procedure; Notification Procedure; and Appendix. 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: Comments may be submitted through www.Regulations.gov or mailed to, Director, National Data Systems (10A7), Austin Information Technology Center,

1615 Woodward Street, Austin, Texas 78772. Comments should indicate that they are submitted in response to “VHA Corporate Data Warehouse-VA (172VA10P2)”. Comments received will be available at regulations.gov for public viewing, inspection or copies.

FOR FURTHER INFORMATION CONTACT: 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 Name is changed to “VHA Corporate Data Warehouses-VA” to clearly indicate that there are multiple data warehouses covered under the system of records notice.

The System Number is changed from 172VA10P2 to 172VA10A7 to reflect the current organizational alignment.

The System Location is being updated to reflect the address locations for VA National Data Centers and contracted data centers are listed in Appendix A.

System Manager, Record Access Procedure, and Notification Procedure is being amended to replace 10P2 and 10P2C with 10A7.

The Purpose of the System is being amended to include reporting purposes for Veterans Authorizations and Preferences and other Veterans Health Information Exchange (VHIE) reporting needs and health care operations.

Categories of Records in the System is being amended to change number 1 from 24VA10P2 and 121VA10P2 to 24VA10A7 and 121VA10A7 respectively, also including Virtual Lifetime Electronic Record (VLER)-VA (168VA10P2). Number 3 and number 4 will replace 114VA16 with 114VA10D. Number 7 to add Health care practitioners' name and other demographic information related to position.

Routine use #5 has been amended to remove General Services Administration (GSA).

The Routine Uses of Records Maintained in the System has been amended by amending the language in Routine Use #6 which states that disclosure of the records to the Department of Justice (DoJ) is a use of the information contained in the records that is compatible with the purpose for which VA collected the records. VA may disclose records in this system of records in legal proceedings before a court or administrative body after determining that the disclosure of the records to the court or administrative body is a use of the information contained in the records that is compatible with the purpose for which VA collected the records. This routine use will now state that 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.

Routine use #20 has been amended by clarifying the language to state, "VA may disclose any information or records to appropriate agencies, entities, and persons when (1) VA suspects or has confirmed that there has been a breach of the system of

records; (2) VA has determined that as a result of the suspected or confirmed breach there is a risk to individuals, VA (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, or persons 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 24 is being added to state, "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. VA needs this routine use for the data breach response and remedial efforts with another Federal agency."

Routine use 25 is also being added to state, "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." This routine use permits disclosure of information for quality assessment audits received by Healthcare Effectiveness Data and Information Set (HEDIS) or similar auditors.

Physical, Procedural and Administrative Safeguards is being updated to clarify that item 1-3 apply to VA data warehouses. In addition, item 5 is added to state,

“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.”

VA Appendix A is being amended to remove the Regional Data Warehouses (RDW), Region 2, Region 3, and Region 4. These RDW’s are being discontinued as the data from these warehouses will be sourced under the Corporate Data Warehouse (CDW). The name of the Veterans Informatics, Information and Computing Infrastructure (VINCI) program is also being changed to VA Informatics and Computing Infrastructure to reflect the current name description. In addition, 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 is being added to Appendix A.

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 for Information and Technology and Chief Information Officer, approved this document on May 20, 2020 for publication.

Dated: August 20, 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: ‘‘VHA Corporate Data Warehouses-VA’’ (172VA10A7)

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: Records are located in VA National Data Centers and contracted data centers listed in Appendix A.

SYSTEM MANAGER(S): Officials responsible for policies and procedures: Assistant Deputy Under Secretary for Health Informatics (10A7), Department of Veterans Affairs, 810 Vermont Avenue, NW, Washington, DC 20420. Officials maintaining this system of records: Director, National Data Systems (10A7), Austin Information Technology Center, 1615 Woodward Street, Austin, Texas 78772.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: Title 38, United States Code, Section 501.

