Department of Veterans Affairs **VHA DIRECTIVE 2007-023**
Veterans Health Administration
Washington, DC 20420 **August 15, 2007**

RELEASE OF VA DATA TO STATE CENTRAL CANCER REGISTRIES

1. PURPOSE: This Veterans Health Administration (VHA) Directive provides policy on releasing Department of Veterans Affairs (VA) cancer registry data to the State cancer registries.

2. BACKGROUND

a. Reporting of the cancer data from the VA Medical Centers to the State cancer registries is presently not uniform and inconsistent with VA guidelines. The rationale for reporting VA 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) allows for the disclosure of VA patient names and addresses to a civil or criminal law enforcement government agency or 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 Title 45 Code of Federal regulations (CFR) 164.512(b).

d. The Privacy Act of 1974 allows for the disclosure of health information contained in the medical records to government agencies charged with the protection of public health under Routine Use #10 under the "Patient Medical Records-VA" (24VA19) Privacy Act system of records notice.

e. Some States have released data obtained from VA to researchers or to other State central registries with patient identifiers (such as name, social security number, date of birth, address, zip code, etc.). VA has determined that VHA health care facilities may report VA cancer data to the States, but re-disclosure of VHA data with patient identifiers by the State is not permitted.

3. POLICY: It is VHA policy that every VHA health care facility must obtain a Data Transfer Agreement (DTA) (see Att. A) in addition to a signed, written request from the State in order to release or disclose VA cancer registry data to a State cancer registry.

4. ACTION: The facility Director is responsible for ensuring:

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

THIS VHA DIRECTIVE EXPIRES AUGUST 31, 2012

b. The written request from the State is on the State agency's letterhead stationery, and that it includes:

(1) Citing the State law that requires health care providers to report names, addresses, and medical 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) Indicating the purpose of the request and stating the State will not allow the information to be used for any purpose other than that which is stated in the request.

(3) Stating 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 the designee.

c. Paper forms created for reporting of the data set are shipped using a secure method that allows for tracking of the package, with signature for receipt required, to ensure the chain of trust in data transfers.

d. Electronic transfer of data are submitted in a secure manner.

NOTE: *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 DTA is completed and signed using the DTA Template in Attachment A. The DTA must address the:

(1) Use or purpose of the requested VA cancer data,

(2) Safeguards the State intends to employ to protect the VA cancer data in their possession,

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

(4) Security requirements necessary for transporting or transmitting the VA cancer data to the State in accordance with VA Directive 6504,

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

(6) State point(s)-of-contact for any occurring issues.

5. REFERENCES

a. VHA Handbook 1605.1

b. VA Directive 6504.

6. FOLLOW-UP RESPONBILILITY: The VHA Office of Patient Care Services (11), Medical Surgical Services is responsible for the contents of this Directive. Questions may be referred to (202) 273-8530.

7. RECISSIONS: None. This VHA Directive expires August 31, 2012.

Michael J. Kussman, MD, MS, MACP
Under Secretary for Health

Attachment

DISTRIBUTION: CO: E-mailed 8/22/07
FLD: VISN, MA, DO, OC, OCRO, and 200 – E-mailed 8/22/07

ATTACHMENT A

DATA TRANSFER AGREEMENT

AGREEMENT FOR EXCHANGE BETWEEN VETERANS HEALTH ADMINISTRATION (VHA) , ____(INSERT DEPARTMENT OF VETERANS AFFAIRS (VA) FACILITY OR PROGRAM OFFICE NAME)___ AND ___(INSERT OUTSIDE STATE AGENCY NAME)___

This Agreement establishes the terms and conditions under which the ___(Insert VA Facility Name)___ will provide, and ___(Insert Name of Outside Agency)___ will use the data to ___(Be very specific in why data is being shared, and state the method of transfer and how that will be accomplished)___ . Any other uses will be subject to prior approval by the ___(Insert Name of the VA Facility Director)___ .

TERMS OF THE AGREEMENT

1. This Agreement is by and between the ___(Insert STATE Agency Name)___ and ___(Insert VA Facility Name)___ (VA FACILITY), a component of the United States Department of Veterans Affairs (VA).

