DATA USE AGREEMENTS

1. REASON FOR ISSUE: This Veterans Health Administration (VHA) directive provides revised information and instruction for the creation and use of Data Use Agreements (DUAs).

2. SUMMARY OF MAJOR CHANGES: This directive revises, consolidates, and updates procedures, functions, content, and circumstances for DUAs. This directive contains an amendment, dated March 1, 2021, to align with VHA Office of Research and Development policy for research data.

3. RELATED ISSUES:

a. VHA Directive 1072, Release of VA Data to State Cancer Registries, dated July 23, 2014.

b. VHA Directive 1080, Access to Individually Identifiable Information in Information Technology Systems, dated January 6, 2017.

c. VHA Directive 1153(1), Access to Centers for Medicare and Medicaid Services (CMS) and United States Renal Data System (USRDS) Data for Veterans Health Administration (VHA) Users Within the Department of Veterans Affairs (VA) Information Technology (IT) Systems, dated April 15, 2016.

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

e. VHA Directive 1605.03, Privacy Compliance Assurance Program and Privacy/Freedom of Information Act (FOIA) Continuous Readiness Review and Remediation, dated September 19, 2019.

f. VHA Handbook 1200.12, Use of Data and Data Repositories in VHA Research, dated March 9, 2009.

4. RESPONSIBLE OFFICE: The VHA Office of Health Informatics (105HIG) is responsible for the contents of this directive. Questions may be referred to the VHA Office of Health Informatics (OHI), Health Information Governance (HIG), National Data Systems (NDS) Office at 202-465-1581 or VHA10P2CDataAgreements@va.gov.

5. RESCISSION: VHA Handbook 1080.01, Data Use Agreements, dated November 20, 2013, is rescinded.

6. RECERTIFICATION: This VHA directive is scheduled for recertification on or before the last working day of January 2026. This VHA directive will continue to serve as

national VHA policy until it is recertified or rescinded.

BY DIRECTION OF THE OFFICE OF UNDER SECRETARY FOR HEALTH:

/s/ Steven L. Lieberman, MD, MBA, FACHE
Acting 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 January 26, 2021.

CONTENTS

DATA USE AGREEMENTS

DATA USE AGREEMENTS

1. PURPOSE

This Veterans Health Administration (VHA) directive establishes guidance for: determining when Federal laws, regulations, or Department of Veterans Affairs (VA) and VHA policies require a Data Use Agreement (DUA); formulating a DUA based upon established templates; and processing and monitoring DUAs. This directive also establishes policy which precludes the use of DUAs in certain circumstances. **AUTHORITY:** Title 38 United States Code (U.S.C.) § 7301(b) and 45 Code of Federal Regulations (C.F.R.) 164.514(e).

2. BACKGROUND

a. VHA is an administration of VA and its only agency component providing health care to Veterans and qualifying as a covered entity. As a covered entity as defined by the Health Insurance Portability and Accountability Act (HIPAA) and in accordance with VHA privacy policy, VHA is required to enter into a DUA under certain data-sharing circumstances, such as when a limited data set (LDS) is used. An LDS is not de-identified information under the HIPAA Privacy Rule and therefore HIPAA regulations still apply. DUAs will also be used under other conditions described in this directive. ***NOTE:*** *See paragraph 12, References, for a list of all VHA privacy policies.*

b. Previously, in cases where the use of a DUA was not mandated by Federal law or regulation, the decision to use a DUA was made by the business data steward. These non-mandated cases led to inconsistent practices when determining the need for and content of a DUA. In December 2010, the Under Secretary for Health formed the Managing Data Workgroup to recommend solutions to VHA's most pressing data management challenges. The Workgroup made several recommendations. One recommendation focused on making data more accessible to those with approved requirements for data access. The term Data Transfer Agreement (DTA) had been adopted within VHA to distinguish between legally required agreements and agreements made as a best practice to protect the organization and the data but not otherwise required by law. While different terms were used to describe different purposes, the same templates were being used for both DUAs and DTAs. Using the same template led to confusion throughout VHA. For consistency and uniformity, this directive stipulates the use of the term "DUA" for agreements subject to this directive, and discontinues the use of the term "DTA."

c. VHA Directive 1080, Access to Individually Identifiable Information in Information Technology Systems, dated January 6, 2017, establishes policy for approving and providing access to VHA personally identifiable information (PII), including protected health information (PHI), in Information Technology (IT) VA systems. This directive, by establishing policy and procedures related to DUAs, sets forth requirements to VHA business data stewards on appropriate terms and conditions associated with transfers of confidential or protected data. ***NOTE:*** *"DUA" as used in this directive is not solely limited to the agreement required by the HIPAA Privacy Rule for covered entities such*

as VHA to use or disclose a Limited Data Set (LDS) of protected health information, but instead is meant to more broadly encompass data sharing agreements of protected health information in other circumstances.

