Department of Veterans Affairs

Memorandum

Date: FEB 0 6 2007

From: Deputy Under Secretary for Health Operations and Management (DUSHOM)
Chief Research and Development Officer (CRADO)

Subj: Certification by Principal Investigators: Security Requirements for VA Research Information

To: Network Directors (10N 1-23)
A

1. The Department of Veterans Affairs (VA) is committed to protecting sensitive information including veteran's personal identifiers, and health information. This commitment to guard all VA sensitive information also includes protecting information collected for research purposes. The research may be related to human subjects, research involving laboratory animals or other sensitive research. It is imperative that VA be able to demonstrate this commitment and develop mechanisms that will allow for documentation of the actions taken to safeguard research information.

2. In order to demonstrate this commitment, the following actions are required:

a) By April 1, 2007 the Assistant Chief of Staff for Research and Development (ACOS/R&D) at each VA health care facility that conducts research will convey to all Principal Investigators (PI) with active research studies, the importance of this issue and the necessity of complying with all applicable Federal laws, regulations and policies related to storage and security of research information. To accomplish this, each ACOS/R&D must send this memo and the attached appendixes to all PIs and assist them in completing the check list and certification.

b) By April 15, 2007, all PIs must submit their completed certification form that is applicable for all his/her active protocols, to the ACOS/R&D at their VA health care facility.

c) By May 1, 2007, all ACOS/R&Ds will compile the certifications, ensure all PIs have submitted their certification and then forward a written certification to the Medical Center Director (MCD) that all PIs have meet the requirement in subparagraph 2b of this memo.

d) By May 15, 2007, all MCDs will certify to their VISN Director that all PIs have met the certification requirements related to storage and security of research information. These certifications will be maintained in the VISN Director's files.

e) VISN Directors should notify their VISN Support Team by May 21, 2007 that they have received certifications from each of their facilities that all PIs have met certification.

3. This certification process must be completed annually with the same due dates each year.

4. For all new research protocols the Principal Investigator(s) must certify that the use, storage, and security of all research information collected for, derived from, or used during the conduct of the research will be in compliance with all VA and VHA requirements. This will require completing a “*Data Security Checklist*” and a “*Principal Investigator’s Certification: Storage & Security of VA Research Information)*” for each new protocol. These forms must be stored with the research protocol files. *Note: A new research protocol is defined as a research study that is approved by the Institutional Review Board (IRB) and the Research and Development Committee on or after the date of this memorandum.*

5. The certification for each new protocol will be required for all research proposals submitted to the Office of Research and Development for funding consideration and must be submitted as a “Just-In-Time” document.

6. Attached are a number of Appendices that will assist the PIs and the ACOS/R&D in complying with these requirements. These include:

a) Background Information, Definitions and Requirements

b) Guidance on Completing the Data Security Checklist for Principal Investigators.

c) Data Security Check List for Principal Investigators.

d) Certification of Compliance with Data Security Requirements for Principal Investigators.

e) Policies on Data Storage and Data Security.

7. Any questions concerning this issue may be addressed to your research office or contact Brenda Cuccherini, Ph.D. (Brenda.cuccherini@va.gov) or Joe Francis, M.D. (joe.francis@va.gov) within the Office of Research and Development.

William F. Feeley
William F. Feeley

Joel Kupersmith
Joel Kupersmith, M.D.

Appendix A

Background, Definitions, and Requirements for Protecting VA Research Information

1. **Additional Background**. The ability of investigators to conduct research within the Department of Veterans Affairs (VA) is a privilege that comes with many responsibilities. One of these responsibilities is to ensure the security of all VA research information. In addition, there must be compliance with all applicable Federal laws, regulations, policies, and guidance related to privacy, confidentiality, storage, and security of research data. Research data generated by VA investigators during the conduct of VA-approved research is owned by the VA and its use and storage must meet all Federal standards including, but not limited to Federal Information Security Management Act of 2002 (FISMA), National Institute of Standards and Technology (NIST) standards for computer systems and encryption, the Privacy Act of 1974, and the Health Insurance Portability and Accountability Act (HIPAA). Compliance requires that VA research information may not be stored on non-VA servers, laptops, or portable media unless specific permissions have been obtained from the person's supervisor, the Assistant Chief of Staff (ACOS)/R&D, the Privacy Officer, and the Information Security Officer (ISO) and all other requirements met as defined by VA policy. In addition there are a number of applicable VA and VHA policies to which investigators and research staff must comply. A list of these policies may be found on ORD's website, www.research.va.gov or on VHA's publication website: www.va.gov/vhapublications. A list of the current policies is attached.

