DEPARTMENT OF VETERAN AFFAIRS

Privacy Act of 1974; System of Records

AGENCY: Department of Veteran Affairs, Office of General Counsel.

ACTION: Notice of a modified system of records.

SUMMARY: VA is amending the current system of record (SOR) (173VA005OP2) the Department of Veterans Affairs (VA) Mobile Application Environment (MAE) by renaming it VA Enterprise Cloud – Mobile Application Platform (VAEC-MAP). The VA MAE has been replaced by VAEC-MAP. VA changed Information Technology providers from Terremark to Amazon Web Services (AWS). In addition, the system location has changed. We are restating the routine uses in full and revising the language to make routine uses align with recent Office of Management and Budget (OMB) guidelines and making minor editorial changes to more clearly articulate uses and to align with standardized VA routine use language. VA is republishing the system notice in its entirety. VAEC-MAP is a cloud hosted system that provides the infrastructure and hosting platform for Mobile Shared Services (i.e. common services used for Mobile applications) and web components of applications used on Mobile devices. Mobile applications connect to VA enterprise services using the VAEC MAP Mobile Shared Services. Mobile applications such as Video Visits Service (VVS), Veteran Affairs Online Scheduling (VAOS), Patient Viewer (PV), and Veteran Affairs Video Connect (VVC) leverage this platform, pipeline, and hosting environment to provide a coordinated scheduling and notification capability to Staff and Veterans among other resources. VAEC-MAP uses the VAEC AWS cloud environment to provide an automated platform and pipeline for the development and hosting of production VA mobile applications. VAEC Common shared services, such as BigFix, Nessus, Splunk, and AD, are leveraged to provide security control implementation and system security visibility to the VA teams responsible for ensuring the security of VA systems. Administrative users of the VAEC-MAP

environment must authenticate to the VA (Citrix Access Gateway or RESCUE) via Personal Identification Verification before using access keys and Identity and Access Management multi-factor authentication to gain access into the environment. System Administrators access the VA network using VA managed Government Furnished Equipment through Virtual Private Network connections to the VA Local Area Network and are authenticated using an Active Directory system managed by VA Network Security Operations Center. Encrypted communications protocols and ports are employed to protect information flowing across the VA network. All system access is managed via Role Based Access Control deployed separately within the environment and adheres to the Least Privilege Principal for all user accounts regardless of role. VAEC-MAP user account management adheres to VA policy or exceeds VA Policy where applicable.

DATES: Comments on this revision of a system of records must be received no later than 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, these revisions will become effective a minimum of 30 days after date of publication in the Federal Register. If VA receives public comments, VA shall review the comments to determine whether any changes to the notice are necessary.

ADDRESSES: Comments may be submitted through www.Regulations.gov or mailed to VA Privacy Service, 810 Vermont Avenue, NW, (005R1A), Washington, DC 20420. Comments should indicate that they are submitted in response to the VA Mobile Application Environment (MAE)-VA (173VA005OP2). Comments received will be available at regulations.gov for public viewing, inspection or copies.

FOR FURTHER INFORMATION CONTACT: For submitting general questions and requests about this revised system please direct correspondence to Mark Ennis (System Owner) [Veteran Affairs 102 2nd Avenue South, Suite 300, St. Petersburg, FL 33701], or at Mark.Ennis@va.gov, and 727-212-0827 (This is not a toll-free number).

SUPPLEMENTARY INFORMATION: VA is amending the current system of record (SOR) (173VA005OP2) the Department of Veterans Affairs (VA) Mobile Application Environment (MAE) by renaming it VA Enterprise Cloud – Mobile Application Platform (VAEC-MAP) and updating the system location.

Signing Authority

The Senior Agency Official for Privacy, or designee, approved this document and authorized the undersigned to sign and submit the document to the Office of the Federal Register for publication electronically as an official document of the Department of Veterans Affairs. Dominic A. Cussatt, Acting Assistant Secretary of Information and Technology and Chief Information Officer, approved this document on May 26, 2021 for publication.

Dated: November 3, 2021.