3. DEFINITIONS

a. **Access.** Access is the viewing, inspecting, or obtaining a copy of individually identifiable information (III) or PHI electronically, on paper, or via another medium.

b. **Business Associate.** For purposes of this directive, a business associate is an entity including an individual, company, or organization that performs or assists in the performance of a function or activity on behalf of VHA that involves creating, receiving, maintaining, or transmitting PHI, or on behalf of VHA, an entity that provides certain services as specified in the HIPAA Privacy Rule that involve the disclosure of PHI by VHA. The term "business associate" also includes a subcontractor that creates, receives, maintains, or transmits PHI on behalf of the business associate. Entities directly tied to a specific research protocol are not business associates. Individuals or organizations providing services subsequent to a research protocol, (e.g., long-term storage of banked research data) are business associates and require Business Associate Agreements (BAAs) prior to disclosure of PHI to the business associate.

c. **Business Associate Agreement.** For purposes of this directive, a BAA is an agreement between VHA and a Business Associate, that must be entered into before PHI can be released to the Business Associate, in order for the Business Associate to perform a covered activity for VHA.

d. **Business Data Steward.** A knowledge worker, business leader, and recognized subject matter expert assigned accountability for the data specifications and data quality of specifically assigned business entities, subject areas, or databases. Business Data Stewards are identified by the line of business or program office and are experts in the way data are used in the performance of VA's mission. They are responsible for defining data requirements and determining access needs and appropriate usage for data.

e. **Data Ownership.** As determined through legal opinion VAOPGCADV 07-2007 by the VA Office of General Counsel (OGC), the official owner of data within VHA is the Under Secretary for Health. All VHA data will fall under the Under Secretary for Health, and the Under Secretary for Health has the implementation and oversight responsibilities for this data. Transfer of ownership of specific data assets may be appropriate based on the circumstances and must be determined and documented prior to data release or disclosure.

f. **Data Use Agreement.** A DUA is a contractual agreement that:

(1) Governs the sharing of data between a business data steward and requestor.

(2) Defines ownership as related to the release of VHA data.

(3) Establishes the specific terms of use and disclosure for the requestor.

(4) Establishes specific ethical expectations and principles regarding access to and use of Veterans' health data.

(5) Defines transfer liability for the protection of the data from the business data steward to the requestor.

(6) Under most circumstances, is considered "internal' if the requestor is within VA and "external" if the requestor is outside VA.

(7) May describe interactive data exchange activity between entities, if applicable.

(8) Serves as a means to establish criteria for using, disclosing, accessing, storing, processing, and disposing of data.

(9) Satisfies HIPAA requirements when providing information within an LDS.

g. **De-identified Information.** De-identified information is health information that does not identify an individual, there is no reasonable basis to believe that the information can be used to identify an individual because the 18 patient identifiers described in the HIPAA Privacy Rule have been removed, and the covered entity does not have actual knowledge that information could be used to identify an individual. Names, street addresses (other than town, city, State and Zip code), telephone numbers, Social Security Numbers, fax numbers, dates directly related to an individual, email addresses, medical record numbers, health plan beneficiary numbers, account numbers, certificate license numbers, vehicle identifiers and serial numbers, device identifiers and serial numbers, URLs, IP address numbers, full face photos (or comparable images) and biometric identifiers are included within the 18 patient identifiers. The covered entity and requestor agree to abide by applicable limitations, qualifications, conditions, or restrictions set forth in the HIPAA Expert Determination associated with de-identified information. The covered entity and the requestor will acknowledge and affirm in writing that the data are also non-identifiable under 5 U.S.C. § 552a, Privacy Act of 1974; 38 U.S.C. § 5701, Confidential Nature of Claims; and 38 U.S.C. § 7332, Confidentiality of Certain Medical Records and is therefore not subject to statutes in its current State. See 45 C.F.R. 164.514(b)(2)(i).

h. **Designated Signatory Official.** For the purposes of this directive, the Designated Signatory Official is the individual authorized to enter into and sign a DUA as or on behalf of the business data steward and the requestor.

i. **Disclosure.** For purposes of this directive, the term disclosure refers to the release, transfer, provision of, access to, or divulging in any other manner information outside VHA. When information is disclosed, VHA retains ownership of the original data through a BAA, contract, or other written agreement. There are some cases in which VHA may choose to relinquish ownership of the copy of the information. Based on opinion from OGC, VHA may give up data ownership when there is no legal requirement, business need, or organizational interest to own the data after it is

disclosed.

j. **Freedom of Information Act.** The Freedom of Information Act (FOIA) is a Federal law that compels the disclosure of agency records to any person upon written request, unless one or more of nine exemptions apply to the records. See 38 C.F.R. 1.554(a)(1)-(9)). FOIA, 5 U.S.C. § 552, is implemented in VA by 38 C.F.R. 1.550-1.562.

k. **Health Information.** Health information is any information, recorded in any form including oral, created or received by a health care provider, public health authority, employer, life insurer, school, university, health care clearinghouse, or health plan that relates to the past, present, or future physical or mental health condition of an individual; the provision of health care to an individual; or payment for the provision of health care to an individual. This encompasses information pertaining to examination, medical history, genetics, diagnosis, and findings or treatment, including laboratory examinations, X-rays, microscopic slides, photographs, and prescriptions. See 45 C.F.R. 160.103.

l. **Individually Identifiable Health Information.** Individually identifiable health information (IIHI) is a subset of health information, including demographic information collected from an individual, that:

(1) Is created or received by a health care provider, health plan, health care clearinghouse (e.g., a HIPAA-covered entity, such as VHA), or employer.

(2) Relates to the past, present, or future physical or mental condition of an individual; the provision of health care; or payment for health care to an individual.

(3) Identifies the individual or a reasonable basis exists to believe the information can be used to identify the individual. ***NOTE:*** *VHA uses the term IIHI to define information covered by the Privacy Act of 1974 and the Title 38 confidentiality statutes (38 U.S.C. § 570, Confidential Nature of Claims and 38 U.S.C. § 7332, Confidentiality of Certain Medical Records), in addition to HIPAA.*

m. **Individually Identifiable Information.** Individually identifiable information (III) is any information pertaining to an individual that is retrieved by the individual's name or other unique identifier, as well as IIHI, regardless of how it is retrieved. III is a subset of PII and is protected by the Privacy Act of 1974. ***NOTE:*** *See VHA Directive 1605.01, Privacy and Release of Information, dated August 31, 2016, for more information about PII.*

n. **Limited Data Set.**

(1) Limited Data Set (LDS) is PHI which excludes certain specified direct identifiers of the individual, their relatives, household members, or employers. These excluded identifiers include the following:

(a) Name.