PURPOSE(S) OF THE SYSTEM: The records and information may be used for clinical decision support, mobile applications presenting patient data, 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; for the planning, distribution and utilization of resources; to monitor the performance of Veterans Integrated Service Networks (VISNs); and to allocate clinical and administrative support to patient medical care. The data may be used for VA’s extensive research programs in accordance with VA policy and to monitor for bio-terrorist activity. In addition, the data may be used to assist in workload allocation for

patient treatment services including provider panel management, nursing care, clinic appointments, surgery, diagnostic and therapeutic procedures; to plan and schedule training activities for employees; for audits, reviews and investigations conducted by the Network Directors Office and VA Central Office; for quality assurance audits, reviews and investigations; for law enforcement investigations; for reporting purposes for Veterans Authorizations and Preferences and other Veterans Health Information Exchange (VHIE) reporting needs; and for health care operations and for personnel management, evaluation and employee ratings, and performance evaluations.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: The records contain information for all individuals:

(1) receiving health care from VHA;

(2) receiving health care from Department of Defense (DoD);

(3) providing the health care;

(4) or working for VA or DoD.

Individuals encompass Veterans, members of the armed services, current and former employees, trainees, caregivers, contractors, sub-contractors, consultants, volunteers, and other individuals working collaboratively with VA.

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

1. Patient health record detailed information, including information from Patient Medical Records—VA (24VA10A7) and Patient National Databases—VA (121VA10A7) and from Virtual Lifetime Electronic Record (VLER)-VA (168VA10P2);

2. The record may include identifying information (e.g., name, birth date, death date, admission date, discharge date, gender, Social Security number, taxpayer identification number); address information (e.g., home and/or mailing address, home telephone number, emergency contact information such as name, address, telephone number, and relationship); prosthetic and sensory aid serial numbers; health record numbers; integration control numbers; information related to medical examination or treatment (e.g., location of VA medical facility providing examination or treatment, treatment dates, medical conditions treated or noted on examination); information related to military service and status;

3. Patient health insurance information, including information from Revenue Program Billing and Collection Records—VA (114VA10D);

4. Medical benefit and eligibility information, including information from Revenue Program Billing and Collection Records—VA (114VA10D);

5. Patient aggregate workload data such as admissions, discharges, and outpatient visits; resource utilization such as laboratory tests, x-rays, pharmaceuticals, prosthetics and sensory aids; employee workload and productivity data;

6. Information on services or products needed in the provision of medical care (i.e., pacemakers, prosthetics, dental implants, hearing aids, etc.); data collected may include vendor name and address, details about and/or evaluation of service or product, price/fee, dates purchased and delivered;

7. Health care practitioners' name, identification number and other demographic information related to position;

8. Employees salary and benefit information;

9. Financial Information from the Financial Management System;

10. Human resource information including employee grade, salary, and tour of duty;

11. Compensation and pension determinations, Veteran eligibility, and other information associated administering Veteran benefits by the Veterans Benefit Administration;

12. Data from other Federal agencies;

13. Patient self-entered data (online forms, etc.).

RECORD SOURCE CATEGORIES: Information in this system of records is provided by Veterans, VA employees, VA computer systems, Veterans Health Information Systems and Technology Architecture (VistA), contracted computer systems, VA Medical Centers, VA Program Offices, VISNs, DoD, other Federal Agencies and non-VA health care providers.

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 any information in this system, except the names and home addresses of Veterans and their dependents, which is relevant to a suspected 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, to a Federal, State, local, tribal, or foreign agency charged with the responsibility of investigating or prosecuting such violation, or charged with enforcing or implementing the statute, regulation, rule or order. 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 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 an individual's eligibility, care history, or other benefits.

3. Disclosure may be made to an agency in the executive, legislative, or judicial branch, or the District of Columbia's government in response to its request or at the initiation of VA, in connection with disease-tracking, patient outcomes, bio-surveillance, or other health information required for program accountability.

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

5. Disclosure may be made to National Archives and Records Administration (NARA) in records management inspections and other activities conducted under Title 44, Chapter 29, of the U.S.C.

6. 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.

7. Records from this system of records may be disclosed to a Federal agency or to a State or local government licensing board and/or to the Federation of State Medical Boards or a similar nongovernment entity which maintains records concerning individuals' 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 agency to obtain information relevant to an agency decision concerning the hiring, retention or termination of an employee.

8. Records from this system of records may be disclosed to inform a Federal agency, licensing boards or the appropriate non-government 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.