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: ‘‘VA Enterprise Cloud – Mobile Application Platform (Cloud) Assessing (VAEC-MAP) (173VA005OP2)

SECURITY CLASSIFICATION: Sensitive But Unclassified (SBU)

SYSTEM LOCATION: The office responsible for the system is the Department of Veteran Affairs, Office of General Counsel, 810 Vermont Ave., NW, Washington, DC, 20420 and Amazon Web Services (AWS) – Seattle, WA

SYSTEM MANAGER(S): Mark Ennis (System Owner) Veteran Affairs 102 2nd Avenue South, Suite 300, St. Petersburg, FL 33701, or at Mark.Ennis@va.gov, and 727-212-0827

(This is not a toll-free number).

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

PURPOSE(S) OF THE SYSTEM: The records and information will be used to provide a repository for the clinical and administrative information that is collected, retrieved, or displayed from within a VA mobile or Web application. The purpose of use will include, but not be limited to, health care treatment information, disability adjudication, and benefits to the Veteran both within the VA Medical Center and in sharing with partners who are participating through the eHealth Exchange in VA's Mobile pilots and subsequent public and enterprise rollout of new applications. Data may also be used at an aggregate, non-personally identifiable level to track and evaluate local or national health and benefits initiatives and preventative-care measures, such as detecting outbreaks of flu or other diseases, detection of antibiotic resistance bacteria, etc. These data may be used for such purposes as scheduling patient treatment services, including nursing care, clinic appointments, surveys, diagnostic, and therapeutic procedures. These data may also be used for the purpose of health care operations, such as producing various management and patient follow up reports; responding to patient and other inquiries; for epidemiological research and other health care-related studies; statistical analysis, resource allocation and planning; providing clinical and administrative support to patient medical care; determining entitlement and eligibility for VA benefits; processing and adjudicating benefit claims by Veterans Benefits Administration Regional Office staff; for audits, reviews, and investigations conducted by staff of VA Central Office and VA's OIG; sharing of health information between and among VHA, DoD, IHS, and other Government and private industry health care organizations; law enforcement investigations; quality assurance audits, reviews, and investigations; personnel management and evaluation; employee ratings and performance evaluations; and employee disciplinary or other adverse action, including

discharge; advising health care professional licensing or monitoring bodies or similar entities of activities of VA and former VA health care personnel.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: The records contain information on Veterans, Veteran beneficiaries, Veteran caregivers, members of the Armed Forces, Reserves and National Guard, and other VA customers in addition to VA authorized users (e.g., VA employees, VA contractors, VA volunteers, and other individuals permitted to have access to VA IT systems).

CATEGORIES OF RECORDS IN THE SYSTEM: The records may include information related to data entered through Web and mobile applications developed and maintained by VA, accessed and updated by the individuals covered by the system as well as by VA-authorized users. The records may contain demographics, personal information (e.g., name, social security numbers, physical address, phone number, email address), health-related information (e.g., vital signs, allergies, medications, health related history, health assessments), benefit-related information, information provided to VA for the potential provision of services and benefits, military history and services, preferences for authorizing the sharing of their health information (e.g., electronic surrogate authorizations, electronic surrogate revocations). The records may include identifiers such as VA's integration control number. The information will be primarily benefits and health-related but may include other information such as customer entered updates to demographic information.

RECORD SOURCE CATEGORIES: Information in this system of records is provided by Veterans and their beneficiaries or caregivers, members of the Armed Services, Reserves or National Guard; VA employees, other VA-authorized users (e.g., DoD), and information from VA computer systems and databases include, but not limited to, Veterans Health Information Systems and Technology Architecture (VistA)- VA (79VA10P2) and National Patient Databases-VA (121VA10P2), VAMCs, Federal and non-Federal VLER/eHealth Exchange partners, and DoD.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

1. Congress

VA may disclose information to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

2. Data Breach Response and Remediation, for VA

VA may disclose information 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 of harm 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, and persons is reasonably necessary to assist in connection with VA's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm…

3. Data Breach Response and Remediation, for Another Federal Agency

VA may disclose information to another Federal agency or Federal entity, when VA determines that the 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.