(b) Address (other than town or city, State, or Zip code).

(c) Phone number.

(d) Fax number.

(e) Email address.

(f) Social Security Number (SSN).

(g) Medical record number.

(h) Health plan number.

(i) Account number.

(j) Certificate and license number.

(k) Vehicle identification.

(l) Device identifier.

(m) Web universal resource locator (URL).

(n) Internet protocol (IP) address number.

(o) Biometric identifier.

(p) Full-face photographic image.

(2) The two patient identifiers that can be included as part of an LDS are dates directly related to an individual and postal address information that is limited to town or city, and State or ZIP code. Thus, an LDS is not de-identified information, and it is covered by the HIPAA Privacy Rule. An LDS may be used and disclosed for research, health care operations, and public health purposes pursuant to a DUA. See 45 C.F.R. 164.514(e).

o. **Memorandum of Understanding.** A Memorandum of Understanding (MOU) is a document which defines the responsibilities of the parties entering into the agreement. An MOU customarily defines business terms, which may include data releases or transfers.

p. **Protected Health Information.** The HIPAA Privacy Rule defines Protected Health Information (PHI) as IIHI transmitted or maintained in any form or medium by a covered entity, such as VHA. ***NOTE:*** *VHA uses the term "protected health information" to define information that is covered by HIPAA but unlike III may or may not be covered by the Privacy Act of 1974 or 38 U.S.C. §§ 5701 and 7332, the Title 38 confidentiality statutes. In addition, PHI excludes employment records held by VHA in its role as an employer.*

q. **Requestor.** For purposes of this directive, the requestor is the person, program office, or entity generating applications to receive VHA III or PHI.

r. **VA Information Technology Systems.** For purposes of this directive, VA Information Technology Systems (VA IT Systems) are any electronic systems containing III or PHI belonging to VHA and that are maintained by either VA or VHA.

s. **VHA Data.** For purposes of this directive, VHA data are factual information related to the VA organizational component responsible for coordinating and providing health care for enrolled Veterans. VHA information systems consist of multiple levels, such as local VA medical facility data.

4. POLICY

It is VHA policy to conform to the legal requirements of using data use agreements (DUAs) to ensure proper use and disclosure of Protected Health Information (PHI) found in Limited Data Sets (LDS) under the HIPAA Privacy Rule. Furthermore, this directive provides policy for implementing data use agreements for other appropriate disclosures of individually-identifiable information and other forms of VHA data. This directive does not apply to the sharing or transmission of VHA research data in research data repositories or in the possession of VHA research investigators.

5. RESPONSIBILITIES

a. **Under Secretary for Health.** The Under Secretary for Health is responsible for:

(1) Ensuring overall VHA compliance with this directive.

(2) Signing approval letters when required to accompany a DUA. See Appendix A.

b. **Deputy Under Secretary for Health.** The Deputy Under Secretary for Health is responsible for ensuring the Director, Office of Health Informatics (OHI), Health Information Governance (HIG) complies with 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 Service Networks (VISNs).

(2) Assisting VISN Directors in resolving implementation and compliance challenges.

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

d. **Director, Office of Health Informatics, Health Information Governance.** The Director, OHI, HIG is responsible for ensuring that the Director, National Data Systems (NDS) creates and updates national policy regarding DUAs.

e. **Director, National Data Systems.** The Director, NDS is responsible for:

(1) Establishing and distributing policies and procedures for access to VHA III and PHI, including the utilization of DUAs, excluding DUAs and procedures related to research III and PHI.

(2) Developing and maintaining processes and mechanisms for collecting, storing, managing, and reporting DUAs on behalf of VHA.

(3) Collecting, storing, and tracking signed copies of completed DUAs from VHA Business Data Stewards on behalf of VHA.

(4) Collaborating with the VHA Privacy Compliance Assurance (PCA) Office to define the assessment scope, questions to be asked, and observations to be made during PCA and VA medical facility self-assessment surveys.

f. **Director, VHA Privacy Office.** The Director, VHA Privacy Office is responsible for:

(1) Providing general subject matter expertise for DUAs when requested and reviewing all DUAs when they are related to disclosures outside VA of national level VHA data requiring national level permissions.

(2) Determining if there is legal authority for the release of VHA data.

(3) Drafting an approval letter for the signature of the Under Secretary for Health, when required to accompany a DUA.

g. **Director, VHA Freedom of Information Act Office.** Director, VHA FOIA Office, is responsible for determining whether the requested information is releasable under the provisions of FOIA.

h. **Director, VHA Privacy Compliance Assurance Office.** Director, VHA PCA Office is responsible for:

(1) Monitoring compliance with this directive in accordance with VHA Directive 1605.03, Privacy Compliance Assurance Program and Privacy/Freedom of Information Act (FOIA) Continuous Readiness Review and Remediation, dated September 19, 2019.

(2) Providing a written report specifying the details if it is determined that the terms of a DUA are not being met and developing a remediation strategy that must be satisfied by the requestor.

(3) Collaborating with NDS to define the assessment scope, questions to be asked, and observations to be made during PCA and VA medical facility self-assessment surveys.