9. For program review purposes and the seeking of accreditation and/or certification, disclosure may be made to survey teams of the Joint Commission (JC), 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. VA health care facilities undergo certification and accreditation by several national accreditation agencies or boards to comply with regulations and good medical practices.

10. Disclosure may be made to a 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 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. 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.

12. Disclosure may be made to the VA-appointed representative of an employee of 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.

13. 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.

14. Disclosure may be made to the Equal Employment Opportunity Commission when requested in connection with investigations of alleged or possible discrimination examination of Federal affirmative employment programs, or for other functions of the EEOC as authorized by law or regulation.

15. To disclose to the Federal Labor Relations Authority (including its General Counsel) information related to the establishment of jurisdiction, the investigation and resolution of allegations of unfair labor practices, or information in connection with the resolution of exceptions to arbitration awards when a question of material fact is raised; to disclose

information in matters properly before the Federal Services Impasses Panel, and to investigate representation petitions and conduct or supervise representation elections.

16. Disclosure of health 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 when approved in accordance with VA policy.

17. Disclosure of name(s) and address(s) of present or former personnel of the armed services, and/or 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.

18. Disclosure of relevant information may be made to individuals, organizations, private or public agencies, etc., with whom VA has a contract or agreement to perform such services as VA may deem practicable for the purposes of laws administered by VA, in order for the contractor or subcontractor to perform the services of the contract or agreement.

19. 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.

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 from this system to a Federal agency for the purpose of conducting research and data analysis to perform a statutory purpose of that Federal agency upon the prior written request of that agency, provided that there is legal authority under all applicable confidentiality statutes and regulations to provide the data and VA has determined prior to the disclosure that VA data handling requirements are satisfied.

22. VA may disclose information from this system of records to OMB for the performance of its statutory responsibilities for evaluating Federal programs.

23. VA may disclose this information to the DoD for joint ventures between the two Departments to promote improved patient care, better health care resource utilization, and formal research studies.

24. 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.

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.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Records are maintained on Storage Area Networks.

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: Records are maintained and disposed of in accordance with records disposition authority approved by the Archivist of the United States. The records are disposed of in accordance with General Records Schedule 20, item 4.

Item 4 provides for deletion of data files when the agency determines that the files are no longer needed for administrative, legal, audit, or other operational purposes.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

1. Access to and use of VA data warehouses are limited to those persons whose official duties require such access, and the VA has established security procedures to ensure that access is appropriately limited. Information security officers and system

data stewards review and authorize data access requests. VA regulates data warehouse access with security software that relies on network authentication. VA requires information security training to all staff and instructs staff on the responsibility each person has for safeguarding data confidentiality.

2. Physical access to computer rooms housing VA data warehouses are restricted to authorized staff and protected by a variety of security devices. Unauthorized employees, contractors, and other staff are not allowed in computer rooms.

3. Data transmissions between VA operational systems and VA data warehouses maintained by this system of record are protected by state-of-the-art telecommunication software and hardware. This may include firewalls, intrusion detection devices, encryption, and other security measures necessary to safeguard data as it travels across the VA Wide Area Network.

4. In most cases, copies of back-up computer files are maintained at off-site locations.

5. 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 contained in this system of records may write to the Director of National Data Systems (10A7), Austin Information Technology Center, 1615 Woodward Street, Austin, Texas 78772. Inquiries should include the person's

full name, Social Security number, location and dates of employment or location and dates of treatment, and their return address.

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 Director of National Data Systems (10A7), Austin Information Technology Center, 1615 Woodward Street, Austin, Texas 78772. Inquiries should include the person's full name, Social Security number, location and dates of employment or location and dates of treatment, and their return address.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

HISTORY: Last full publication provided in 79 FR 4377 dated January 27, 2014.

VA APPENDIX A:

Database Name	Location
Corporate Data Warehouse	Austin Information Technology Center, 1615 Woodward Street, Austin, TX 78772.
VA Informatics and Computing Infrastructure (VINCI)	Austin Information Technology Center 1615 Woodward Street Austin, TX 78772
HealtheIntent at Cerner Technology Centers (CTC)	Primary Data Center Kansas City, MO Continuity of Operations/Disaster Recovery (COOP/DR) Data Center Lee Summit, MO

[FR Doc. 2020-18653 Filed: 8/24/2020 8:45 am; Publication Date: 8/25/2020]