VHA ACCESS TO AND USE OF CENTERS FOR MEDICARE AND MEDICAID SERVICES AND UNITED STATES RENAL DATA SYSTEM DATA

1. REASON FOR ISSUE:

a. This Veterans Health Administration (VHA) directive states authority and policy for providing authorized users access to data from the United States Department of Health and Human Services (HHS) Centers for Medicare and Medicaid Services (CMS) and the National Institute of Diabetes and Digestive and Kidney Diseases (NIDDK) United States Renal Data System (USRDS) as outlined under 5 U.S.C. § 552a and the Health Insurance Portability and Accountability Act (HIPAA) regulations.

b. This VHA directive also states standards for management, distribution, storage, processing and disposition of data obtained from CMS and USRDS for health care operations and research.

2. SUMMARY OF MAJOR CHANGES: This directive:

a. Incorporates material previously found in VHA Handbook 1153.01(1), Use of Centers for Medicare and Medicaid (CMS) and United States Renal Data System (USRDS) Data in the Veterans Health Administration (VHA), dated April 15, 2016.

b. Updates the policies for disclosing, storing, processing and disposing of data from CMS and the USRDS.

c. Outlines acceptable uses of CMS and USRDS data by VHA employees and contractors and establishes policy and oversight responsibility for these uses.

3. RELATED ISSUES: VA Directive 0710, Personnel Suitability and Security Program, June 4, 2010; VA Directive 6500, VA Cybersecurity Program, dated February 24, 2021; VA Directive 6502, VA Enterprise Privacy Program, dated May 5, 2008; VA Handbook 0710, Personnel Suitability and Security Program dated May 2, 2016; VA Handbook 6500, Risk Management Framework for VA Information Systems VA Information Security Program dated February 24, 2021; VHA Directive 0710, Personnel Suitability and Security Program, dated October 11, 2018; VHA Directive 1200.01(1), Research and Development Committee, dated January 24, 2019; VHA Directive 1200.05(2), Requirements for the Protection of Human Subjects in Research, dated January 7, 2019; VHA Directive 1605.01, Privacy and Release of Information, dated August 31, 2016; VHA Directive 1907.01, VHA Health Information Management and Health Records, dated April 5, 2021; VHA Directive 6300(1) Records Management, dated October 22, 2018; VHA Directive 6300.01(3), Records Management Continuous Readiness Review and Remediation, dated August 17, 2017; VHA Handbook 1605.04, Notice of Privacy Practices, dated October 7, 2015.

4. RESPONSIBLE OFFICE: The VHA Chief Strategy Office (CSO), VHA Medicare and Medicaid Analysis Center (MAC) (108) and the Office of Research and Development (ORD) (14RD) are responsible for the content of this VHA directive. Questions may be addressed to the Director, VHA Medicare and Medicaid Analysis Center (MAC) at MACstaff@va.gov.

5. RESCISSIONS: VHA Directive 1153(1), Access to Centers for Medicare and Medicaid Services (CMS) and United States Renal Data System (USRDS) Data for VHA Users within the VA Information Technology (IT) Systems, dated April 15, 2016; and VHA Handbook 1153.01, Use of Centers for Medicare and Medicaid Services (CMS) and United States Renal Data System (USRDS) Data in the Veterans Health Administration, dated April 15, 2016, are rescinded.

6. RECERTIFICATION: This VHA directive is scheduled for recertification on or before the last working day of November 2026. This VHA directive will continue to serve as national VHA policy until it is recertified or rescinded.

BY THE DIRECTION OF THE OFFICE OF THE UNDER SECRETARY FOR HEALTH:

/s/ Mark Upton, MD
Deputy to the Assistant Under Secretary
for Health for Community Care,
Performing the Delegable Duties of the
Deputy Under Secretary for Health

NOTE: *All references herein to VA and VHA documents incorporate by reference subsequent VA and VHA documents on the same or similar subject matter.*

DISTRIBUTION: Emailed to the VHA Publications Distribution List on November 30, 2021.