(4) Reviewing DUAs in instances of national VHA data existing outside VA, when such DUAs are required, to ensure security requirements and responsibilities for proper documentation.

i. **Director, VHA Health Care Security Requirements Office.** Director, VHA Health Care Security Requirements (HCSR) Office is responsible for reviewing DUAs in instances of disclosures of national VHA data outside VA, when such DUAs are required, to ensure security requirements and responsibilities are properly documented.

j. **VHA Program Officers.** VHA Program Officers are responsible for ensuring that all personnel under their direction comply with the requirements of this directive.

k. **Veterans Integrated Services Network Director.** The VISN Director is responsible for ensuring that all personnel under their direction comply with the requirements of this directive.

l. **VA Medical Facility Director.** The VA medical facility Director is responsible for ensuring that all personnel under their direction comply with the requirements of this directive.

m. **VA Medical Facility Chief Officers.** The VA medical facility Chief Officers are responsible for ensuring that all personnel under their direction comply with the requirements of this directive.

n. **VHA Program Office Privacy Liaison.** The VHA Program Office Privacy Liaison is responsible for:

(1) Annually reviewing their VA medical facility's compliance with this directive and reporting these findings to the VHA PCA Office as a part of the VA medical facility self-assessment survey to ensure that an annual review of compliance is maintained.

(2) Notifying the VHA PCA Office to schedule an assessment if it is suspected that the terms of a DUA are not being met.

o. **VHA Business Data Stewards.** VHA Business Data Stewards can function at national, VISN, and VA medical facility levels. VHA Business Data Stewards are responsible for:

(1) Determining if a DUA is required. ***NOTE:*** *Consultation with the VHA Privacy Office may be necessary to make this determination.*

(2) Entering into a DUA before transferring or sharing VHA data, as required by this directive and other VHA policy. ***NOTE:*** *See paragraph 12, References, for a comprehensive list of related policies.*

(3) Determining whether ownership is retained or relinquished when sharing copies of VHA data with non-Federal entities. ***NOTE:*** *VHA retains ownership in the original data files shared.*

(4) Consulting with the VHA Business Data Steward's Privacy Officer and others (e.g., the VHA Business Data Steward's Information System Security Officer (ISSO)) as appropriate to determine if the data can and should be shared and if relinquishing ownership of the copies provided to the requestor is appropriate as defined by this directive.

(5) Ensuring that OGC reviews and approves DUAs in circumstances when guidance to prohibit or permit disclosure of the data are not defined in law, regulation, or other VHA policies.

(6) Being accountable for the release of the data and monitoring any DUA the VHA Business Data Steward generates as defined by this directive.

(7) Determining if a national review by VHA HCSR Office and VHA Privacy Office is appropriate.

(8) Forwarding a signed copy of each new DUA completed to NDS for tracking and archival purposes. Program offices should maintain an official source copy of the DUA for inspection and review.

(9) Notifying the VHA PCA Office to schedule an assessment if it is suspected that the terms of a DUA are not being met.

p. **VHA Business Data Steward's Information System Security Officers.** The VHA Business Data Steward's ISSO is responsible for:

(1) Reviewing and providing concurrence or non-concurrence for all DUAs generated by the VHA Business Data Steward based on compliance with VA information or cybersecurity policies. ***NOTE:*** *See paragraph 12, References, for a comprehensive list of related policies.*

(2) Annually reviewing their VA medical facility's compliance with this directive and reporting these findings to the VHA PCA Office as a part of the VA medical facility self-assessment survey to ensure an annual compliance review is maintained.

(3) Notifying the VHA PCA Office to schedule an assessment if it is suspected that the terms of a DUA are not being met.

q. **VHA Business Data Steward's Privacy Officers.** The VHA Business Data Steward's Privacy Officers are responsible for:

(1) Reviewing any DUA when sharing or disclosing VA medical facility-level PII with an outside entity.

(2) Providing concurrence or non-concurrence for all DUAs generated by an associated VHA Business Data Steward, based on whether privacy legal authority exists for sharing VHA data.

(3) Annually reviewing their VA medical facility's compliance with this directive and reporting these findings to the VHA PCA Office as a part of the VA medical facility self-assessment survey to ensure that an annual review of compliance is maintained.

(4) Notifying the VHA PCA program to schedule an assessment if it is suspected that the terms of a DUA are not being met.

6. DETERMINING WHEN A DATA USE AGREEMENT IS REQUIRED OR PROHIBITED

a. Determining if a DUA is required or prohibited is based on who is requesting the information and the manner and purpose for which the requestor will use the data. The business data steward is ultimately responsible for this determination. Refer to the DUA Decision Tree at the VHA Data Portal (http://vaww.vhadataportal.med.va.gov/PolicyAdmin/DataUseAgreements.aspx) and Appendix A, Case Use Examples, for further details. ***NOTE:*** *This is an internal VA website that is not available to the public.*

b. In general, the purpose of a DUA is:

(1) To document the transfer of liability to an external entity if ownership of the data transfers and to document such change in data ownership.

(2) To bind the behavior of the requestor to specific data use limitations if ownership is retained by VHA. Specified behaviors must include adherence to VA's ethical principles for access to and use of Veterans' health data.

(3) To clearly and specifically communicate ethical standards regarding access and use of Veterans' health data.

(4) To document ownership status; establish appropriate rules based on this status and establish criteria to access, use, disclose, store, process, copy, transfer, and dispose of data; and identify who has access to and control of the information at both origination and requestor locations.

(5) To decide to provide the data under VHA discretion in situations where VHA may condition the use, release, or disclosure of VHA data on the signing of the DUA.

