



Privacy Act of 1974; System of Records

AGENCY: Department of Veterans Affairs (VA), Veterans Health Administration (VHA).

ACTION: Notice of a Modified System of Records.

SUMMARY: As required by the Privacy Act of 1974, 5 U.S.C. 552a(e), notice is hereby given that the Department of Veteran Affairs (VA) is amending the system of records currently entitled “Virtual Lifetime Electronic Record (VLER)-VA” (168VA10P2) as set forth in the Federal Register 77 FR 27859. VA is amending the system of records by revising the System Name; System Number; System Location; System Manager; Purpose; Categories of Individuals Covered by the System; Category of Records in the System; Records Source Category; Routine Uses of Records Maintained in the System; Policies and Practices for Storage of Records; Policies and Practices for Retrievability of Records; Policies and Practices for Retention and Disposal of Records; Administrative, Technical, and Physical Safeguards; and Record Access Procedure. VA is republishing the system notice in its entirety.

DATES: Comments on the amendment of this 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 amended 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 Ave. NW, Room 1064, Washington, DC 20420; or by fax to (202) 273-9026 (not a toll-free number). Comments should indicate that they are submitted in response to Health Information Exchange (HIE)-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. (This is not a toll-free number.) In addition, comments may be viewed online at www.Regulations.gov.

FOR FURTHER INFORMATION CONTACT: Office of Information and Technology (OI&T), Privacy Officer, Department of Veterans Affairs, 1100 First Street, NE, Washington, D.C. 20420, telephone (202) 632-7524. (This is not a toll-free number.)

SUPPLEMENTARY INFORMATION: The System Name is being changed from “Virtual Lifetime Electronic Record (VLER)-VA” to “Health Information Exchange-VA”.

The System Number is changed from 168VA10P2 to 168VA005 to reflect the current departmental alignment.

The System Location is being amended to add Philadelphia Information Technology Center, 3900 Woodland Avenue, Philadelphia, PA 19104; Amazon Web Services (AWS) Government Cloud (GovCloud), 410 Terry Ave North, Seattle, WA 98109 and 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.

The System Manager is being amended to replace Director Standards and Interoperability, Chief Health Informatics Office/Office of Informatics and Analytics/Veterans Health Information with Chief Technology & Integration Officer Veterans Affairs Office of Electronic Health Record Modernization at 811 Vermont Avenue Office 5084 Washington, DC 20420.

The Purpose is being amended to remove VLER/Nationwide Health Information Network (NwHIN) partners. Being added is information stored in VA computer systems, such as the Data Access Service (DAS) and VA contracted computer systems which

are used for benefit and claims adjudication as well as data for VA Data Sharing and Interoperability Initiatives with VA partners. These partners include, but are not limited to, Veteran Health Information Exchange (VHIE) external partners, The Sequoia Project, eHealth Exchange partners, Direct Partners, Carequality, CommonWell, VA-approved third party payers and contracted providers, educational affiliates, Veteran Service Organizations (VSOs), VA AppCatalog Mobile applications, federal agencies (to include Indian Health Service, Bureau of Prisons, Internal Revenue Service (IRS), Social Security Administration (SSA), Department of Defense (DoD), Health and Human Services, and others), and State Registries. This section adds “for health care operations and reimbursement for care provided” as purposes of the data.

The Categories of Individuals Covered by the System is being amended to remove caveat of VA employees who access information through VLER to state “VA employees” and add VA contractors. In addition, other VA patients, VA contracted and private providers and payers, VA contracted Health Information Handlers, VSO staff, and VA system integrators who resolve information technology (IT) trouble tickets, DoD providers, educational affiliate staff with approved VA access.

The Categories of Records in the System is being amended to add scanned & imported paper records & non-radiology images, Service Treatment Record (STR) (and transformed DAS STR), Community Health Summaries –DoD, Questionnaires and Deployment Assessments (Armed Forces Health Longitudinal Technology Application (AHLTA) only), Contact Logs, Diet, Patient Mood and Immunizations as examples under patient demographic and health information from external health care providers and VHIE external partners; and opt-out forms, participate in sharing after opting out forms and future forms developed for VHIE as examples under information on Veterans’ preferences regarding the sharing of their health information. This section will add

information on health information exchange and Direct users, claims adjudication information, research records, education information and device or patient created data.

The Records Source Category is being amended to replace 79VA19 with 79VA10A7, 121VA19 with 121VA10A7, and 24VA19 with 24VA10A7. Federal and non-federal VLER/NwHIN partners and DoD is being removed and replaced with VHIE external partners. This section will add eHealth Exchange partners, Carequality and CommonWell, Direct Messaging providers, non-VA care providers, patient or individual device generated data through a VA AppCatalog Mobile application, homeless shelters, government agencies such as DoD, SSA, IRS, Health and Human Services, Bureau of Prisons, Indian Health Services and others, and State Registries.