2. **Definitions**: A first step in protecting this data is to clearly define research information. It is also necessary to understand that this term includes more than information found in a veteran's medical record. The definitions of these terms are found below.

a. Data: Within this document the term data refers to data collected for, used in, or derived from the conduct of a research project.

b. Preparatory to Research: Within VHA, "preparatory to research" refers to activities that are necessary for the development of a specific protocol. Privacy Health Information (PHI) from data repositories or medical records may be reviewed during this process, but only aggregate data may be recorded and used in the protocol. Within the VA, preparatory to research does NOT involve the identification of potential subjects and recording of data that would be used to recruit these subjects or to link to other data. The preparatory to research activity ends once the protocol has been approved by the Institutional Review Board (IRB) and the Research and Development (R&D) Committee.

c. Removed from the VA: Means that the data's destination is other than sites within a VA facility.

d. Research Information: Information that is a subset of sensitive information that is or has been collected for, used in or derived from the conduct of a research project. This can include individually identifiable information and de-identified information derived from human subjects. It also includes data or information from research involving laboratory animals or other types of sensitive research. .

e. Individually Identifiable Information: Any information, including health, financial information, and employment information, maintained by VHA pertaining to an individual that also identifies the individual by name or other unique identifier. Privacy Act systems of records, medical records, personnel files, and limited data sets are all considered individually identifiable information.

f. De-identified information: Information that does not identify an individual, (or relative, employers, or household members of an individual) as required by VHA Handbook 1605.1 Appendix B and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. It must also meet the Common Rule (38 CFR 16) definition of de-identified. De-identified information may not include any of the 18 direct identifiers stipulated by the HIPAA Privacy Rule, e.g., name; social security number; medical record number; age; address; e-mail address; device identifiers and serial numbers; dates directly related to the individual such as birth date, admission dates, discharge dates; or any other unique identifying number, characteristic, or code. (See 45 CFR 164.514(a), (b) for the complete list of direct identifiers). De-identified information may not include any codes that are in any way derived from or related to these direct identifiers or other information about the individual, e.g., de-identified information may not include portions of social security numbers or scrambled social security numbers.

g. VA Sensitive Information: These terms are defined in VA Directive 6504 as: All Department data on any storage media or in any form or format, which requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, and records about individuals requiring protection under various confidentiality provisions such as the Privacy Act or HIPAA.

3. **Requirements for Protecting Research Information**. The Federal statutes, regulations, and policies (VA and VHA) listed in Appendix E contain a number of requirements. As defined within these statutes, regulations, and policies investigators and other research staff must comply with the following requirements. *Note: This list is not inclusive of all requirements. Please consult the regulations, polices, and guidance documents for all requirements not listed below.*

- VA research data may not be stored outside the VA unless applicable permissions have been obtained from the person's supervisor, the ACOS/R&D, the Privacy Officer, and the ISO. This includes storage on non-VA computer systems/servers, desk top computers located outside the VA, laptops, or other portable media.

- Data transfer to a non-VA computer system/server or site must only occur after the required permissions have been obtained and the transfer must be in compliance with requirements found in VA Directive 6504.

- When VA data is stored on non-VA systems, the system must meet all requirements set forth in FISMA including the required Certification and Accreditation of the system.

- The data residing on non-VA laptops and portable media must be encrypted and password protected with only authorized individuals having access to the data.

- All Research Information residing on laptops, other portable media, or personal computers not within a VA health care facility must be encrypted and password protected. *Note: The original data may not be stored on laptops or portable media and all laptops regardless of their location within or outside the VA must be encrypted if used for any research purposes.*

- Research subjects or veterans names, addresses, and Social Security Numbers (real or scrambled) may only be stored within the VA and on VA servers. If the data is coded, the key to linking the code with these identifiers must also be stored within the VA.

- All protocols that will include the collection, use and/or storage of research information including subject identifiers and PHI that are submitted to an IRB and to a R&D Committee for approval must contain specific information on all sites where the data will be used or stored, how the data will be transmitted or transported, specifically who will have access to the data, and how the data will be secured. If copies of the data will be placed on laptops or portable media a discussion of the security measures for these media must be included.