2. This data transfer agreement covers the transfer and use of data by the __(Insert STATE Agency Name)___ and ___(Insert VA Facility Name)___, for the project specified in this agreement. This Agreement supersedes any and all previous data.

3. The terms of this Agreement can be changed only by a written modification of 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.

4. The __(Insert STATE Agency Name)___ will be designed as custodians of the VA data for the <STATE AGENCY name> and will be responsible for complying with all conditions of use and for establishment and maintenance of security arrangements as specified in this Agreement to prevent unauthorized use and disclosure of the ___(Insert VA Facility Name)___'s data provided under this agreement. The STATE AGENCY agrees to notify the ___(Insert VA Facility Name)___ within 15 days of any change of custodianship.

a. **Technical Representative for** ___(Insert VA Facility Name)___

Insert Name and Phone Number
Address

b. **Custodian for** __(Insert STATE Agency Name)___

Insert Name and Phone Number
Address

5. The following named individuals are designated as their agencies' Points of Contact for performance of the terms of the Agreement.

a. **Point-of-contact on behalf of** ___(Insert VA Facility Name)___

Insert Name and Phone Number
Address

b. **Point-of-contact on behalf of** __(Insert STATE Agency Name)___

Insert Name and Phone Number
Address

6. Except as VHA shall authorize in writing, the __(Insert STATE Agency Name)___ shall not disclose, release, reveal, show, sell, rent, lease, loan, or otherwise grant access to the VHA data covered by this Agreement to any person outside the __(Insert STATE Agency Name)___. The __(Insert STATE Agency Name)___ agrees that, access to the data covered by this Agreement shall be limited to the minimum number of individuals who need the access to VA data to perform this Agreement.

7. The parties mutually agree that any derivative data or file(s) that is created from the original data may be retained by the __(Insert STATE Agency Name)___ until the project specified in this DTA has been completed. The use of the data will be for the time period covered by the written request (Insert Time Frame).

8. The Agreement may be terminated by either party at any time for any reason upon 30 days written notice. Upon such notice, the VA facility will notify the __(Insert STATE Agency Name)___ to destroy or return such data at Users expense using the same procedures stated in the above paragraph of this section.

9. The __(Insert STATE Agency Name)___ will provide appropriate administrative, technical, and physical safeguards to ensure the confidentiality and security of the VA data and to prevent unauthorized use or access to it. VA sensitive information must not be transmitted by remote access unless VA-approved protection mechanisms are used. All encryption modules used to protect VA data must be validated by NIST to meet the currently applicable version of Federal Information Processing Standards (FIPS) 140 (See http://csrc.nist.gov/cryptval/140-1/1401val.htm for a complete list of validated cryptographic modules).

a. Only approved encryption solutions using validated modules may be used when protecting data during transmission. Additional security controls are required to guard VA sensitive

information stored on computers used outside VA facilities. All VA data must be stored in an encrypted partition on the hard drive and must be encrypted with FIPS 140 validated software.

b. The application must be capable of key recovery and a copy of the encryption key(s) must be stored in multiple secure locations. Further, the __(Insert STATE Agency Name)___ agrees that the data must not be physically moved or transmitted in any way from the site indicated in item number 5 without first being encrypted and obtaining prior written approval from the ___(Insert VA Facility Name)___.

c. If the data __(Insert STATE Agency Name)___ becomes aware of the theft, loss or compromise of any device used to transport, access or store VA information, or of the theft, loss or compromise of any VA data, the __(Insert STATE Agency Name)___ must immediately report the incident to his or her supervisor. That supervisor must within one hour inform the ___(Fill in VA Information Security Officer and the Director names and phone numbers)___. The ISO will promptly determine whether the incident warrants escalation, and comply with the escalation requirements for responding to security incidents.

10. The authorized representatives of VHA and the Inspector General will be granted access to premises where the data are kept by the __(Insert STATE Agency Name)___ for the purpose of confirming that the __(Insert STATE Agency Name)___ is in compliance with the security requirements.