(6) Not used in situations where VHA is mandated by policy or required by law or regulation to release or disclose the data.

c. Whether a DUA is required or prohibited, the business data steward has accountability for the data under their oversight. It is the business data steward's prerogative to record data sharing activity by using other mediums, e.g., memorandums, written narratives. At a minimum, the following data elements must be captured by the data steward using a DUA or other data sharing agreement, for aggregate reporting purposes:

(1) Name of the requestor.

(2) Type or category of data shared.

(3) Stated use of the data.

(4) Authority under which the data was disclosed.

(5) Final disposition of the data.

(6) Ownership status of the data provided to the requestor.

(7) Any limitations on the use of the data (such as with a LDS).

(8) A prohibition on any data re-identification when this is applicable.

d. A DUA is required in the following instances:

(1) The HIPAA Privacy Rule requires a covered entity to use a DUA when the covered entity uses or discloses a LDS, unless there is other authority for the PHI use/disclosure to ensure the requestor of the LDS will only use or disclose the PHI for the specific purposes listed in the Privacy Rule.

(2) When VHA PHI is to be shared with a non-VA entity, a DUA is required prior to the disclosure unless prohibited in paragraph 6.e. of this directive or other circumstances. A DUA is also required when VHA III (broader than PHI) is shared with a non-VA entity. VHA must be able to identify the specific disclosure authority under all applicable VA confidentiality statutes and regulations which would allow such a disclosure. For purposes of this directive, the VHA Privacy Office determines the applicable disclosure authority. For guidance on disclosure authority, contact the VHA Privacy Office at VHAPrivIssues@va.gov.

(3) In special circumstances, such as when a signed agreement is in place (see paragraph 7 of this directive).

e. Under certain circumstances, such as public health authority and congressional mandate, a DUA should not be used because the disclosure will be made without any conditions. These circumstances preclude VHA from putting any further conditions upon the release or disclosure of the data. Adherence to VA's ethical principles for access to and use of Veterans' health data remains a component of the data release or disclosure. DUAs are not used in the following circumstances:

(1) When VHA discloses data in response to a FOIA request.

(2) When there is a BAA in place with a business associate as required by HIPAA regulations.

(3) When VHA data are requested by an entity that is charged with health care

oversight of VA specifically for the purpose of their oversight activities, including but not limited to:

(a) The White House.

(b) The Office of Management and Budget.

(c) A Member of Congress.

(d) The House Veterans' Affairs Committee and Senate Veterans' Affairs Committee.

(e) The Government Accountability Office.

(f) The Department of Health and Human Services, Office for Civil Rights.

(g) VHA Office of Research Oversight.

(h) VA Office of the Inspector General.

(i) The Office of the Secretary of Veterans Affairs for purposes of health care oversight.

(4) When VHA data are requested by a law enforcement entity for a specific criminal activity pursuant to a Privacy Act of 1974 (b)(7), law enforcement request, or pursuant to a standing request.

(5) When VHA data are requested by a State public health authority pursuant to a standing written request letter or when VHA initiates release to the State public health authority for the purpose of promoting public health and patient safety with the exception of a State Cancer Registry.

(6) When VHA data are disclosed to a State abuse hotline in order to report suspected or alleged abuse.

(7) When VHA data are disclosed for the purpose of treatment or payment.

(8) When VHA data are requested by a member of Congress in response to an inquiry from a Veteran for assistance in a VA matter. ***NOTE:*** *This is not considered health care oversight*. *A written authorization or a copy of the original correspondence from the Veteran requesting the Congressperson's assistance must be provided.*

(9) When VHA data regarding a Veteran's health, health care, or payment for care are disclosed to that Veteran, their legal representative (e.g., a Veterans Service Organization), authorized family member, or friend authorized by the Veteran to have access to the Veteran's PHI.

(10) When an agreement is in place that expressly and wholly binds specific behavior related to data sharing, such as certain MOUs, or other data sharing agreements.

(11) When PHI is being shared with an individual, subject to HIPAA authorization.

7. SPECIAL CIRCUMSTANCES AND EXCEPTIONS

a. When internal Data Use Agreements (DUAs) are required by agreement with external entities, such as the Centers for Medicare and Medicaid Services (CMS), these mandates specify particular handling and processing requirements in order to track internal redistribution of the information (see Appendix A, Case Use Examples, for further detail).

b. Depending on the reason for the data sharing, other types of written agreements such as a Memorandum of Understanding (MOU), Cooperative Research and Development Agreement (CRADA), or standing written request letter, may supplant a DUA. These agreements must cite the authority to disclose data and expressly document any limitations of the data sharing.

c. To determine requirements for the use of DUAs in VA research, refer to VHA Handbook 1200.12, Use of Data and Data Repositories, dated March 9, 2009.

8. ESTABLISHING DATA USE AGREEMENTS

a. When a DUA is required by regulation such as the HIPAA Privacy Rule or VHA policy, the DUA template(s) referenced in this directive and released by NDS must be used unless there are noted exceptions. These templates facilitate VHA-wide reporting capabilities and ensure that required language is used as well as foster the ease of data sharing.

b. The DUA templates are tailored for sharing VHA PHI or de-identified information with other Federal and non-Federal entities as well as the sharing of information based on an LDS. The differences between these templates relate to the ownership of the data and the rules that are in place based on that ownership status. ***NOTE:*** *Some VHA program offices may have prior authorization to use other unique or alternative DUA templates. For situations that do not fall into the above scenarios, please contact: VHA10P2CDataAgreements@va.gov.*

9. PROCESSING AND MONITORING DATA USE AGREEMENTS

a. When the VHA Business Data Steward has determined a DUA is required and the appropriate template has been completed, the DUA is reviewed and processed in accordance with the DUA Process Flow (Chart is available at the VHA Data Portal: http://vaww.vhadataportal.med.va.gov/Home.aspx. ***NOTE:*** *This is an internal VA website that is not available to the public.*).

b. This process is outlined as follows:

(1) The appropriate DUA is generated by the VHA Business Data Steward and completed by the requestor.