CONTENTS

VHA ACCESS TO AND USE OF CENTERS FOR MEDICARE AND MEDICAID SERVICES AND UNITED STATES RENAL DATA SYSTEM DATA

VHA ACCESS TO AND USE OF CENTERS FOR MEDICARE AND MEDICAID SERVICES AND UNITED STATES RENAL DATA SYSTEM DATA

1. PURPOSE

This Veterans Health Administration (VHA) directive states the policy for providing authorized users with access to data from the United States Department of Health and Human Services (HHS) Centers for Medicare and Medicaid Services (CMS) and the National Institute of Diabetes and Digestive and Kidney Diseases (NIDDK) United States Renal Data System (USRDS) as outlined under 5 U.S.C. § 552a and the Health Insurance Portability and Accountability Act (HIPAA). This VHA directive also states standards for using, disclosing, storing, processing and disposing of data from CMS and USRDS. It addresses both research and operational uses of the data.
AUTHORITY: 5 U.S.C. § 552a; 38 U.S.C. § 7301(b).

2. BACKGROUND

a. VHA purchases CMS and USRDS data to improve understanding of the quality and cost drivers in delivering health care to Veterans, to better anticipate Veteran health care needs, to accurately forecast financial requirements for providing appropriate health care, and to provide a resource for research. This use is authorized through Information Exchange Agreement (IEA) agreements with CMS and NIDDK. The information received from CMS pursuant to this agreement is used to conduct statistical studies and analyses, which support VHA research as well as administrative plans and policies. The scope of this agreement does not include the business processes of VHA's health care program, such as eligibility and enrollment determinations, revenue operations (including insurance coverage determination and billing) or purchased care decisions (fee-basis care).

b. With the enactment of the Privacy Act, Congress required agencies to employ reasonable technological safeguards to protect individually identifiable health information that is stored electronically. CMS and USRDS data are distributed to approved users within VHA who have legal authority to access the data and have demonstrated their ability to safeguard the data through a data request processes for operations and research uses. VHA’s goal is to optimize the benefits realized from its investment in CMS and USRDS data while protecting the privacy and security of Veterans’ personal and health care data. CMS and USRDS data users within VHA must follow all applicable laws and regulations that pertain to privacy or security of highly sensitive information, including any additional requirements enforced specifically for use of CMS and USRDS data.

c. HIPAA and the implementing regulations at 45 C.F.R. parts 46, 160 and 164, include general administrative requirements and security and privacy guidelines that pertain to Individually Identifiable Health Information (IIHI). This includes health information that concerns the physical or mental health or condition of an individual, the provision of health care to an individual or the payment for the provision of health care to an individual and identifies the individual or can be used to identify an individual. The

HIPAA Privacy Rule regulates the use and disclosure of Protected Health Information (PHI), that is, IIHI held by covered entities.

3. DEFINITIONS

NOTE: *All definitions are specific to CMS and USRDS data use and are not necessarily terms relating to general data use.*

a. **Access.** Access is the ability to view and use information in any VA-controlled information technology (IT) system resource.

b. **CMS Data.** CMS data is individually identifiable information disclosed by CMS. There are two types of CMS data defined in the VHA-CMS IEA for use in VHA:

(1) **Raw CMS Data.** Raw CMS data is CMS data maintained in a CMS System of Records (SOR). Pursuant to CMS internal policies, raw CMS data will remain in a CMS SOR and are subject to CMS policies even after proper legal disclosure to VHA.

(2) **Merged CMS Data.** Merged CMS data is CMS data that has been combined with VHA data and are maintained in VHA SOR, "Consolidated Data Information System-VA" (97VA10).

c. **Data Re-use.** Data re-use is the use of CMS or USRDS data for a use other than the originally approved use. The data to be re-used may be obtained directly from a source other than the Information Custodian (IC), including from another user, such as a VA research or operations data repository.

d. **Operational Use.** Operational use is the use of the CMS or USRDS data for VHA program administration, operational or other purposes, not including research use. Requests for operational use of the data are approved by VHA Medicare and Medicaid Analysis Center (MAC).

e. **Operations and Research Partnership.** An Operations and Research Partnership is a single project that includes both operational and VA approved research objectives and may involve both operational data use and research data use.

f. **Research Use.** Research use is the use of CMS or USRDS data within VA-approved research protocols. The research protocols must meet the definition of research and be approved by a VA Research & Development Committee (R&DC) and if applicable, its subcommittees. Data requests for research use are approved by VA Information Resource Center (VIReC).

g. **United States Renal Data System Data.** The United States Renal Data System (USRDS) is a data system that collects, analyzes and distributes information about end-stage renal disease (ESRD) in the United States. USRDS data is individually identifiable data disclosed by the NIDDK. There are two types of USRDS data defined in the VHA-NIDDK IEA for use in VHA:

(1) **Raw USRDS Data.** Raw USRDS data is USRDS data maintained in a NIDDK SOR. Pursuant to NIDDK internal policies, raw USRDS data remain in a NIDDK SOR and are subject to NIDDK policies even after proper legal disclosure to VHA.

