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: Pursuant to the Privacy Act of 1974, notice is hereby given that the VA is modifying the system of records titled “Veterans Crisis Line Database-VA” (158VA10NC5). This system of records is used to document contact interactions with the Veterans Crisis Line (VCL), and to assist with follow-up care based on those interactions. Statistical evaluation data from these records will be used for developing suicide prevention efforts, program and quality assurance improvement, and providing reports to VA officials, Congressional members and the public.

DATES: Comments on this modified 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, the modified system of records 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, (005X6F), Washington, DC 20420. Comments should indicate that they are submitted in response to “Veterans Crisis Line Database-VA” (158VA10NC5). Comments received will be available at regulations.gov for public viewing, inspection or copies.

FOR FURTHER INFORMATION CONTACT: Stephania Griffin, VHA Chief Privacy Officer, Department of Veterans Affairs, 810 Vermont Avenue, NW, Washington, DC 20420; telephone 704-245-2492 (Note: This is not a toll-free number).

SUPPLEMENTARY INFORMATION: VA is modifying the system of records by revising the System Name, System Number, System Location, System Manager, Authority for Maintenance in the System, Purpose of the System, Categories of Individuals Covered by this System, Categories of Records in the System, Records Source Categories, 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, and Administrative, Technical and Physical Safeguards.

VA is modifying the system of records by revising the System Name, Number and System Location.

The System Name will be changed from “Veterans Crisis Line Database-VA” to “Veterans Crisis Line Records-VA”.

The System Number will be changed from 158VA10NC5 to 158VA10 to reflect the current VHA organizational routing symbol.

The System Location is being updated to remove “back-up copies of the database are maintained in accordance with VA OIT enterprise management policies.” This section will include verbiage indicating that records are maintained at the Health Resource Center (HRC) in Topeka, Kansas and “Additional and supplemental data is stored within the Microsoft Government Community Cloud.”

The System Manager is being updated to replace “Office of Mental Health Operations (10NC5)” with “Office of Mental Health and Suicide Prevention, 513-233-1748 (this is not a toll-free number)”.

The Authority for Maintenance in the System is being amended to include 38 U.S.C. 1720F, Public Law 110-110 (Joshua Omvig Veterans Suicide Prevention Act); and Public Law 114-247 (No Veterans Crisis Line Call Should Go Unanswered Act).

The Purpose has been amended to include “The records and information may be used for documenting contact interactions with the VCL and follow-up care; including, but not limited to: services with the Peer Support Outreach Center; management for Customers with Complex Needs; collaboration with stakeholders with whom VCL has a documented partnership, arrangement or agreement; referrals to the VA Medical Center Suicide Prevention Coordinators; and follow-up verbal or written correspondence. The records may also be used for statistical evaluation, reporting, program improvement and quality assurance.”

The Categories of Individuals Covered by the System is being amended to remove friends and family of Veterans. This section will include “Service members and anyone concerned about a Veteran or Service member who accessed the VCL. The VCL also receives contact from the general public within the Continental United States (CONUS) and Outside the Continental United States (OCONUS) and as such would have records from these contacts. In addition, records include the names and contact information of the Crisis Line response team and the name and contact information of the VHA Medical Center Suicide Prevention Coordinator.”

The Categories of Records in the System is removing “The records may include information related to: 1. The Veterans Crisis Line call logs via the VCL Application include the following information: a. Identifies, by full name, the Veterans

Crisis Line responder; b. Identifies, by full name, the Suicide Prevention Coordinator; c. Documents information regarding calls to the Veterans Crisis Line which may include: (1) Calls from an anonymous person with incomplete identification information; (2) Calls from a Veteran, including Veterans who are not registered in VA health care system (non-VA); (3) Calls from family and friends of the affected Veteran (In this case, the system shall indicate that the call was not made from the affected Veteran). d. Identifies the VA Medical Center closest to the caller's physical location; e. Records Crisis Line referrals in the Veteran's electronic medical record when the referral is made to a VA Medical Center for follow-up care; f. Provides a means for Suicide Prevention Coordinators to document their follow-up measures; g. Provides access to call log data for reporting purposes: Provides information related to the number of calls, callers demographic information, the types of calls, and follow-up care. 2. The suicide attempts and completions data is collected in the Austin Information Technology Center (AITC) standard query language (SQL) database. The information includes attempt or completion, military conflict, VA enrolled, gender, age, mental health diagnosis, medical diagnosis, previous attempts, month of event, method used, outcome, intent, seen at a VA within 7 days of attempt, seen at VA within 30 days of attempt, where seen, had suicide been addressed, and last recorded pain score."