4. Law Enforcement

VA may disclose information that, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, to a Federal, state, local, territorial, tribal, or foreign law enforcement authority or other appropriate entity charged with the responsibility of investigating or prosecuting such

violation or charged with enforcing or implementing such law. The disclosure of the names and addresses of veterans and their dependents from VA records under this routine use must also comply with the provisions of 38 U.S.C. 5701.

5. DoJ for Litigation or Administrative Proceeding

VA may disclose information to the Department of Justice (DoJ), or in a proceeding before a court, adjudicative body, or other administrative body before which VA is authorized to appear, when:

(a) VA or any component thereof;

(b) Any VA employee in his or her official capacity;

(c) Any VA employee in his or her official capacity where DoJ has agreed to represent the employee; or

(d) The United States, where VA determines that litigation is likely to affect the agency or any of its components,

is a party to such proceedings or has an interest in such proceedings, and VA determines that use of such records is relevant and necessary to the proceedings.

6. Contractors

VA may disclose information to contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for VA, when reasonably necessary to accomplish an agency function related to the records.

7. OPM

VA may disclose information to the Office of Personnel Management (OPM) in connection with the application or effect of civil service laws, rules, regulations, or OPM guidelines in particular situations.

8. EEOC

VA may disclose information to the Equal Employment Opportunity Commission (EEOC) in

connection with investigations of alleged or possible discriminatory practices, examination of Federal affirmative employment programs, or other functions of the Commission as authorized by law.

9. FLRA

VA may disclose information to the Federal Labor Relations Authority (FLRA) in connection with: the investigation and resolution of allegations of unfair labor practices, the resolution of exceptions to arbitration awards when a question of material fact is raised; matters before the Federal Service Impasses Panel; and the investigation of representation petitions and the conduct or supervision of representation elections.

10. MSPB

VA may disclose information to the Merit Systems Protection Board (MSPB) and the Office of the Special Counsel 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.

11. NARA

VA may disclose information to NARA in records management inspections conducted under 44 U.S.C. 2904 and 2906, or other functions authorized by laws and policies governing NARA operations and VA records management responsibilities.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Records are stored in the AWS Cloud.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records may be retrieved by name, social security number, VA's integration control number, or other assigned identifiers of the individuals for whom they are maintained.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Records from this system that are needed for audit purposes will be disposed of 6 years after a

user's account becomes inactive. Routine records will be disposed of when the agency determines they are no longer needed for administrative, legal, audit, or other operational purposes. These retention and disposal statements are pursuant to NARA General Records Schedules GRS 20, item 1c and GRS 24, item 6a.

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 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 access with security software that authenticates users and requires individually-unique codes and passwords. VA requires information security training for 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. 3. Data transmissions between operational systems and national administrative databases, warehouses, and data marts maintained by this system of record are protected by stateof-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.

RECORD ACCESS PROCEDURES: Individuals seeking information regarding access to and contesting of records in this system may write the Director of VA Connected Health, VHA Office of Informatics and Analytics, Department of Veterans Affairs, 810 Vermont Avenue NW., Washington, DC 20420. Inquiries should, at a minimum, include the person's

full name, social security number, type of information requested or contested, their return address, and phone number.

CONTESTING RECORD PROCEDURES: Individuals seeking information regarding access to and contesting of records in this system may write the Director of VA Connected Health, VHA Office of Informatics and Analytics, Department of Veterans Affairs, 810 Vermont Avenue NW., Washington, DC 20420. Inquiries should, at a minimum, include the person's full name, social security number, type of information requested or contested, their return address, and phone number.

NOTIFICATION PROCEDURES: Individuals who wish to determine whether this system of records contains information about them should contact the Director of VA Connected Health, VHA Office of Informatics and Analytics, Department of Veterans Affairs, 810 Vermont Avenue NW., Washington, DC 20420 or via the Web at http://mobilehealth.va.gov. Inquiries should include the person's full name, social security number, and their return address.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: N/A

HISTORY: VA Mobile Application Environment (MAE)-VA (173VA005OP2) last full publication provided in 78 FR 66806 dated November 6, 2013.

[FR Doc. 2021-24368 Filed: 11/5/2021 8:45 am; Publication Date: 11/8/2021]