(2) **Merged USRDS Data.** Merged USRDS data is USRDS data that has been combined with VHA data and are maintained in VHA SOR titled "Consolidated Data Information System-VA" (97VA10).

h. **VA-Controlled Information Technology System.** A VA-controlled IT system is any IT system, platform, or data venue internal or external to VA that is required to comply with VA organizational security and privacy requirements and monitored by VA for security and privacy control compliance on an ongoing basis. Connections to VA-controlled external systems require a VA-managed interface.

4. POLICY

It is VHA policy that access to CMS and USRDS data within VHA is granted to authorized users by the MAC and the VIReC. It is VHA policy that MAC and VIReC are the sole sources of CMS and USRDS data in VHA.

5. RESPONSIBILITIES

a. **Under Secretary for Health.** The Under Secretary for Health is responsible for ensuring overall VHA compliance with this directive.

b. **Deputy Under Secretary for Health.** The Deputy Under Secretary for Health is responsible for supporting the program office with implementation and oversight of this directive.

c. **Assistant Under Secretary for Health for Operations.** The Assistant Under Secretary for Health for Operations is responsible for:

(1) Communicating the contents of this directive to each of the Veterans Integrated Services Networks (VISNs).

(2) Assisting VISN Directors to resolve implementation and compliance challenges.

(3) Providing oversight of VISNs to ensure compliance with this directive and its effectiveness.

d. **Assistant Under Secretary for Health for Discovery, Education and Affiliate Networks.** The Assistant Under Secretary for Health for Operations for Discovery, Education and Affiliate Networks (DEAN) is responsible for promoting collaboration and coordination with researchers and operational uses, to drive ongoing improvement and innovation in education, training and advancements in scientific research.

e. **Chief Research and Development Officer.** The CRADO is responsible for:

(1) Establishing and maintaining VHA-wide requirements for access to CMS and USRDS data for research uses, in accordance with 5 U.S.C. § 552a, 45 C.F.R. parts 46, 160 and 164 and 38 C.F.R. part 16.

(2) Providing sufficient resources to VIReC to maintain an oversight function for managing access to CMS and USRDS data for research uses in VHA.

(3) Charging the Office of Research and Development (ORD) Research and Advisory Board (RAB) Chair to oversee VIReC's requirements for research use of CMS and USRDS data.

f. **VHA Chief Strategy Officer.** The VHA Chief Strategy Officer (CSO) is responsible for:

(1) Overseeing the VHA Medicare and Medicaid Analysis Center (MAC).

(2) Establishing and maintaining VHA-wide requirements for access to CMS and USRDS data for operational uses, in accordance with 5 U.S.C. § 552a and 45 C.F.R. parts 46, 160 and 164.

(3) Providing sufficient resources (e.g., funding) to maintain an oversight function for managing access to CMS and USRDS data for operational uses in VHA.

(4) Providing guidance on special concerns or issues regarding requests for use of CMS and USRDS data for VHA operations.

g. **CMS Data Advisory Committee Co-Chairs.** The CMS Data Advisory Committee (DAC) is co-chaired by the MAC and VIReC Directors and is comprised of stakeholders from a cross-section of VA and VHA organizations who are responsible for data governance within VA. Upon request of MAC and VIReC, this committee is responsible for making recommendations on issues related to managing access to, disclosure or receipt of CMS and USRDS data.

h. **VHA Medicare and Medicaid Analysis Center Director.** MAC is a field office within the VHA Chief Strategy Office. The MAC Director, who is the Information Custodian (IC) for CMS and USRDS data for operational use, is responsible for:

(1) Updating the VHA SOR titled "Consolidated Data Information System-VA" (97VA10).