For clarification, this section will now state "These records include VCL records regarding interactions with VCL staff, including call recordings and care coordination. These records may include names, home and mailing addresses, phone numbers, email addresses, Internet Protocol addresses, dates of birth and Social Security Numbers, limited health information obtained from the customer and/or the VA medical record, and other personal information related to:

1. Full name of the VCL staff, local emergency personnel and VA Medical Center employees involved in VCL interactions and care coordination.
2. Electronic record documentation and audio recordings regarding contact to the VCL which may include:
    (a) Contact with an anonymous person with incomplete identification information;
    (b) Contact from a Veteran, including Veterans who are not registered in the VA Health Care System;
    (c) Contact with the general public within the CONUS and OCONUS;
    (d) Contact with family and friends of the affected Veteran;
    (e) Contact with Service members and/or their family and friends;
    (f) Electronic correspondence from sources such as White House, Congressional offices, contractors, Office of Inspector General, and other parties.
3. VA Medical Center closest to the customer's physical location;
4. VCL request to a VA Medical Center for follow-up care;
5. Documentation from VA Medical Center's Suicide Prevention Coordinators regarding their follow-up measures.

The Record Source Categories has been updated to replace "Information in this system of records is provided by VHA employees," with "Information in this system of records is provided by persons who contact VCL through phone, chat, text, email and digital media with resultant outreach contacts, VHA electronic health records (i.e., Joint

Legacy Viewer, Millennium, Compensation and Pension Record Interchange, Medora), VHA employees, public records, persons employed at public safety answering points, and first responder personnel."

Routine Use number 3 is being updated to replace "Disclosure may be made to other Government agencies in support of data exchanges of electronic medical record information approved by the individual" with "Data Breach Response and Remediation, for VA: 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."

The following Routine Uses will be added:

12. Department of Defense (DoD), Defense Health Agency (DHA): To the DoD for the purpose of VHA health care operations as defined in the Health Insurance Portability and Accountability Act Privacy Rule, 45 CFR parts 160 and 164 and to the DHA, as a health care provider, for the purpose of DHA health care operations. VHA, as a health care provider, must be able to share health care information with other entities and health care providers for VA to perform certain health care operations, such as quality assessment and improvement activities and medical reviews.

13. To an organization with whom VA has a documented partnership, arrangement or agreement for the purpose of identifying and correlating patients.

14. To a Federal agency, Federal entity, or an organization with whom VA has a documented partnership, arrangement or agreement in response to its request or at the initiation of VA, in connection with research initiatives approved by VHA that may include, but is not limited to, patient outcomes or other health information required for program accountability.

15. To persons who may prevent a serious and imminent threat to the safety of an individual or the public as long as the disclosure is to a person(s) that is in a position reasonably able to prevent or lessen the threat, including the individual threatened. This Routine Use provides authority for the VCL to collaborate with law enforcement to initiate an emergency dispatch when a Veteran has shown an indication of harm towards self or others.

16. Non-VA Health Care Providers, for Treatment: To a non-VA health care provider, such as DoD and the Department of Health and Human Services, for the purpose of treating any VA patient, including Veterans. This Routine Use gives authority for the VCL to provide Veteran information to a non-VA health care provider when the VCL has encouraged the Veteran to seek medical care, and a VA Medical Center is not the best option.

17. Law Enforcement, for Locating Fugitive: In compliance with 38 U.S.C. 5313B(d), to any Federal, state, local, territorial, tribal or foreign law enforcement agency in order to identify, locate or report a known fugitive felon. If the disclosure is in response to a request from a law enforcement entity, the request must meet the requirements for a qualifying law enforcement request under the Privacy Act, 5 U.S.C. 552a(b)(7).