4. **Explanation of concepts or terms used in this document**:

a. Restriction to access. Access to data should be restricted to those:

(1) Individuals named within the research protocol, on the research informed consent, and the HIPAA-compliant authorization form.

(2) Individuals who are responsible for oversight of the research program.

(3) VA investigators who require access “preparatory to research” if their activity meets requirements set forth in VHA policy.

b. Procedures for reporting loss or theft. The loss or theft of VA research data/information or portable media such as laptops or personal computers (PC)s is covered in VA Directive 6504. In addition, medical facilities should have policies and procedures specific to the facility. The research office will be able to assist you in locating these documents. At a minimum the following should occur as soon as it is discovered that there has been a loss:

(1) Report the loss or theft to security/police officers immediately.

- If you are within a VA health care facility, the VA police must be notified.

- If you are on travel or at another institution, the security/police officers at the institution such as hotel security, university security etc., must be notified as well as the police in the jurisdiction where the event occurred.

- Obtain the case number and the name and badge number of the investigating officer(s). If possible obtain a copy of the case report.

(2) Immediately call or e-mail the following regarding the incident:

- Your supervisor,
- Your facility's VA's privacy officer, and
- Your facility's VA security officer.

(3) Important: Your facility's procedure may include others to notify such as the COS or the MCD. You must determine the name of your facility's privacy officer and ISO so that you will have their name and contact information available.

5. Any questions regarding these issues can be directed to your research office or contact Brenda Cuccherini, Ph.D. ((202)254-0277 or Brenda.cuccherini@va.gov) or Joe Francis, M.D., Deputy CRADO ((202)254-0183 or joe.francis@va.gov) within the Office of Research and Development.

Appendix B

Instructions for Completing the "Data Security Check List for Principal Investigators" and the "Principal Investigator's Certification: Storage and Security of VA Research Information" Template

These instructions will assist all ACOS/R&Ds, Principal Investigators, Medical Center Directors, and VISN Directors fulfill their responsibilities related to the certification process for Principal Investigators related to the storage and security of research data.

1. By April 1, 2007 the Assistant Chief of Staff for Research and Development (ACOS/R&D) at each VA health care facility that conducts research will convey to all Principal Investigators (PI) with active research studies, the importance of these issues and the necessity of complying with all applicable Federal laws, regulations and policies related to storage and security of VA research information. To accomplish this, each ACOS/R&D must send this memo and the attached appendixes to all PIs and assist them in completing the check list and certification.

2. By April 15, 2007, all PIs must submit their completed certification form that is applicable for all his/her active protocols, to the ACOS/R&D at their VA health care facility.

3. By May 1, 2007, all ACOS/R&Ds will compile the certifications, ensure all PIs have submitted their certification and then forward a written certification to the medical centers Director (MCD) that all PIs have completed the required certification related to the storage and security of VA research information.

4. By May 15, 2007, all MCDs will certify to their VISN Director that all PIs have met the certification requirements related to storage and security of VA research information. These certifications will be maintained in the VISN director's files.

5. VISN Directors should notify their VISN Support Team by May 21, 2007 that they have received certifications from each of their facilities that all PIs have met certification.

6. This certification process must be completed annually with the same due dates each year.

7. Any questions concerning this issue may be addressed to your research office or contact Brenda Cuccherini, Ph.D. (Brenda.cuccherini@va.gov) or Joe Francis, M.D. (joe.francis@va.gov) within the Office of Research and Development.

Appendix C
Data Security Checklist for Principal Investigators

Date:
Name of Protocol:
Name of PI:
PI's Phone Number and e-mail address:
Name of Privacy Officer (PO):
PO's Phone & e-mail address
Name of ISO:
ISO's Phone Number and e-mail address
Instructions*: If you answer NO to any one of the statements, you may not remove or transmit the data outside the VA and you must consult with your supervisor, ISO and Privacy Officer. If the research will not obtain any VA sensitive information/data the statements below should be marked as not applicable (N/A).*

Yes	No	N/A	Specific Requirement
			All VA sensitive research information is used and stored within the VA
			All copies of VA sensitive research information are used and remain within the VA

If you have answered yes or N/A to both statements above, stop here.