(2) Overseeing development of policies for use of CMS and USRDS data within VHA.

(3) Developing and implementing requirements and procedures for the distribution and oversight of CMS and USRDS data for VHA operational uses.

(4) Approving requests for operational use of CMS and USRDS data.

(5) Balancing the strategic need for streamlined access to CMS data with the necessity to protect data security and privacy.

(6) Collaborating with Record Managers to ensure proper disposition of both raw and merged data.

(7) Determining whether authorized data users are approved to access CMS and USRDS data by:

(a) Verifying that authorized data users have legal authority to access CMS and USRDS data under 5 U.S.C. § 552a, 45 C.F.R. parts 46, 160 and 164.

(b) Attesting that all authorized data users have satisfied the mandatory VHA Privacy and HIPAA training requirements.

(8) Developing business agreements and serving as a VHA procuring agent for procurement of CMS data.

(9) Creating an annual finder file consisting of Veteran identifiers for submission to CMS and USRDS for data matching.

i. **Office of Research and Development, Research Advisory Board Chair.** The ORD RAB is comprised of stakeholders from a cross-section of VA and VHA organizations. It is chaired by the Director of Health Services Research and Development (HSR&D) Service. The ORD RAB Chair is responsible for:

(1) Providing oversight and guidance to VIReC related to managing, distributing and dispositioning of CMS and USRDS research data, in accordance with research requirements and the protection of human subjects.

(2) Providing guidance to users on special concerns or issues regarding requests for research use of CMS and USRDS data.

(3) Collaborating with CRADO for oversight of CMS and USRDS data policies. ***NOTE:*** *For more information, see paragraph 5.e.(3).*

j. **VA Information Resource Center Director.** VIReC is a national research resource center under ORD, HSR&D. The VIReC Director, who is the Information Custodian (IC) for CMS and USRDS data for research use, is responsible for:

(1) Developing and implementing requirements and procedures for the distribution and oversight of CMS and USRDS data for VHA research uses.

(2) Overseeing development of policies for use of CMS data within VHA.

(3) Approving requests for research use of CMS and USRDS data.

(4) Balancing the strategic need for streamlined access to CMS data with the necessity to protect data security and privacy.

(5) Collaborating with Record Managers to ensure proper disposition of both raw and merged data.

(6) Determining whether authorized data users are approved to access CMS and USRDS data by:

(a) Verifying that authorized data users have legal authority to access CMS and USRDS data under 5 U.S.C. § 552a, 45 C.F.R. parts 46, 160 and 164.

(b) Attesting that all users have satisfied the mandatory VHA Privacy and HIPAA training requirements.

(7) Verifying compliance with Federal and VHA policies governing human subjects' research and VA data use.

k. **Data Requestor.** A Data Requestor is a Project Manager (for operations use) or Principal Investigator (for research use) who is responsible for:

(1) Submitting required documentation as required by the ICs to obtain access to CMS and USRDS data on behalf of a project to the MAC or VIReC. ***NOTE:*** *For more information, see paragraph 7.c.(1).*

(2) Overseeing all aspects of the project, including the authorized data users' access to CMS and USRDS data. ***NOTE:*** *For more information, see paragraph 5.l.*

(3) Reporting to the IC immediately of any incident by any authorized data user involving data confiscation or risk to data security or privacy.

(4) Notifying the IC of termination of data use and for managing data disposition.

(5) Complying with all applicable VA and VHA policy.

(6) Verifying compliance of authorized data users with the requirements of the Data Use Agreement (DUA).

l. **Authorized Data Users.** Authorized data users are individuals who have access to CMS or USRDS data on a given project. An authorized data user is an individual who is permitted by 5 U.S.C. § 552a, 45 C.F.R. parts 160 and 164, and VA and VHA policy to have access to VA IT systems and data for official purposes after completing the required privacy and security training, signing the VA National Rules of Behavior, and obtaining approval from VHA Medicare and Medicaid Analysis Center (MAC) or the VA Information Resource Center (VIReC). They include but are not limited to VHA employees, VHA contractors and their subcontractors. ***NOTE:*** *An authorized data user can also be a Data Requestor.* Authorized data users are responsible for:

(1) Complying with all applicable VA and VHA policy.

(2) Following all requirements of the DUA as directed by the data requestor.