18. The Joint Commission (TJC), for Accreditation: To survey teams of TJC, College of American Pathologists, American Association of Blood Banks, and similar national accreditation agencies or boards with which VA has a contract or agreement to conduct

such reviews, as relevant and necessary for the purpose of program review or the seeking of accreditation or certification.

19. Phone Operators, for the Hearing-Impaired: To telephone company operators acting in a capacity to facilitate phone calls to or for hearing-impaired individuals, such as Veterans, Veterans' family members, non-VA providers, using telephone devices for the hearing-impaired, including Telecommunications Devices for the Deaf or Text Telephones.

20. Health/Welfare Agencies, etc., for Veteran's Basic/Emergency Needs: To health and welfare agencies, housing resources and utility companies in situations where VA needs to act quickly in order to provide basic or emergency needs for the Veteran and Veteran's family where the family resides with the Veteran or serves as a caregiver.

21. Former Employee or Contractor, Representative, for Litigation Involving Individual: To a former VA employee or contractor, as well as the authorized representative of a current or former employee or contractor of VA, in pending or reasonably anticipated litigation against the individual regarding health care provided during the period of his or her employment or contract with VA.

The Policies and Practices for Storage of Records is being amended to remove verbiage indicating that records are maintained on an SQL server at AITC in Austin, Texas. This section will now state "Electronic records are maintained and transmitted to Storage Area Networks at the AITC in Austin, Texas; Storage Area Network at the Health Resource Center in Topeka, Kansas; and the Microsoft Government Community Cloud."

Policies and Practices for Retrievability of Records is being updated to include telephone numbers.

Policies and Practices for Retention and Disposal of Records is being updated to remove “these records are maintained as a permanent record, pending approval of a new records schedule”. This section will now state, “Records in this system are retained and disposed of in accordance with the schedule approved by the Archivist of the United States, VHA Records Control Schedule 10-1, Item Number 1930.1.”

The Administrative, Technical and Physical Safeguards is being amended to remove the following verbiage from number 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. They are required to take annual VA mandatory data privacy and security training. 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.”

Number 2 will also be removed, “Access to computer rooms at the VA AITC is limited in accordance with VA OIT national security policies. Peripheral devices are placed in secure areas (areas that are locked or have limited access) or are otherwise protected. Information stored on the Veterans Crisis Line Database-VA may be accessed by authorized VA employees. Access to file information is controlled at two levels; the systems recognize authorized employees by series of individually unique passwords/codes as a part of each data message, and the employees are limited to only that information in the file which is needed in the performance of their official duties. Information that is downloaded from the Veterans Crisis Line Database-VA 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."

Number 2 will now state, "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."

The following Safeguards will be added:

3. 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.

4. 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.

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

6. VA Enterprise Cloud data storage conforms to security protocols as stipulated in VA Directives 6500 and 6517. Access control standards are stipulated in specific agreements with cloud vendors to restrict and monitor access.

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. Kurt D. DelBene, Assistant Secretary for Information and Technology and Chief Information Officer, approved this document on May 2, 2023 for publication.

Dated: June 6, 2023

Amy L. Rose,

Program Analyst,

VA Privacy Service,

Office of Information Security,

Office of Information and Technology,

Department of Veterans Affairs.

SYSTEM NAME AND NUMBER: “Veterans Crisis Line Records-VA” (158VA10)

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: Records are maintained at the Department of Veterans Affairs (VA) Austin Information Technology Center (AITC) in Austin, Texas and Health Resource Center (HRC) in Topeka, Kansas. In addition, information from these records or copies of records may be maintained at the Department of Veterans Affairs, 810 Vermont Avenue, NW, Washington, DC. Additional and supplemental data is stored within the Microsoft Government Community Cloud.

SYSTEM MANAGER(S): Official responsible for policies, procedures and system of records; Acting Executive Director, Office of Mental Health and Suicide Prevention, 810 Vermont Avenue, NW, Washington, DC 20420; (513)-233-1748 (this is not a toll-free number).

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 38 U.S.C. 501 and 1720F, Public Law 110-110 (Joshua Omvig Veterans Suicide Prevention Act); and Public Law 114-247 (No Veterans Crisis Line Call Should Go Unanswered Act).