(2) The VHA Business Data Steward's ISSO and the VHA Business Data Steward's Privacy Officer must review the DUA to determine if the terms of the agreement comply with all applicable Federal laws, regulations, and VA and VHA policies. The Business Data Steward's ISSO and the Business Data Steward's Privacy Officer will provide a concurrent signature for the terms of a DUA.

(3) The DUA is signed by the VHA Business Data Steward and the Designated Signatory Official of the requestor.

(4) The VHA Business Data Steward determines whether a national review by VHA HCSR Office and VHA Privacy Office is appropriate. This includes situations where the data being disclosed is either of a national level (such as data containing patient or beneficiary information which is stored within national data warehouses or registries) or is released on a recurring basis.

(5) A signed copy of the completed DUA must be forwarded to NDS for tracking and archival purposes. Instructions for submission are provided on the DUA Page on the VHA Data Portal. (See http://vaww.vhadataportal.med.va.gov/PolicyAdmin/DataUseAgreements.aspx. ***NOTE:*** *This is an internal VA website that is not available to the public*). This is considered the official Federal record.

c. In circumstances where guidance to prohibit or permit disclosure of the data are not defined in law, regulation, or VHA policies, VHA Business Data Stewards will ensure the DUA is reviewed and approved by VA OGC. There may be consultation with other offices including VHA Privacy, VA Information Security, VA National Center for Ethics in Health Care, and National Data Systems.

d. If there is an approval letter that must be signed by the Under Secretary for Health, VA OGC must review and concur prior to gaining the signature of the Under Secretary for Health.

e. VHA Business Data Stewards are accountable for ensuring the terms of the DUA are being met and must confirm compliance with the requestor on an annual basis if ownership is retained by VHA. If the VHA Business Data Steward, VA medical facility Privacy Officer, or VA medical facility ISSO suspects the terms of a DUA are not being met, the facility Compliance and Business Integrity Office and the VHA PCA Office must be notified to schedule an assessment to determine if the requestor is compliant with the DUA. If it is determined that the terms of the agreement are not being met, PCA must provide a written report specifying the details. PCA will develop a remediation strategy that must be satisfied by the requestor. Questions about whether the ethical principles for data access and use are being met should be referred to the VA National Center for Ethics in Health Care.

f. VA medical facility Privacy Officers, in collaboration with VA medical facility ISSOs,

will annually review their VA medical facility's compliance with this directive and report these findings to PCA as part of the VA medical facility self-assessment survey to ensure an annual compliance review is maintained. NDS and PCA must collaborate to define the assessment scope, questions to be asked, and observations to be made during PCA and VA medical facility self-assessment surveys. Questions about whether the ethical principles for data access and use are being met should be referred to the VA National Center for Ethics in Health Care.

10. TRAINING

There are no formal training requirements associated with this directive.

11. 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 Manager or Records Liaison.

12. REFERENCES

a. 5 U.S.C. § 552.

b. 38 U.S.C. § 5701.

c. 38 U.S.C. § 7301(b).

d. 38 U.S.C. § 7332.

e. 38 C.F.R. 1.550-1.559.

f. 45 C.F.R. Parts 160 and 164.

g. VA Directive 6066, Protected Health Information (PHI) and Business Associate Agreements Management, dated September 2, 2014.

h. VA Directive 6500, VA Cybersecurity Program, dated January 24, 2019.

i. VA Handbook 6500.6, Contract Security, dated March 12, 2010.

j. VHA Directive 1072, Release of VA Data to State Cancer Registries, dated July 23, 2014.

k. VHA Directive 1080, Access to Individually Identifiable Information in Information Technology Systems, dated January 6, 2017.

l. VHA Directive 1153(1), Access to Centers for Medicare and Medicaid Services (CMS) and United States Renal Data System (USRDS) Data for Veterans Health

Administration (VHA) Users Within the Department of Veterans Affairs (VA) Information Technology (IT) Systems, dated April 15, 2016.

m. VHA Directive 1605, VHA Privacy Program, dated September 1, 2017.

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

o. VHA Directive 1605.02, Minimum Necessary Standard for Access, Use, Disclosure, and Requests for Protected Health Information, dated April 4, 2019.

p. VHA Directive 1605.03, Privacy Compliance Assurance Program and Privacy/Freedom of Information (FOIA) Continuous Readiness Review and Remediation, dated September 29, 2019.

q. VHA Handbook 1605.05, Business Associate Agreements, dated July 22, 2014.

r. VHA Handbook 1200.12, Use of Data and Data Repositories in VHA Research, dated March 9, 2009.

s. Certificate of Confidentiality, National Institutes of Health, http://grants.nih.gov/grants/policy/coc/.

t. DUA Templates. http://vaww.vhadataportal.med.va.gov/PolicyAdmin/DataUseAgreements.aspx. ***NOTE:*** *This is an internal VA website that is not available to the public.*

u. Fact Sheet: Veterans Health Administration Guidance for Sharing Data with Other Federal Agencies, Volume 01, Number 01, June 2019, https://vaww.vhadataportal.med.va.gov/PolicyAdmin/PolicyAdministrationOverview.aspx . ***NOTE:*** *This is an internal VA website that is not available to the public.*

v. "How to Request CMS Data," MAC homepage, http://vaww.va.gov/medicareanalysis/. ***NOTE:*** *This is an internal VA website that is not available to the public.*

w. "VA Data Governance Council Clarification of Roles and Responsibilities," October 2, 2019, https://www.ea.oit.va.gov/VA_EA/Business-Models_Reports.asp.

