Department of
Veterans Affairs

Memorandum

Date: May 29, 2008

From: Chief Officer, Office of Research Oversight (ORO)(10R)

To: ALL ORO Staff

COMPLIANCE OVERSIGHT PROCEDURES FOR USE AND STORAGE OF VA SENSITIVE RESEARCH INFORMATION

The Office of Research Oversight (ORO) has adopted the following procedures for its oversight of compliance with Department of Veterans Affairs (VA) requirements for the use and storage of electronic and hard-copy research information.

A. Electronic storage and use of VA sensitive research information, including identifiable private information and protected health information on university affiliate servers.

1. VA Handbook 6500 Sections 6.a.(1)(b)1 and 6.a.(1)(b)2 require that the Information Security Officer (ISO) work with the VA facility to identify and mitigate risks to the confidentiality, integrity, and availability of VA sensitive information; present identified risks to the facility Director and the Chief Information Officer (CIO); and maintain on file the decisions of the facility Director and the CIO regarding mitigation of risks.

2. Sections 6.a.(13)(a) and 6.a.(13)(b) require that physical and wireless connections to or from information systems outside VA be documented through a Memorandum of Understanding (MOU) and a System Interconnection Agreement (SIA) specifying the conditions of sharing and the applicable technical and security requirements. The MOU and SIA must be approved by Office of Information and Technology (OI&T) management and the ISO.

3. Section 6.c.(4)(c) requires written permission from the relevant VA supervisor and the ISO before sensitive information can be removed from the VA facility.

4. Section 6.c.(4)(d) requires that VA sensitive information reside in a protected VA environment at all times, or it must be encrypted. OI&T must approve the protective conditions being employed.

5. Section 6.c.(4)(j) specifies that VA sensitive information may not reside on non-VA owned Other Equipment (OE) without specific designation and approval in advance by the relevant VA supervisor and a waiver from the VA CIO.

6. Section 6.c.(4)(o) requires that all devices used to transmit and store VA information outside VA's protected environment use Federal Information Processing Standards (FIPS) 140-2 approved encryption.

B. ORO OVERSIGHT

1. Per A1 and A2 above: Where VA sensitive research information resides on an affiliate information system that is interconnected with the VA information system, ORO will verify the existence of an MOU and an SIA documenting the arrangement and approved by OI&T management and the ISO. In the absence of such documentation, ORO will require a written

statement from the ISO and the facility Director as to why the existing arrangement is acceptable. Where in doubt about acceptability, ORO Central Office will refer the matter to OI&T Central Office for review.

2. Per A3, A4, A5, and A6 above: For any arrangement under which VA sensitive research information is not held in a protected VA computing environment (for example on affiliate servers not interconnected with VA systems), ORO will verify the existence of written permission from the relevant VA supervisor and the ISO and a waiver from the VA CIO. In the absence of such documentation, ORO will require a written statement from the ISO and the facility Director as to why the existing arrangement is acceptable. Where in doubt about acceptability, ORO Central Office will refer the matter to OI&T Central Office for review.

C. Electronic storage and use of VA sensitive research information, including identifiable private information and protected health information, on desktop computers or external hard drives inside or outside VA.

1. VA Handbook 6500 §6.c.(4)(d) requires that VA sensitive information be in a protected VA computing environment at all times, or it must be encrypted. OI&T must approve the protective conditions being employed.

2. Section 6.c.(4)(o) requires that all devices used to transmit and store VA information outside VA's protected environment use FIPS 140-2 approved encryption.

3. As of the date of this memorandum, OI&T had not approved an encryption product for use with VA desktop computers (local drives) and external hard drives.

D. ORO OVERSIGHT:

1. Per C1, C2, and C3 above: Until an encryption solution is approved and deployed by OI&T, ORO will verify that VA sensitive research information is not stored on desktop computers or external hard drives, regardless of location inside or outside VA. In such cases, ORO will require a written statement from the ISO and the facility Director as to why the existing arrangement is acceptable. Where in doubt about the acceptability of a practice, ORO Central Office will refer the matter to OI&T Central Office for review.

E. Hard copy (paper) storage and use of VA sensitive research information, including identifiable private information and protected health information, inside or outside VA (e.g., in investigators' offices or laboratories located within a VHA facility or on university affiliate property).

1. VA Handbook 6500 Section 6.b.(4)(b)14.f requires that employees follow "clear desk" practices to protect VA sensitive information (in any form) in uncontrolled environments.