PURPOSE(S) OF THE SYSTEM: The records and information may be used for documenting contact interactions with the Veterans Crisis Line (VCL) and follow-up care including, but not limited to: services with the Peer Support Outreach Center; management for Customers with Complex Needs; collaboration with stakeholders with whom VCL has a documented partnership, arrangement or agreement; referrals to the VA Medical Center Suicide Prevention Coordinators; and follow-up verbal or written correspondence. In addition, the information will be used for statistical reports for the purpose of evaluating the need for the development of further suicide prevention efforts to include education and research. The records may also be used for statistical

evaluation, reporting, program improvement and quality assurance. Additionally, the statistical reports will be used to provide information related to suicide to the VA officials, congressional members and the public.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: The records include information concerning Veterans, Service members and anyone concerned about a Veteran or Service member who contacted the VCL. The VCL also receives contact from the general public within the Continental United States (CONUS) and Outside the Continental United States (OCONUS) and as such would have records from these contacts. In addition, records include the names and contact information of the Crisis Line response team and the name and contact information of the Veterans Health Administration (VHA) Medical Center Suicide Prevention Coordinator.

CATEGORIES OF RECORDS IN THE SYSTEM: These records include VCL records regarding interactions with VCL staff, including call recordings and care coordination. These records may include names, home and mailing addresses, phone numbers, email addresses, Internet Protocol addresses, dates of birth and Social Security Numbers, limited health information obtained from the customer and/or the VA medical record, and other personal information related to:

1. Full name of the VCL staff, local emergency personnel and VA Medical Center employees involved in VCL interactions and care coordination.

2. Electronic record documentation and audio recordings regarding contact to the VCL which may include:
    (g) Contact with an anonymous person with incomplete identification information;
    (h) Contact from a Veteran, including Veterans who are not registered in the VA Health Care System;

(i) Contact with the general public within the CONUS and OCONUS;

(j) Contact with family and friends of the affected Veteran;

(k) Contact with Service members and/or their family and friends;

(l) Electronic correspondence from sources such as White House, Congressional offices, contractors, Office of Inspector General and other parties.

3. VA Medical Center closest to the customer's physical location;

4. VCL request to a VA Medical Center for follow-up care;

5. Documentation from VA Medical Center's Suicide Prevention Coordinators regarding their follow-up measures.

RECORD SOURCE CATEGORIES: Information in this system of records may be provided by persons who contact VCL through phone, chat, text, email and digital media with resultant outreach contacts, VHA electronic health records (e.g., Joint Legacy Viewer, Millennium, Compensation and Pension Record Interchange, Medora), VHA employees, public records, persons employed at public safety answering points, and first responder personnel.

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 of VHA or any of its business associates, 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 both 38 U.S.C. 7332 and 45 CFR parts 160, 161, and 164.

1. Congress: 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. National Archives and Records Administration (NARA): 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.

3. Data Breach Response and Remediation, for VA: 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.

4. Law Enforcement: 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, provided that the disclosure is limited to 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. 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. Department of Justice (DoJ), Litigation and Administrative Proceeding: To the DoJ, or in a proceeding before a court, adjudicative body or other administrative body before which VA is authorized to appear, when:

1. VA or any component thereof;
2. Any VA employee in their official capacity;
3. Any VA employee in their individual capacity where DoJ has agreed to represent the employee; or
4. 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 the use of such records is relevant and necessary to the proceedings.

6. Contractors: 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. Federal Agencies, Fraud and Abuse: To other Federal agencies to assist such agencies in preventing and detecting possible fraud or abuse by individuals in their operations and programs.

8. Equal Employment Opportunity Commission (EEOC): To the 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. Federal Labor Relations Authority (FLRA): To the 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. Merit Systems Protection Board (MSPB): To the 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. Data Breach Response and Remediation, for Another Federal Agency: 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.

12. Department of Defense (DoD), Defense Health Agency (DHA): To the DoD for the purpose of VHA health care operations as defined in the Health Insurance Portability and Accountability Act Privacy Rule, 45 CFR parts 160 and 164 and to the DHA, as a health care provider, for the purpose of DHA heath care operations.