x. VIReC's VA/CMS Data for Research Projects Policies," http://vaww.virec.research.va.gov/Index-VACMS.htm. ***NOTE:*** *This is an internal VA website that is not available to the public.*

y. Department of Veterans Affairs Ethical Framework Principles for Access to and Use of Veterans' Data, Ethics Principles for Access to and Use of Veteran Data | Office of Information and Technology (va.gov)

APPENDIX A

CASE USE EXAMPLES

1. INTRODUCTION

Paragraph 6 in the body of this directive provides overall guidance when Data Use Agreements (DUAs) are required or should not be used. This appendix provides additional information about the guidance including exceptions and unique circumstances and identifies other sources of governance.

2. CENTERS FOR MEDICARE AND MEDICAID SERVICES DATA

a. The Veterans Health Administration (VHA) is required to create internal DUAs when redistributing Center for Medicare and Medicaid Services (CMS) raw and merged data (VA/CMS data) to internal VHA users in compliance with the Information Exchange Agreement between VHA and CMS, and VHA Directive 1153(1), Access to Centers for Medicare and Medicaid Services (CMS) and United States Renal Data System (USRDS) Data for Veterans Health Administration (VHA) Users Within the Department of Veterans Affairs (VA) Information Technology (IT) Systems, dated April 15, 2016.

b. Guidance for providing VA/CMS data for administrative purposes is provided by VHA Medicare and Medicaid Analysis Center (MAC). MAC requirements for obtaining VA/CMS data, including the requirement for a DUA, can be found under the "How to Request CMS Data" tab on the MAC homepage (http://vaww.va.gov/medicareanalysis/. ***NOTE:*** *This is an internal VA website that is not available to the public.).*

c. Guidance for providing VA/CMS data for research purposes is provided by VA Information Resource Center (VIReC). VIReC requirements for obtaining VA/CMS data can be found in the document "VIReC's VA/CMS Data for Research Projects Policies" (http://vaww.virec.research.va.gov/Index-VACMS.htm. ***NOTE:*** *This is an internal VA website that is not available to the public.).*

3. LIMITED DATA SETS

A DUA may be required when sharing data that meets the definition of a limited data set (LDS) under the Health Insurance Portability and Accountability Act's (HIPAA) Privacy Rule. For guidance on LDS, see VHA Directive 1605.01, Privacy and Release of Information, dated August 31, 2016.

4. NON-FEDERAL GOVERNMENT ENTITIES

a. **State Cancer Registries.** See VHA Directive 1605.01 Privacy and Release of Information, dated August 31, 2016, and VHA Directive 1072, Release of VA Data to State Cancer Registries, dated July 23, 2014, for guidance.

b. **Public Health Authorities.** See VHA Directive 1605.01 for guidance.

c. **State, Local, or Municipal Courts.** VHA protected health information (PHI) may be released for use in proceedings of a State, local, or municipal court upon receipt of a court order issued or approved by a judge or a subpoena if the same is also signed by a judge (has the effect of a court order). A DUA should not be used if the data are being disclosed pursuant to a court order. See VHA Directive 1605.01 for more information.

d. **State Prescription Drug Monitoring Programs.** VHA may disclose individually identifiable health information (IIHI) to a State Prescription Drug Monitoring Program (SPDMP) without the signed written authorization of the patient for whom the medication was prescribed. Disclosure may be for the purpose of querying the SPDMP or reporting mandatory prescription information to the State. For more information, see: *https://vaww.vets.vaco.portal.va.gov/sites/privacy/vhapo/PrivacyWiki/Registries.aspx.* ***NOTE:*** *This is an internal VA website that is not available to the public.*

e. **All Other Non-Federal Government Entities.** VHA Business Data Stewards may authorize disclosure of VHA data to other non-Federal government agencies in accordance with Federal law, the HIPAA Privacy Rule, or VA and VHA policy. Absent a signed, written authorization from the data subject and those exceptions listed in paragraph 7 in the body of this directive, a DUA or other documentation that contains the elements of a DUA is required, unless prohibited by law, regulation, VA or VHA policies. If the data are to be used by a business associate (for a reason separate and apart than the one specified in the Business Associate Agreement), contractor, or other non-government agent on behalf of the requestor, then this must be specified in the DUA. ***NOTE:*** *The VHA Business Data Steward's Privacy Officer must identify the authority under which the data may be disclosed.*

5. NON-GOVERNMENTAL ORGANIZATIONS OR INDIVIDUALS

a. **Freedom of Information Act Requests.** If the requested data are processed under the Freedom of Information Act (FOIA), a DUA should not be used. The request must be processed by the Business Data Steward's VHA FOIA Officer in accordance with VHA policy.

b. **Research Data Requests.** At times, VHA data will be requested by non-VA investigators for research projects that are not VA research projects nor collaborative research projects with VA investigators. For policies pertaining to the management of research data, data transfers, and data use agreements, please refer to VHA Handbook 1200.12, Use of Data and Data Repositories, dated March 9, 2009, and applicable Office of Information and Technology and VHA privacy policies, including VHA Directive 1605.01. Additional information about the various privacy laws and regulations that may apply to release of information (ROI) for Non-VA Investigators (Extramural) is available at, https://dvagov.sharepoint.com/sites/vacovetsprivacy/vhapo/Pages/laws.aspx. ***NOTE:*** *This is an internal VA website that is not available to the public.*

