RELEASE OF VA DATA TO STATE CANCER REGISTRIES

1. REASON FOR ISSUE: This Veterans Health Administration (VHA) Directive establishes policy for releasing Department of Veterans Affairs (VA) Central Cancer Registry data to State Cancer Registries.

2. SUMMARY OF MAJOR CHANGES: This directive updates policy and procedures for releasing VA Central Cancer Registry Data to State Cancer Registries, and provides an updated Data Use Agreement template for release of that data.

3. RELATED ISSUES: VA Directive 1080, VA Directive 6500, VA Handbook 6500, VHA Handbook 1080.01, and VHA Handbook 1605.1.

4. RESPONSIBLE OFFICE: The Assistant Deputy Under Secretary for Health for the Office of Patient Care Services, Specialty Care Services (10P4E) is responsible for the contents of this Directive. Questions may be referred to the National Program Director of Oncology at 202-461-7120.

5. RESCISSION: VHA Directive 2009-046, dated October 1, 2009, is rescinded.

6. RECERTIFICATION: This VHA Directive is scheduled for recertification on or before the last working day of July 2019.

Carolyn M. Clancy, MD
Interim Under Secretary for Health

DISTRIBUTION: E-mailed to the VHA Publications Distribution List 0728/2019.

RELEASE OF VA DATA TO STATE CANCER REGISTRIES

1. PURPOSE: This Veterans Health Administration (VHA) Directive establishes policy for releasing Department of Veterans Affairs (VA) Central Cancer Registry data to State Cancer Registries. **AUTHORITY:** 38 U.S.C. § 5701(f)(2); 5 U.S.C. § 552a(b)(3); and 45 CFR 164.512(b).

2. BACKGROUND:

a. Reporting of the cancer data from VA medical facilities to the State Cancer Registries is at present neither uniform nor always congruent with VA existing guidelines. The rationale for reporting VA Central Cancer Registry data to the State Cancer Registries is to ensure a complete understanding of the national cancer burden and mortality.

b. Title 38 United States Code (U.S.C.) § 5701(f)(2) allows for the disclosure of VA patient names and addresses to a criminal or civil law enforcement government agency instrumentality charged with the protection of public health or safety pursuant to a written request from the agency that indicates the information is provided for a purpose authorized by law.

c. The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule allows for the disclosure of health information to a public health authority for the purpose of preventing or controlling disease including the conduct of public health surveillance under 45 CFR-164.512(b).

d. The Privacy Act of 1974 provides authority for VHA to disclose Protected Health Information (PHI), excluding 38 U.S.C. § 7332 protected information, to a State Cancer Registry upon written request pursuant to Privacy Act System of Records 24VA10P2, "Patient Medical Records-VA" Routine Use. 10.

e. Some States have released data obtained from VA to researchers or to other State Cancer Registries with patient identifiers (such as name, social security number, date of birth, address, zip code, etc.). VA has determined that VA medical facilities may report VA cancer data to the States but re-disclosure of VA data with patient identifiers by the State to another entity is prohibited under the terms of the required Data Use Agreement.

3. POLICY: It is VHA policy that every VA medical facility and the VA Central Cancer Registry must obtain a Data Use Agreement (DUA) (see Appendix A), in addition to a signed, written request letter from the State on State Agency letterhead in order for VA to release or disclose data to a State Cancer Registry. ***NOTE:*** *The written request may be considered a standing written request letter for ongoing reporting to the State Cancer Registry, if continuous reporting is required. A standing request is valid for 3 years, at which time it must be reissued.*

4. RESPONSIBILITIES: The VA medical facility Director (in the case of release from a VA medical facility) or the VA Central Cancer Registry National Coordinator (in the case of release from the VA Central Cancer Registry) is responsible for ensuring that:

a. Names, addresses, and health information of patients with cancer are not disclosed to a State Public Health Authority, such as a State Cancer Registry, unless an appropriate written request letter is received and a DUA is executed.

b. Written request from the state must be on the state agency's official letterhead, includes:

(1) A citation of the State law that requires health care providers to report names, addresses, and health record data to the State Cancer Registry and the State law that authorizes the State to enforce or compel compliance with the cancer reporting requirement, e.g., power to sanction or issue cease and desist orders;

(2) The purpose of the request and agreement that the State will not allow the VA information to be utilized for any other purpose than that stated in the request;

(3) A statement that the organization, agency, or instrumentality is aware of the penalty provision of 38 U.S.C. § 5701(f); and

(4) The signature of the head of the agency or official designee.

c. Electronic transfer of data is accomplished in a secure manner in accordance with Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program (VA Handbook 6500).