2. Sections 6.b.(4)(b)14.k and 6.b.(4)(b)16.b require that VA sensitive information on printouts and other media be kept in locked files or cabinets when not in use.

3. Section 6.c.(3)(c) requires written authorization from the relevant VA supervisor to transport, transmit, access, or use VA sensitive information outside VA facilities.

4. Section 6.c.(4)(c) requires written permission from the relevant VA supervisor and the ISO before VA sensitive information can be removed from the VA facility.

F. ORO OVERSIGHT:

1. Per E1 and E2 above: Regardless of location inside or outside a VA facility, ORO will verify that hard copies of VA sensitive research information are kept in locked files or cabinets when not in use. Where in doubt about the acceptability of a practice, ORO Central Office will refer the matter to OI&T Central Office for review.

2. Per E3 and E4 above: ORO will verify documentation of approval by the relevant VA supervisor and the ISO of any arrangement under which hard copies of VA sensitive research information are transported or used outside a VA facility. Where in doubt about the acceptability of an arrangement, ORO Central Office will refer the matter to OI&T Central Office for review.

G. ADDITIONAL CONSIDERATIONS:

1. VHA Directive 2007-040 requires that the facility Privacy Officer and ISO review all human research projects as nonvoting members of the Institutional Review Board (IRB) or Research and Development Committee (R&DC). ORO will verify that such review has taken place.

2. ORO strongly recommends that the R&DC seek Privacy Officer and ISO review of non-human research projects that involve the possible or potential use of VA sensitive Information, i.e., individually identifiable private information, proprietary information, or other information whose improper use or disclosure could adversely affect VA's mission.

3. Research data that do not include individually identifiable private information, proprietary information, or other information whose improper use or disclosure could adversely affect VA's mission do not constitute VA sensitive Information. The Privacy Officer and ISO are not required to review non-human research projects that do not involve the possible or potential use of VA sensitive Information.

4. ORO recommends that VHA facilities review any MOUs and SIAs documenting research information security arrangements annually to ensure that they are current and accurate.

5. These ORO procedures do not apply to use or disclosure of information in accordance with legally effective informed consent and properly executed HIPAA authorization.

6. The Office of General Counsel, OI&T, and/or the VHA Privacy Office may issue specific policy regarding access to research subject data by sponsor monitors. ORO will conduct oversight of that policy when issued.

J. Thomas Puglisi, PhD

Attachment: Selected Terms and Definitions

Selected Terms and Definitions
From VA Handbook 6500, Appendix A

Compensating Security Controls - The management, operational, and technical controls (i.e., safeguards or countermeasures) employed by an organization in lieu of the recommended controls in the low, moderate, or high baselines described in NIST SP 800-53, that provide equivalent or comparable protection for an information system.

Memorandum of Understanding (MOA) / Memorandum of Agreement (MOA) - A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission. In this guide, an MOU/A defines the responsibilities of two or more organizations in establishing, operating, and securing a system interconnection.

Other Equipment (OE) - Non-VA owned equipment, including employees' personal equipment, commercial equipment (such as hotel and internet café equipment), and equipment owned by other agencies.

Storage Media – Any device or hard copy method for the retention of applications and data so that they are available for use. Storage media include: paper, hard drives, removable drives (such as Zip disks), CD-ROM or CD-R discs, DVDs, flash memory, USB drives, and floppy drives.

System Interconnection - The direct connection of two or more IT systems for the purpose of sharing data and other information resources

System Interconnection Agreement (SIA) / Interconnection Security Agreement (ISA) - An agreement established between the organizations that own and operate connected IT systems to document the technical requirements of the interconnection. The ISA also supports a Memorandum of Understanding or Agreement between the organizations.

VA Data / VA Information – Information owned or in the possession of VA or any entity acting for or on the behalf of VA.

VA Sensitive Information / VA Sensitive Data – 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, records about individuals requiring protection under various confidentiality provisions such as the Privacy Act and the HIPAA Privacy Rule, and information that can be withheld under the Freedom of Information Act. Examples of VA sensitive information include the following: individually-identifiable medical, benefits, and personnel information; financial, budgetary, research, quality assurance, confidential commercial, critical infrastructure, investigatory, and law enforcement information; information that is confidential and privileged in litigation such as information protected by the deliberative process privilege, attorney work-product privilege, and the attorney-client privilege; and other information which, if released, could result in violation of law or harm or unfairness to any individual or group, or could adversely affect the national interest or the conduct of federal programs.