6. OTHER FEDERAL GOVERNMENT ENTITIES

VHA may share data with other Federal agencies, provided a DUA is in place in

order to ensure that the data will only be used for the purpose(s) for which it was requested. Contingent upon special exceptions, DUAs are prohibited in the following circumstances:

a. **Federal Entities Charged with Health Care or Research Oversight.** When VHA data are requested for oversight activities by a Federal government agency charged with health care or research oversight. Examples of such agencies include but are not limited to the Executive Office of the President, the Office of Management and Budget, a member of Congress, the United States House of Representatives Committee on Veterans' Affairs or its respective subcommittees, the United States Senate Committee on Veterans' Affairs or its respective subcommittees, the United States Department of Health and Human Services, the VA Office of the Inspector General, the Governmental Accountability Office, and the VHA Office of Research Oversight.

b. **Federal Courts.** When VHA PHI will be disclosed for use in proceedings of a Federal court upon receipt of a court order signed by a judge or a subpoena issued or also signed by a judge. (See VHA Directive 1605.01 for more information).

7. VA CONTRACTORS

Generally, DUAs are not used when sharing data with VA contractors pursuant to a valid contract that includes a description of the use, transfer, and all privacy and security requirements set forth in VA Handbook 6500.6, Contract Security, dated March 12, 2010. Exception: A DUA is required when a business associate wants to use an LDS for another purpose approved by VHA. ***NOTE:*** *For more information on the security requirements in contracts, see VA Handbook 6500.6.*

APPENDIX B

DATA USE AGREEMENT TEMPLATES

1. INTRODUCTION

The Data Use Agreements (DUA) templates have been designed to contain the essential elements that describe the use and disclosure of Veterans Health Administration (VHA) protected health information (PHI) being shared. All templates describe what VHA PHI is being shared and with whom; the templates ensure the appropriate levels of security and privacy reviews are conducted. All templates cite the authorities under which VHA may share the data and describe the means of its transfer, storage, and access. These templates vary based on ownership status of the requested data and the language associated with protecting the data. The DUA templates are individually described below, and the templates are available at the VHA Data Portal: http://vaww.vhadataportal.med.va.gov/PolicyAdmin/DataUseAgreements.aspx. ***NOTE:*** *This is an internal VA website that is not available to the public.*

2. DATA USE AGREEMENTS FOR FEDERAL ENTITIES

a. When data are shared with Federal entities, ownership of the copy of the data transfers to the other Federal entity. As a component of the Federal government, the entity is subject to much of the same information security laws and regulations, such as the Federal Information Security Management Act and Federal Information Processing Standards as VA. Similarly, when data are received by VHA from another Federal entity, the data becomes VHA data.

b. When sharing VHA PHI with other Federal entities, the data may become part of those Federal entities' Privacy Act System of Records Notices if a personal identifier is used to retrieve information by the Federal entity. In other instances where information is not retrieved by a personal identifier, references to a Privacy Act System of Records will not be applicable and should not be included in the DUA. ***NOTE:*** *Information disclosed as part of a limited data set (LDS) cannot be retrieved by an individual identifier (e.g., name, account number, email address, picture, Social Security Number) and therefore is not covered by the Privacy Act of 1974.*

3. DATA USE AGREEMENTS FOR NON-FEDERAL ENTITIES

When sharing VHA PHI with non-Federal entities, VHA may choose to retain or relinquish ownership of the data depending on the situation. The DUA binds the behavior of the requestor to specific uses or limitations of the data including ethical expectations and principles regarding access to and use of Veterans' health data.

4. DATA USE AGREEMENTS FOR LIMITED DATA SETS WITH FEDERAL ENTITIES

This template has specific language to address requirements of the HIPAA Privacy Rule and ethical expectations and principles regarding access to and use of Veterans' health data.

5. DATA USE AGREEMENTS FOR LIMITED DATA SETS WITH NON-FEDERAL ENTITIES

This template has specific language to address requirements of the HIPAA Privacy Rule and ethical expectations and principles regarding access to and use of Veterans' health data.

6. DATA USE AGREEMENTS FOR RELEASE OF DE-IDENTIFIED INFORMATION TO NON-FEDERAL ENTITY

This template outlines conditions under which a covered entity (VHA) provides a requestor with de-identified information. In using this DUA template and associated de-identified information, the covered entity and requestor agree to abide by the conditions, qualifications, and limitations set forth in the Health Insurance Portability and Accountability Act's (HIPAA) Privacy Rule Expert Determination provisions and ethical expectations and principles regarding access to and use of Veterans' health data. ***NOTE:*** *If all 18 HIPAA identifiers are removed, as prescribed by the Privacy Rule's safe harbor de-identification process, then the limitations set forth in the Expert Determination provision would not be required.*

7. DATA USE AGREEMENTS FOR THE PURPOSE OF RESEARCH WITH NON-FEDERAL ENTITIES

This template establishes terms and conditions, including ethical expectations and principles regarding access to and use of Veterans' health data, under which a VA medical facility or VHA program office can provide VHA PHI to a requestor with a non-Federal organization to use for the purpose of research. For guidance pertaining to the management of research data, data transfers, and DUA please refer to VHA Handbook 1200.12, Use of Data and Data Repositories, dated March 9, 2009, and the Office of Research and Development at https://www.research.va.gov/resources/policies/human_research.cfm.