(3) Reporting to the IC and Data Requestor immediately of any incident by any authorized user involving data confiscation or risk to data security or privacy.

6. MANAGEMENT OF CMS AND USRDS DATA IN VHA

a. **Obtaining CMS and USRDS Data in VHA.**

(1) The VHA CSO provides funding, and MAC serves as the VHA procuring agent, for annual and intermittent orders of CMS and USRDS data.

(2) MAC and VIReC collaborate to create an annual "finder" file consisting of Veteran identifiers which are sent to CMS and USRDS for the purpose of matching and extracting associated CMS and USRDS data.

(3) In order to limit VHA expenses and to avoid the dissemination of inconsistent conclusions across VHA by analysis of different versions of the same datasets, end-of-year adjudicated CMS and USRDS data are obtained for VHA use. Additional datasets may be obtained under special circumstances at the discretion of MAC and VIReC.

(4) The MAC Director or the VIReC Director may request data directly from CMS or NIDDK on behalf of Data Requestors in special circumstances, including requests for data not covered by the IEA or for data to be used for only one VHA project.

(5) No other VHA office, program or employee is permitted to request data directly from CMS or NIDDK without express written permission from MAC Director (for operational use) or VIReC Director (for research use).

b. **Receiving, Managing and Validating CMS and USRDS Data.** The ICs:

(1) Receive data directly from CMS and USRDS and add it to the data warehouse.

(2) Maintain shipment and tracking information on all CMS and USRDS data received and warehoused.

(3) Perform quality checks on CMS and USRDS data when feasible.

c. **Transferring Data between MAC and VIReC.** The ICs transfer CMS and USRDS data to each other for distribution or validation of data quality. The following types of data may be transferred between MAC and VIReC:

(1) Finder files and data used to develop finder files, except when access is specifically limited to MAC or VIReC by the data owner.

(2) CMS data that are included in both the MAC and VIReC DUAs with CMS.

(3) USRDS data.

d. **Data Disposition.** The ICs ensure proper disposition of both raw and merged data.

(1) ICs must destroy raw CMS data and raw USRDS data at the end of data use in accordance with requirements set forth in the CMS or NIDDK IEAs and CMS DUA.

(2) ICs must ensure that merged CMS data and merged USRDS data is transferred to the appropriate local records management personnel for disposition in accordance with VHA Directive 6300.01(3), Records Management Continuous Readiness Review and Remediation, dated August 17, 2017, and VHA Record Control Schedule (RCS) 10-1.

7. DISTRIBUTION OF CMS AND USRDS DATA IN VHA

a. **Types of Data Information Custodians Distribute.**

(1) Raw CMS data and raw USRDS data, with written approval for each use from CMS or NIDDK.

(2) Merged CMS data and merged USRDS data.

b. **Management of Data Distribution.**

(1) The requested use of the CMS and USRDS data determines which IC is responsible for oversight of data distribution. If the data is requested for research use, the IC is VIReC. If the data is requested for operational use, the IC is MAC.

(2) The ICs create and revise procedures and standard processes for how prospective Data Requestors may request access to CMS and USRDS data.

c. **Request Process and Data Use Agreements.**

(1) MAC and VIReC require that Data Requestors submit documents in order to obtain access to CMS and USRDS data. ***NOTE:*** *To access MAC's intranet website, see https://vaww.va.gov/MEDICAREANALYSIS/index.asp. To access VIReC's intranet website, see https://vaww.virec.research.va.gov/Index-VACMS.htm. These are internal VA websites that are not available to the public.*

(2) Requests for CMS and USRDS data must include an affirmation from the Data Requestor that:

(a) The data requested comprise the minimum necessary data for the project.

(b) The data provided to the project will be stored and maintained securely.

(c) Merged data will be dispositioned in accordance with VHA Directive 6300.01(3) and RCS 10-1. Raw data will be dispositioned in accordance with the DUA with CMS.

(d) The project has approval to use PHI as documented by a VHA Privacy Officer.