If the original or copies of VA research information are removed from the VA the following apply: *See Appendix A for definition of terms used in this document.*

Yes	No	N/A	Specific Requirements
			Permission to remove the data has been obtained from 1) your immediate supervisor, 2) your ACOS/R&D, 3) the VA Information Security Officer (ISO), and 4) the VA Privacy Officer.
			A property pass for the equipment (Laptop etc.) has been obtained.
			The laptop or other portable media is encrypted and password protected. ***Note****: Contact the VA ISO at your facility for encryption issues*.
			Data are not transmitted as an attachment to unprotected e-mail messages.
			Names, addresses, and Social Security Numbers (real and scrambled) have been replaced with a code. ***Note****: Names, addresses, and Social Security Numbers (real or scrambled) may only be maintained on a VA server and documentation of the procedure by which the data were coded must remain within the VA*
			Data sent via mail or delivery service have been encrypted. ***Note****: It is preferable to send data on CDs or other media by a delivery service where there is a "chain of custody".*
			For data that will reside on a non-VA server: The server has be certified and accredited as required by Federal Information and Security Management Act of 2002 (FISMA). ***Not****e: your facilities ISO should be consulted.*
			Access to the data is only by those who are authorized to access it and the access is related to VA-approved research.
			Procedures for reporting theft or loss of sensitive data or the media such as a laptop, containing sensitive data are in place and familiar to the researcher and all others who have access to, use, store, or transport the data.

Appendix D

Principal Investigator's Certification: Storage & Security of VA Research Information

Instructions:

1. This certification must be completed by all Principal Investigators (PI) and submitted to their facility's ACOS/R&D no later then April 15, 2007. It must also be completed and submitted to the ACOS/R&D by April 15th annually there after. If you are PI on more then one research protocol, you may a) complete a form for each protocol, b) list additional protocols and date of R&D approval on the bottom of this form, or c) attach a separate list.

2. This form must be completed for each new protocol and a copy of this form must remain with the research protocol file.

3. This form must be submitted to ORD during the Just-In-Time process if you will be funded by ORD for a research project.

I certify to the best of my knowledge that all VA sensitive information associated with the research study entitled ____and approved by the Research and Development Committee on ___________ is being used, stored and security in accordance with the applicable VA and VHA policies and guidance.

Name: ____________________________

Title: _____________________________

Date: _____________________________

Phone: ____________________________

E-mail: ____________________________

Appendix E

ORD Cyber Security and Privacy

The Office of Research and Development is dedicated to upholding the standards of cyber security and privacy as established by VA. It is also the responsibility of all VA researchers and staff to be familiar with and to comply with existing policies, procedures and directives regarding the protection of human subjects in research and the use and disclosure of individually-identifiable information.

Memos from the Chief R&D Officer

- Research Responsibilities for Protecting Sensitive Information: Memo from William Feeley, Deputy Under Secretary for Health for Operations & Management, and Dr. Joel Kupersmith, Chief Research and Development Officer (June 12, 2006)
- Cyber Security and Privacy: Memo from Dr. Michael J. Kussman, Principal Deputy Under Secretary for Health, and Dr. Joel Kupersmith, Chief Research and Development Officer (June 27, 2006)
- Researcher Contacts with Veterans: Memo from Dr. Michael J. Kussman, Principal Deputy Under Secretary for Health, and Dr. Joel Kupersmith, Chief Research and Development Officer (July 10, 2006)

VA Cyber Security and Privacy Policies

- VHA Handbook 1200.5 - Requirements for the Protection of Human Subjects in Research
- VHA Handbook 1605.1 - Privacy and Release of Information
- VA Handbook 5011/5 - Human Resource Management policy regarding flexible work arrangements (telework)
- VA Directive and Handbook 6102 - regarding internet and intranet services
- VA IT Directive 06-2 - Safeguarding Confidential and Privacy Act-Protected Data at Alternative Work Locations
- VA IT Directive 06-5 – Use of Personal Computing Equipment
- VA IT Directive 06-6 – Safeguarding Removable Media
- VHA Directive 6210 - regarding automated information systems security
- VA Directive 6212 - Security of External Electronic Connections VA Directive 6500 – on the VA Information Security Program
- VA Directive 6500 – on the VA Information Security Program
- VA Directive 6502, Handbook 6502.1 and Handbook 6502.2 - regarding the privacy program, One VA Privacy Violation Tracking System (PVTS), and Privacy Impact Assessment (PIA)
- VA Directive 6504 - restrictions on transmission, transportation and use of, and access to, VA data outside VA facilities
- VHA Directive 2004-002 - regarding commercial or external web hosting services
- 45 CFR Parts 160 and 164 Health Insurance Portability and Accountability Act (HIPAA)