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 #15 is being added to state, "Disclosure of Veteran identifiers and demographic information (e.g., name, SSN, address, date of birth) may be made to an

organization with whom VA has a documented partnership, arrangement or agreement (e.g., Health Information Exchange (HIE), Health Information Service Provider (HISP) Direct, CommonWell Health Alliance network), for the purpose of identifying and correlating patients.” VA needs this ability to share demographic information for correlation and identification purposes.

Routine use #16 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 #17 is being added to state, 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. VA must be able to provide information to FLRA to comply with the statutory mandate under which it operates.

Policies and Practices for Storage of Records is being amended to remove storage area network (SAN) and mobile devices and add electronic storage media

including, but not limited to, magnetic tape, disk, laser optical media and solid-state flash media.

The Retrievability section is being amended to add electronic data interchange personal identifier (EDIPI), medical record number, problem list, geographic location and other demographic, medical or medication information.

Policies and Practices for Retention and Disposal is being amended to replace 'in accordance with the records disposition authority approved by the Archivist of the United States, health information stored on electronic media storage is maintained for seventy-five (75) years after the last episode of patient care and then deleted' with GRS 4.3 Items 020, 030, 031 and Electronic Health Records schedule, National Archives and Records Administration (NARA) job # N1-15-02-3, item 1a, 1b, 2, 3, 4, 5, 6.

The Administrative, Technical and Physical 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."

Records Access Procedure is being amended to replace Director Standards and Interoperability, Chief Health Informatics Office/Office of Informatics and Analytics/Veterans Health Information, with Director, VHIE, Office of Health Informatics/Veterans Health Administration and to add "or contact their closest VA Medical Center (VAMC)". Being added to this section is that requests should contain the full name, address and telephone number of the individual making the inquiry.

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 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: "Health Information Exchange-VA" (168VA005)

SECURITY CLASSIFICATION: None.

SYSTEM LOCATION: Records are maintained at Department of Veterans Affairs (VA), Austin Information Technology Center (AITC), 1615 Woodward Street, Austin, TX 78772, Philadelphia Information Technology Center (PITC), 3900 Woodland Avenue, Philadelphia, PA 19104; Amazon Web Services(AWS) Government Cloud (GovCloud), 410 Terry Ave North, Seattle, WA 98109; and 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): Official maintaining this system of records and responsible for policies and procedures is Chief Technology & Integration Officer Veterans Affairs, Office of Electronic Health Record Modernization at 811 Vermont Avenue Office 5084 Washington, DC 20420.

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

PURPOSE(S) OF THE SYSTEM: The records and information stored in VA computer systems, including the Data Access Service (DAS) and VA contracted systems, such as Cerner products, may be used for the ongoing communication of current healthcare, benefit and claims adjudication data, for VA Data Sharing and interoperability initiatives with VA partners. These partners include, but are not limited to, Veteran Health Information Exchange (VHIE) external partners, The Sequoia Project and eHealth Exchange partners, Direct Partners, Carequality, CommonWell, VA-approved third party payers and contracted providers, educational affiliates, Veteran Service Organizations (VSOs), VA AppCatalog Mobile applications, State Registries and federal agencies (to include Indian Health Service, Bureau of Prisons, IRS, DoD, Health and Human

Services, and others). This data is used to promote improved quality of patient care, reduce duplicative ordering of tests, services and pharmaceuticals; for statistical analysis to produce various management, workload tracking, and follow-up reports; to track 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 (VISN); to allocate clinical and administrative support to patient to include but not limited to Healthcare treatment, disability adjudication, and benefits, and for health care operations and reimbursement for care provided.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: The records contain information on Veterans and the family members or caregivers; members of the armed services, Reserves or National Guard, other VA patients, VA employees and contractors, VA contracted and private providers and payers, VA contracted Health Information Handlers, VSO staff, DoD providers, education affiliate staff with approved VA access, and VA system integrators who resolve information technology (IT) trouble tickets.

CATEGORIES OF RECORDS IN THE SYSTEM: The records may include patient demographic information (e.g., electronic data interchange personal identifier (EDIPI), name, address, phone numbers, date of birth, social security number); patient demographic and health information from external health care providers and VHIE external partners, e.g., medications, allergies, consultations and referrals, history and physicals, discharge summaries, diagnostic studies, procedures notes, advanced directives, problem lists, laboratory results, lists of procedures and encounters, scanned & imported paper records & non-radiology images, Service Treatment Records (STR) (and transformed DAS STR), Community Health Summaries –DoD, Questionnaires and Deployment Assessments (Armed Forces Health Longitudinal Technology Application

[AHLTA] only), Contact Logs, Diet, Patient Mood, and immunizations, benefits information (e.g., disability rating, service connection rating), information on Veterans' preferences regarding the sharing of their health information (e.g., authorizations, restriction requests, revocation of authorizations, opt-out forms, participate in sharing after opting out forms and future forms developed for VHIE, information on VHIE and Direct users, claims adjudication information, research records and education information, as well as device- or patient- created data relating to the above.