(3) The IC reviews and approves the request to access CMS and USRDS data for research and operational uses. Once the request is approved, a DUA between the IC and the Data Requestor, must be executed prior to release of data. Data must be transferred to projects or contractors in accordance with VA and VHA data security policies as described in VA Handbook 6500, Risk Management Framework for VA Information Systems VA Information Security Program, dated February 24, 2021. ***NOTE:*** *Data sharing from an approved project to secondary project or contractor requires a separate DUA with MAC or VIReC as applicable.*

d. **Data Storage Requirements for Authorized Data Users.**

(1) CMS and USRDS data used by VA employees must be stored and used only in VA-controlled IT systems.

(2) VA contractors and subcontractors must store and analyze data on VA-controlled IT systems to comply with VA data security requirements in VA Handbook 6500, unless the IC grants written approval for release of the data to a non-VA-controlled IT system following a successful audit of the external server by VA and VHA Privacy and Security authorities.

e. **Data Re-use.**

(1) Re-use of merged CMS data or merged USRDS data is not permitted without prior written approval from the IC.

(2) Re-use of raw CMS data or raw USRDS data is not permitted without prior written approval from CMS or NIDDK, respectively, and the IC. The IC will contact CMS or NIDDK directly for this approval.

(3) Data transfer methods must be approved by the IC.

f. **Special Requirements for Operations and Research Data Use Partnerships.**

(1) Because use of CMS and USRDS data for operations and research partnered projects requires coordination between the ICs, both aspects of the operations and research partnered project must obtain approval from both ICs to use all CMS and USRDS data obtained for the project.

(2) Governance of CMS and USRDS data use for projects arising from operations and research partnerships is managed jointly by the ICs while the project is open for both operations and research use:

(a) When operations use is concluded and research data use continues, data governance is assumed solely by VIReC, and the operations data is dispositioned in accordance with RCS 10-1 and VHA Directive 6300.01(3).

(b) When research use is concluded and operations data use continues, governance for the operations use of the data is assumed solely by MAC and the

research data is dispositioned in accordance with RCS 10-1 and VHA Directive 6300.01(3).

(3) Regardless of the type of project (operations or research), access to data for operations use is permitted only while the operations project is open. Access to data for research use is permitted only while the research project is open.

(4) On a case-by-case basis, ICs collaborate on the development of appropriate data request processes, ongoing oversight and data disposition.

g. **Ongoing Oversight of Data Use.** The IC oversees continued use of the data by:

(1) Developing and managing a process for renewal of authorization for data use.

(2) Providing a list of locations where data are used or stored to the VHA Privacy Compliance Assurance (PCA) Office.

(3) All CMS and USRDS Data Requestors are subject to an audit of their privacy and security practices by VHA PCA and must make their operations available to PCA for inspection within 30 days of a request for an audit. ***NOTE:*** *For more information, see VHA Directive 6300.01(3).*

h. **Maintaining Records.** The IC maintains records for each data request, including:

(1) Documents submitted by the data requestor.

(2) Documentation of the IC's review process, data preparation and release, oversight of data use, retention and disposition of data.

i. **Suspension and Termination of Data Use for Cause.**

(1) The IC may suspend use of the data:

(a) If there is suspected or known non-compliance of any provision of the DUA, VA or VHA policy. The IC may seek advice from the ORD RAB or CMS DAC as applicable.

(b) When data has been confiscated by an oversight or law enforcement office/body. The Data Requestor must report the incident to the IC immediately.

(2) The Data Requestor's access to the data, including that of all affiliated authorized data users, must be removed during the suspension.

(3) The Data Requestor, approving officials and the oversight body will be notified of the suspension, the reason for the suspension, and steps required for remediating the precipitating condition(s).

(4) The IC may approve resumption of data use when all conditions precipitating the suspension have been remediated.

(5) Data use may be terminated by the IC, in consultation with the oversight body, in which conditions precipitating the suspension are not remediated.

(6) The Data Requestor and the approving officials are notified of the termination.

(7) The Data Requestor's access to the data, including that of all affiliated authorized data users, is removed permanently upon notification of termination.

j. **Ending a Project's Data Use.**

(1) Operations data use ends when the project no longer needs the data or at the expiration of the DUA, whichever comes first, or for research uses at the close of R&DC approval for the project.

(2) The Data Requestor is responsible for notifying the IC of termination of data use and for managing data disposition.

(3) Merged CMS Data and merged USRDS data will be dispositioned in accordance with RCS 10-1 and VHA Directive 6300.01(3).