d. The Information Security Officer (ISO) and Privacy Officer reviews all DUAs before they are signed to ensure that they comply with VHA Handbook 1605.1, Privacy and Release of Information and VHA Handbook 1080.01, Data Use Agreements. ***NOTE:*** *VA medical facility staff may seek the assistance of the Regional Counsel, when appropriate, in evaluating the applicable law relative to the statutory authority of the State Cancer Registry to require cancer reporting and to enforce compliance with the reporting requirement.*

e. That a DUA for the Release of Data (see Appendix A) is completed and signed. The DUA must address the:

(1) Use or purpose of the requested VA data;

(2) Safeguards the State intends to employ to protect the VA data in their possession. These safeguards must address HIPAA security rule compliant controls that are implemented to protect the information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction;

(3) State's authorized use and disclosure of the VA data;

(4) Security requirements necessary for transporting or transmitting the VA data to the State in accordance with VA Handbook 6500, Information Security Program;

(5) Procedures for reporting any data breaches to VA; and

(6) State point(s) of contact for all data exchange and security related issues.

f. That a copy of the completed DUA is provided to the VA Central Cancer Registry Director.

5. REFERENCES:

a. VA Directive 6500, Managing Information Security Risk: VA Information Security Program.

b. VA Handbook 6500, Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program.

c. VHA Directive 1080 and Handbook 1080.01, Access to Personally Identifiable Information in Information Technology Systems, and Data Use Agreements.

d. VHA Handbook 1605.1, Privacy and Release of Information.

e. VHA Handbook 1605.02, Minimum Necessary Standard for Protected Health Information.

DATA USE AGREEMENT (DUA) WITH NON-FEDERAL ENTITIES

AGREEMENT FOR DATA EXCHANGE BETWEEN VETERANS HEALTH ADMINISTRATION (VHA), <INSERT FACILITY OR PROGRAM OFFICE NAME> AND <INSERT NON-FEDERAL ENTITY NAME>

Purpose: This Agreement establishes the terms and conditions under which the VHA <INSERT FACILITY/PROGRAM OFFICE NAME> will provide, and <INSERT ENTITY NAME>, its contractors and agents, will use VHA data <PROVIDE DESCRIPTION OF PROJECT INCLUDING TYPE OF DATA AND HOW IT WILL BE USED>.

TERMS OF THE AGREEMENT:

1. This Agreement is by and between <INSERT ENTITY NAME>, its contractors and agents (hereafter the "Requestor") and the VHA <INSERT FACILITY OR PROGRAM OFFICE NAME> (hereafter the "VHA"), a component of the U.S. Department of Veterans Affairs.

2. This Agreement supersedes any and all agreements between the parties with respect to the transfer and use of data for the purpose described in this agreement, and preempts and overrides any instructions, directions, agreements, or other understanding in or pertaining to any other prior communication with respect to the data and activities covered by this Agreement.

3. VHA will retain ownership of the original data and <INSERT ENTITY NAME> will receive a copy. Data transferred under this agreement becomes the property of <INSERT ENTITY NAME>.

4. Upon completion of the project, or at the request of VHA after making an ownership decision, the Requestor will securely return or destroy, at VHA option, all data gathered, created, received or processed.

5. <INSERT NAME OF OFFICIAL AND ENTITY> will be responsible for the observance of all conditions of use and for establishment and maintenance of appropriate administrative, technical and physical security safeguards to prevent unauthorized use and to protect the confidentiality of the data. The Requestor agrees to notify the VHA within fifteen (15) days of any change in the named Requestor.

6. VHA will ensure the secure transfer of the data to <INSERT NAME OF OFFICIAL AND ENTITY>. The method of transfer will be: <INSERT METHOD OF TRANSFER.>

The following named individuals are designated as their agencies' Points of Contact for performance of the terms of the Agreement. All questions of interpretation or compliance with the terms of this Agreement should be referred to the VHA official named below.

VHA's Point-of-Contact on behalf of <INSERT FACILITY/PROGRAM OFFICE NAME>
Name:
Title:
Telephone:

Other Points-of-Contact on behalf of <INSERT FACILITY/PROGRAM OFFICE NAME>
Name:
Title:
Telephone:

Points-of-Contact on behalf of <INSERT NON-FEDERAL ENTITY NAME>
Name:
Title:
Telephone:

7. In the event VHA determines or has a reasonable cause to believe that the Requestor disclosed or may have used or disclosed any part of the data other than as authorized by this Agreement or other written authorization from the person designated in item number 5 of this Agreement, VHA in its sole discretion may require the Requestor to: (a) promptly investigate and report to /VHA the Requestor's determinations regarding any alleged or actual unauthorized use or disclosure, (b) promptly resolve any problems identified by the investigation; (c) if requested by VHA, submit a formal response to an allegation of unauthorized disclosure; and (d) if requested, return VHA's data files to the Data Owner. If VHA reasonably determines or believes that unauthorized disclosures of Data Owner's data in the possession of Requestor have taken place, the VHA may refuse to release further data to the Requestor for a period of time to be determined by VHA, or may terminate this Agreement.

