Department of Veterans Affairs

Memorandum

Date: DEC 12 2008

From: Assistant Secretary for Information & Technology (005)

Subj: Follow-up Response to Clinical Trial Monitor Access (WebCIMS #419925)

To: Under Secretary for Veterans Health Administration (10)

1. In response to your memorandum, Clinical Trial Monitor Access (WebCIMS #397373), the Office of Information & Technology (OI&T) concurs with the suggested methods outlined below, of providing clinical trial monitors with access to pertinent medical records of Department of Veterans Affairs (VA) study subjects. There is an exception to "option a" as noted below.

a. Limited Read-Only Access to Selected Data –

A clinical patient group involving only study subjects who have consented to participate in the clinical trial can be established within the Computerized Patient Record System (CPRS). Permissions can be set to allow only authorized individuals (including clinical trial monitors) to have read-only access to these patients' records. For multi-site clinical trials involving a VA principal investigator (e.g., VA, NIH, or industry sponsored study), read-only access of a clinical patient group may allow better consistency in central monitoring.

Under this option, monitors would be required to take the VA Cyber Security Awareness Training and sign the National Rules of Behavior. This training is available via the internet and can be accessed through the VA Learning Management System (LMS) at https://www.lms.va.gov/plateau/user/login.jsp. The course generally takes one hour to complete, and must be taken annually. This training is applicable to multiple studies reviewed by the same monitor.

b. VA Employee Driver –

This method has been successfully employed by VA Medical Centers (VAMC) in oversight visits of the Joint Commission on Accreditation of Healthcare Organizations (JCAHO). A VA employee "driver" accesses the system with the monitor watching and shows the monitor only the information that the monitor needs and is authorized to see for the specific trial.

c. Stand-alone Download –

Before any visit, the monitors would provide the VAMC with a list of particular data they desire to review on that visit. The VAMC would download that data in advance, to a computer not connected to any VA system. The study monitor would be provided with access to that computer at the VAMC. The computer would be cleansed of the data after the monitoring visit. If a laptop is used to download these data, the laptop must be encrypted. Usually, this method would require a document signed by the VA employee who downloaded the data certifying that the information on the stand-alone computer were taken from and matches the data in the relevant VA system.

- In a variation, which would not require the monitor to provide a list of desired information in advance, the monitor would be given access to a stand-alone computer to which all study data have been downloaded. A VA certification to verify that the data are true would still be required. If a laptop is used to download this data, the laptop must be encrypted.

- In a more streamlined variation of this method, the VA facility would purchase a laptop computer to be dedicated for this purpose. The monitor would be present and witness the downloading of the requested data to the laptop computer, and subsequently be given access. No VA certification would be required and the laptop would be cleansed of the data after the monitoring visit.

2. These suggested methods are in compliance with VA Information Security Program, Directive and Handbook 6500 and Directive 0710. OI&T understands that because full access to the medical records system is not required or being sought, and the patient has authorized the access that will be provided, the methods outlined above reduce the risk of a data breach. We also agree that if full access to VA data systems is required, background investigations and training will be necessary.

3. We concur that appropriate staff from OI&T and VHA should work together to develop detailed guidance to implement the suggested methods. Jaren Doherty, Associate Deputy Assistant Secretary, Office of Cyber Security, will take the lead on behalf of OI&T. Mr. Doherty can be reached at 202-461-6426.

Robert T. Howard