(4) Raw data are dispositioned in accordance with the requirements of the CMS or NIDDK DUA.

k. **Re-opening a Project.** Once a project has closed, the Data Requestor must submit a new data access request and receive approval from the IC prior to accessing the data.

8. PROVIDING DATA TO NON-VHA OFFICES WITHIN VA

Data use by VA offices external to VHA is not covered in the VHA-CMS IEA or the VHA-USRDS IEA. To avoid duplication of VA costs in purchasing data, MAC may provide data to these VA organizations but must obtain prior written approval from CMS or NIDDK before releasing the data.

9. DATA PROVIDED DIRECTLY FROM CMS OR NIDDK

VA employees or contractors who previously received data directly from CMS or NIDDK for non-VHA purposes, may transfer and use the data within VHA only with prior approval from CMS or NIDDK and the IC. Data that is brought into VHA becomes VHA data once it is merged with VHA data.

10. DE-IDENTIFIED OR AGGREGATE CMS OR USRDS DATA

a. CMS data that have been de-identified remain under the oversight of the IC and will not be redistributed or used beyond the scope of the approved use without prior written approval from the IC.

b. Aggregate CMS or USRDS data refers to data that meet CMS's small cell size suppression policy (i.e., no cells 10 or smaller. Values of zero "0" are permitted.) and does not contain direct personal identifiers and does not require IC approval before disclosure or use.

11. DELEGATION OF ADDITIONAL INFORMATION CUSTODIANS

Projects may create new data sources that include CMS or USRDS data. These new data sources may not be redistributed or reused without prior written approval from the IC. With a written agreement, the IC may delegate partial or complete IC authority to the Data Requestors to redistribute or reuse the CMS or USRDS data contained in the new data source.

12. TRAINING

Authorized data users will have access to VA-controlled (IT) systems and data for official purposes after completing the VHA-required privacy and security training, signing the VA National Rules of Behavior and obtaining approval from MAC for operations use or VIReC for research use. All data users are required to complete Talent Management System (TMS) course numbers:

(1) 10176, "VA Privacy and Information Security Awareness and Rules of Behavior" or a VA approved substitute.

(2) 10203, "Privacy and HIPAA Training" or a VA approved substitute.

13. RECORDS MANAGEMENT

All records regardless of format (e.g., paper, electronic, electronic systems) created by this directive must be managed as required by the National Archives and Records Administration (NARA) approved records schedules found in VHA Records Control Schedule 10-1. Questions regarding any aspect of records management should be addressed to the appropriate Records Officer.

14. REFERENCES

a. 5 U.S.C. § 552a.

b. 38 U.S.C. § 7332.

c. 38 C.F.R. part 16.

d. 45 C.F.R. parts 160 and 164.

e. VA Directive 6500, VA Cybersecurity Program, dated February 24, 2021.

f. VA Directive 6502, VA Enterprise Privacy Program, dated May 5, 2008.

g. VA Handbook 0710, Personnel Suitability and Security Program, dated May 2, 2016.

h. VA Handbook 6500, Risk Management Framework for VA Information Systems VA Information Security Program, dated February 24, 2021.

i. VHA Directive 1200.01(1), Research and Development Committee, dated January 24, 2019.

j. VHA Directive 1200.05(2), Requirements for the Protection of Human Subjects in Research, dated January 7, 2019.

k. VHA Directive 1605.01, Privacy and Release of Information, dated August 31, 2016.

l. VHA Directive 6300.01(3), Records Management Continuous Readiness Review and Remediation, dated August 17, 2017.

m. VHA Handbook 1605.04, Notice of Privacy Practices, dated October 7, 2015.

n. VHA Records Control Schedule (RCS) 10-1, December 2020.

o. VHA System of Records ‘‘Consolidated Data Information System-VA” (97VA10).

p. “Information Exchange Agreement (IEA) between Department of Health and Human Services, Centers for Medicare & Medicaid Services and Department of Veterans Affairs, Veterans Health Administration,” VHA no. 08-200, CMS no. 2009-02, June 15, 2009.

q. “Information Exchange Agreement (IEA) between National Institute of Diabetes and Digestive and Kidney Diseases and Department of Veterans Affairs, Veterans Health Administration,” VHA no. 2011-01, July 29, 2011.