8. Access to the VHA data shall be restricted to authorized <insert Entity name> employees, contractors, agents and officials who require access to perform their official duties in accordance with the uses of the information as authorized in this Agreement. Such personnel shall be advised of: (1) the confidential nature of the information; (2) safeguards required protecting the information; and (3) the administrative, civil and criminal penalties for noncompliance contained in applicable Federal laws. The Requestor agrees to limit access to, disclosure of and use of all data provided under this Agreement. The Requestor agrees that access to the data covered by this Agreement shall be limited to the minimum number of individuals who need the access to the Information Owner's data to perform this Agreement.

9. <INSERT ENTITY NAME>, its contractors or agents, will protect the privacy and confidentiality of any individually identifiable information contained in the data consistent with the Privacy Act of 1974, and, to the extent applicable, standards promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), 38 U.S.C. 5701(f),and other applicable laws, regulations, and policies. The Requestor may provide data access to appropriate employees, contractors, and other authorized Requestors. Except as may be required in a public health emergency to protect life and health of individuals and populations, and for authorized follow-up activities described herein, the Requestor will not attempt to identify the individuals whose records are contained in the data provided under this agreement or link these data with other data sources for identification purposes.

10. The information provided may not be disclosed or used for any purpose other than as outlined in this Agreement. If the Requestor wishes to use the data and information provided by VHA under this Agreement for any purpose other than those outlined in this Agreement, the Requestor shall make a written request to VHA describing the additional purposes for which it seeks to use the data. If VHA determines that the Requestor's request to use the data and information provided hereunder is acceptable, VHA shall provide the Requestor with written approval of the additional use of the data.

11. The Requestor hereby acknowledges that criminal penalties under § 1106(a) of the Social Security Act (42 U.S.C. § 1306(a)) may apply to disclosures of information that are covered by § 1106 and that are not authorized by regulation or by Federal law. The Requestor further acknowledges that criminal penalties under the Privacy Act (5 U.S.C. § 552a(i)(3)) may apply if it is determined that the Requestor, or any individual employed or affiliated therewith, knowingly and willfully discloses VHA's data. Finally, the Requestor acknowledges that criminal penalties may be imposed under 18 U.S.C. § 641 if it is determined that the Requestor, or any individual employed or affiliated therewith, has taken or converted to his own use data file(s), or received the file(s) knowing that they were stolen or converted.

12. Authority for <INSERT PROGRAM OFFICE> to share this data for the purpose indicated is under the HIPAA Privacy Rule, is <INSERT LEGAL CITATION>, under the Privacy Act is <INSERT LEGAL CITATION OR ROUTINE USE FROM THE APPLICABLE PRIVACY ACT SYTEM OF RECORD> and under 38 USC 5701 <INSERT LEGAL CITATION> and 38 USC 7332 <INSERT LEGAL CITATION, IF THIS STATUTE IS APPLICABLE>.

13. <INSERT ENTITY NAME> will ensure that its contractors and agents abide by the terms and conditions of this agreement. The VA or VHA may request verification of compliance.

14. The terms of this Agreement can be changed only by a written modification to the agreement by the agency signatories (or their designated representatives) to this Agreement or by the parties adopting a new agreement in place of this Agreement.

15. This Agreement may be terminated by either party at any time for any reason upon 30 days written notice. Upon such notice, VHA will notify the Requestor to destroy or securely return such data at Requestor's expense using the same procedures stated in the above paragraph of this section.

16. On behalf of both parties the undersigned individuals hereby attest that he or she is authorized to enter into this Agreement and agrees to all the terms specified herein.

_____ _____

INSERT NAME OF ENTITY SIGNER Date
INSERT TITLE OF ENTITY SIGNER
INSERT PROGRAM OFFICE OF ENTITY
INSERT NAME OF ENTITY

_____ _____

INSERT NAME OF VHA SIGNER Date
INSERT TITLE OF VHA SIGNER
INSERT VHA PROGRAM OFFICE
Veterans Health Administration

Concur/Non-Concur:

INSERT NAME OF VHA PROGRAM OFFICE ISO

_____ _____

Signature Date

Concur/Non-Concur:

INSERT NAME OF VHA PROGRAM OFFICE PRIVACY OFFICER

_____ _____

Signature Date