13. To an organization with whom VA has a documented partnership, arrangement or agreement for the purpose of identifying and correlating patients.

14. To a Federal agency, Federal entity or an organization with whom VA has a documented partnership, arrangement or agreement in response to its request or at the initiation of VA, in connection with research initiatives approved by VHA that may

include, but is not limited to, patient outcomes or other health information required for program accountability.

15. Law Enforcement, for Wellness Check: To law enforcement to initiate a wellness check or an emergency dispatch when a Veteran has shown an indication of harm towards self or others during a VCL contact.

16. Non-VA Health Care Providers, for Treatment: To a non-VA health care provider, such as the DoD and the Department of Health and Human Services, for the purpose of treating any VA patient, including Veterans.

17. Law Enforcement, for Locating Fugitive: In compliance with 38 U.S.C. 5313B(d), to any Federal, state, local, territorial, tribal or foreign law enforcement agency in order to identify, locate or report a known fugitive felon. If the disclosure is in response to a request from a law enforcement entity, the request must meet the requirements for a qualifying law enforcement request under the Privacy Act, 5 U.S.C. 552a(b)(7).

18. The Joint Commission (TJC), for Accreditation: To survey teams of TJC, College of American Pathologists, American Association of Blood Banks and similar national accreditation agencies or boards with which VA has a contract or agreement to conduct such reviews, as relevant and necessary for the purpose of program review or the seeking of accreditation or certification.

19. Phone Operators, for the Hearing-Impaired: To telephone company operators acting in a capacity to facilitate phone calls to or for hearing-impaired individuals, such as Veterans, Veterans' family members, non-VA providers, using telephone devices for the hearing-impaired, including Telecommunications Devices for the Deaf or Text Telephones.

20. Health/Welfare Agencies, etc., for Veteran's Basic/Emergency Needs: To health and welfare agencies, housing resources and utility companies in situations where VA needs to act quickly in order to provide basic or emergency needs for the Veteran and the Veteran's family where the family resides with the Veteran or serves as a caregiver.

21. Former Employee or Contractor, Representative, for Litigation Involving Individual: To a former VA employee or contractor, as well as the authorized representative of a current or former employee or contractor of VA, in pending or reasonably anticipated litigation against the individual regarding health care provided during the period of his or her employment or contract with VA.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Electronic records are maintained and transmitted to Storage Area Networks at the AITC in Austin, Texas; Storage Area Network at the Health Resource Center in Topeka, Kansas; and the Microsoft Government Community Cloud.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records are retrieved by name, telephone number, 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 in this system are retained and disposed of in accordance with the schedule approved by the Archivist of the United States, VHA Records Control Schedule 10-1, Item Number 1930.1.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

1. VA will maintain the data in compliance with applicable VA security policy directives that specify the standards that will be applied to protect sensitive personal information. VA's security measures comply with applicable Federal Information Processing Standards issued by the National Institute of Standards and Technology.

2. 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.

3. 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.

4. 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.

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

6. VA Enterprise Cloud data storage conforms to security protocols as stipulated in VA Directives 6500 and 6517. Access control standards are stipulated in specific agreements with cloud vendors to restrict and monitor access.

RECORD ACCESS PROCEDURE: Individuals seeking information on the existence and content of records in this system pertaining to them should contact vhavclprivacy@va.gov. A request for access to records must contain the requester’s full

name, address, telephone number, be signed by the requester, and describe the records sought in sufficient detail to enable VA personnel to locate them with a reasonable amount of effort.

CONTESTING RECORD PROCEDURES: Individuals seeking to contest or amend records in this system pertaining to them should contact VHAVCLRequestsforInformation@va.gov. A request to contest or amend records must state clearly and concisely what record is being contested, the reasons for contesting it, and the proposed amendment to the record.

NOTIFICATION PROCEDURE: Generalized notice is provided by the publication of this notice. For specific notice, see Record Access Procedure, above.

EXEMPTIONS PROMULGATED FOR THE SYSTEM: None.

HISTORY: 80 FR 23073 (April 24, 2015).

[FR Doc. 2023-12401 Filed: 6/9/2023 8:45 am; Publication Date: 6/12/2023]