

New ORO Guideline for Enforcement of VA Handbook 6500 §6.c(4)(j)
Regarding VA Sensitive Research Information on Non-VA “Other Equipment”

January 31, 2012

1. **VA Handbook 6500** (Information Security Program Handbook) (September 18, 2007) **§6.c(4)(j)** currently requires that: “VA sensitive information may not reside on other non-VA owned Other Equipment (OE) unless specifically designated and approved in advance by the appropriate VA official (supervisor), and a waiver has been issued by the VA’s CIO.”
2. The Deputy Assistant Secretary (DAS) for Information Security, acting on behalf of the VA Assistant Secretary for Information and Technology (VA’s CIO), reviews waiver requests and makes the decision to approve or disapprove the prospective storage of VA sensitive information (VASI) on OE. *See* Office of Cyber Security (OCS) “VA 6500 Waiver Clarification/Update” (August 2011) [“OCS Clarification”]. The process for applying for a VA CIO waiver is located at: https://vaww.infoprotection.va.gov/ca/VA_6500_Waiver.aspx
3. According to VA Handbook 6500 §6.c.(4)(j), VASI – such as protected health information (PHI) used in VA research – may not reside on OE (e.g., affiliate servers; non-VA computers), unless a VA CIO waiver has been issued. The OCS Clarification (p.7), however, describes two alternate methods of documentation that may substitute for the VA CIO waiver: (1) *If* there is a system interconnection between a site/university and VA, and there is a Memorandum of Understanding/Interconnection Security Agreement (MOU/ISA) approved by the Enterprise Security Change Control Board (ESCCB) in place; or (2) If a contract is in place with a vendor and the security controls are appropriately addressed in the contract (*see* VA Handbook 6500.6). If either of these two situations applies, the VA CIO waiver would not be required for the VASI to reside on OE.
4. Based on current VA Handbook 6500 policy, the Office of Research Oversight (ORO) has been reviewing compliance with §6.c(4)(j) as part of its Research Information Protection Program (RIPP) reviews of VA research programs, and requiring remediation where noncompliance has been found. Several factors suggest a different compliance approach.
5. To date, the (former) DAS for Information Security has approved only one waiver for VASI to reside on OE. Moreover, §6.c(4)(j) requires the VA CIO waiver to be issued *prior to* VASI being placed on OE. In other words, there is no VA Handbook 6500 provision for the DAS for Information Security to grant *retroactive* waivers for VASI currently residing on OE that ORO might identify during a RIPP review.
6. A revision of VA Handbook 6500 is currently in draft form. The current draft indicates that a VA CIO waiver will no longer be required for VASI to reside on OE. Instead, VASI will be allowed to reside on OE with an approved *local* facility

agreement in place (e.g., MOU, contract, data use agreement) which outlines all of the required and agreed upon security/privacy requirements. The local facility individuals signing the agreement must ensure that the appropriate security/privacy requirements are included in the agreement and accept the risk of the VASI on OE. These agreements must be reviewed by the facility Information Security Officer and Privacy Officer to ensure that VA requirements are being met. *Note that this is not yet current policy.*

7. Because of the preceding factors, ORO will cease making findings of noncompliance related to VA Handbook 6500 §6.c(4)(j). However, prior to issuance of the revised VA Handbook 6500, if ORO encounters VASI on OE during one of its RIPP site reviews, and there is no VA CIO waiver or other applicable exception, ORO may document its Observation in the RIPP report. The facility is then responsible for deciding, without ORO's endorsement, *whether and how* to address the situation. For example, the facility may: attempt to obtain a VA CIO waiver per current policy; meet one of the waiver exceptions set forth in the OCS Clarification; de-identify the data on the OE; remove the VASI from the OE; transfer ownership of a *copy* of the VA data to the OE site; arrange for donation of the OE to VA; or establish a local agreement for storage of the VASI on OE with appropriate security/privacy requirements in place.

[Note that ORO will continue to enforce regulations and policy requirements for the *disclosure* of PHI to non-VHA entities, e.g., VHA Handbook 1605.1].

8. This Guideline pertains solely to ORO's enforcement of VA Handbook 6500 §6.c(4)(j) as it pertains to VA sensitive research information. It does not prevent any other relevant office within VA from enforcing the §6.c(4)(j) requirement according to the standard operating procedures of that office.
9. This Guideline automatically expires upon issuance of a revised VA Handbook 6500 (superseding the September 18, 2007, version).