RECORD SOURCE CATEGORIES: Information in this system of records is provided by Veterans and their family members or caregivers, members of the Armed Services, Reserves or National Guard, other VA patients, VA employees and contractors, VA computer systems, Veterans Health Information Systems and Technology Architecture (VistA)-VA (79VA10A7), National Patient Databases-VA (121VA10A7), Patient Medical Record—VA (24VA10A7), VA contracted computer systems, HIE external partners, Direct Messaging providers, non-VA care providers, VA AppCatalog Mobile application, homeless shelters, State Registries, and government agencies such as DoD, SSA, IRS, Health and Human Services, Bureau of Prisons, Indian Health Services and others.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING

CATEGORIES OF USERS AND 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 of information to a health participant for the purpose of providing care or treatment to VA patients, reimbursement for health care services, or determining eligibility for government disability benefits.

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 NARA and the General Services Administration (GSA) in records management inspections conducted under authority of Title 44, Chapter 29, of the United States Code (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. 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.

8. VA may disclose information to officials of the Merit Systems Protection Board (MSPB), or the Office of 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 authorized by law.

9. VA may disclose information to the Equal Employment Opportunity Commission when requested in connection with investigations of alleged or possible discriminatory practices, examination of Federal affirmative employment programs, or for other functions of the Commission as authorized by law or regulation.

10. VA may disclose to the Fair Labor Relations Authority (FLRA) (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 Impasse Panel, and to investigate representation petitions and conduct or supervise representation elections.

11. Disclosures of relevant information may be made to individuals, organizations, private or public agencies, or other entities with whom VA has a contract or agreement or where there is a subcontract to perform the 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.

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

13. VA may disclose any information or records to appropriate agencies, entities, and persons when (1) VA suspects or has confirmed that 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.

14. 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 the VA data handling requirements are satisfied.

15. Disclosure of Veteran identifiers and demographic information (e.g., name, SSN, address, date of birth) may be made to an organization with whom VA has a documented partnership, arrangement or agreement (e.g., Health Information Exchange (HIE), Health Information Service Provider (HISP) Direct, CommonWell Health Alliance network), for the purpose of identifying and correlating patients.

16. VA may disclose information from this system to another Federal agency or Federal entity, when VA determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

17. 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.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Records are maintained on electronic storage media including, but not limited to, magnetic tape, disk, laser optical media and solid-state flash media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records are retrieved by electronic data interchange personal identifier (EDIPI), problem list, geographic location and other demographic, medical or medication information, name, social security number or other assigned identifiers of the individuals on whom they are maintained. For reporting purposes records can also be retrieved by Internal Control Number (ICN).

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: GRS 4.3 Items 020, 030, 031 and Electronic Health Records schedule, NARA job # N1-15-02-3, item 1a, 1b, 2, 3, 4, 5, 6.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

1. Access to and use of national administrative databases, warehouses, and data marts are limited to those persons whose official duties require such access, and the VA implements Federal Information Security Management Act mandated security protocols or, when appropriate, 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 access with security software that authenticates users and requires individually unique codes and passwords. VA provides 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 national administrative databases, warehouses, and data marts is restricted to authorized staff and protected by a variety of security devices. Unauthorized employees, contractors, and other staff are not allowed in computer rooms. The Federal Protective Service or other security personnel provide physical security for the buildings housing computer rooms and data centers.

3. Data transmissions between operational systems and national administrative databases, warehouses, and data marts 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.

6. The AWS GovCloud infrastructure as a service cloud-computing environment has been authorized at the high-impact level under the Federal Risk and Authorization Management Program (FedRAMP). The secure site-to-site encrypted network connection is limited to access via the VA trusted internet connection (TIC).

RECORD ACCESS PROCEDURES: Individuals seeking information regarding access to and contesting of records in this system may write the Director, VHIE, Office of Health Informatics/Veterans Health Administration at VACO, 810 Vermont Avenue NW,

Washington, DC 20420, or contact their closest VAMC. Requests should contain the full name, address and telephone number of the individual making the inquiry.

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

NOTIFICATION PROCEDURES: Individuals who wish to determine whether this system of records contains information about them should contact their closest VAMC.

Inquiries should include the person's full name, social security number, location and dates of treatment or location and dates of employment and their return address.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

HISTORY: Last full publication provided in 77 FR 27859 dated May 11, 2012.

[FR Doc. 2021-01516 Filed: 1/22/2021 8:45 am; Publication Date: 1/25/2021]