11. No findings, listing, or information derived from the data, with or without identifiers, may be released if such findings, listing, or information contain any combination of data elements that might allow the deduction of a veteran without first obtaining written authorization from the appropriate System Manager or the person designated in item number 18 of this Agreement. Examples of such data elements include, but are not limited to: social security number, geographic indicator, age, sex, diagnosis, procedure, admission and/or discharge date(s), or date of death. The ___(Insert VA Facility Name)___ shall be the sole judge as to whether any finding, listing, information, or any combination of data extracted or derived from its files provided under this Agreement identifies or would, with reasonable effort, permit one to identify an individual or to deduce the identity of an individual. The review of the findings is for the sole purpose of assuring that data confidentiality is maintained and that individuals cannot be identified from the findings. The ___(Insert VA Facility Name)___ agrees to make this determination about approval and to notify the __(Insert STATE Agency Name)___ within 2 weeks after receipt of findings. The ___(Insert VA Facility Name)___ may withhold approval for publication only if it determines that the format in which data are presented may result in identification of individual.

12. The __(Insert STATE Agency Name)___ may not reuse the ___(Insert VA Facility Name)___ original or work file(s) for any other purpose.

13. In the event that the ___(Insert VA Facility Name)___ determines or has a reasonable cause to believe that the __(Insert STATE Agency Name)___ 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 appropriate System Manager or the person designated in item number 17 of this Agreement, the ___(Insert VA Facility Name)___ in its sole discretion may require the __(Insert STATE Agency Name)___ to:

a. Promptly investigate and report to the ___(Insert VA Facility Name)___ the ___(Insert the STATE Agency's determinations regarding any alleged or actual unauthorized use or disclosure)___;

b. Promptly resolve any problems identified by the investigation;

c. If requested by the ___(Insert Name of the VA Facility)___, submit a formal response to an allegation of unauthorized disclosure; and

d. (d) if requested, return the ___(Insert VA Facility Name)___'s data files to the ___(Insert VA Facility Name)___. If the ___(Insert VA Facility Name)___ reasonably determines or believes that unauthorized disclosures of VA's data in the possession of __(Insert STATE Agency Name)___ have taken place, the ___(Insert VA Facility Name)___ may refuse to release further data to the __(Insert STATE Agency Name)___ for a period of time to be determined by the ___(Insert VA Facility Name)___, or may terminate this Agreement.

14. The __(Insert STATE Agency Name)___ acknowledges that criminal penalties under the Privacy Act (5 U.S.C. §552a(i)(1)) may apply if it is determined that the __(Insert STATE Agency Name)___, or any individual employed or affiliated therewith, knowingly and willfully discloses VA's data. Any person found guilty under the Privacy Act shall be guilty of a misdemeanor and fined not more than $5,000. Finally, the __(Insert STATE Agency Name)___ acknowledges that criminal penalties may be imposed under 18 U.S.C. §641 if it is determined that the __(Insert STATE Agency Name)___, 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.

15. All questions of interpretation or compliance with the terms of this Agreement should be referred to the ___(Insert Name of VHA Official's Name in Item 17)___ , or successor.

16. Authority for VHA to share this data for the purpose indicated is under the HIPAA Privacy Rule is 45 CFR 164.512(b), under the Privacy Act is Routine Use #10 under the "Patient Medical Records-VA" (24VA19) Privacy Act system of records notice and under 38 U.S.C. 5701(f), which allows for the disclosure of VA patient names and addresses to a civil or criminal law enforcement government agency or 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.

17. On behalf of both parties the undersigned individuals hereby attest that ___(Insert Name of One Party)___ and ___(Insert Name of Second Party)___ is authorized to enter into this Agreement and agrees to all the terms specified herein.

_____	_____	_____	_____
(VA's Responsible Official Organization Transferring Data)	(Date)	(STATE's Responsible Official Organization Receiving Data)	(Date)

Concur/Non-Concur:

_____	_____
(VA Facility's Information Security Officer Name and Organization)	(Date)