

South Florida VA Foundation for
Research & Education
Miami, Florida

SFVAFRE MEMORANDUM
No.....005

February 1, 2011

COMPUTER AND PORTABLE ELECTRONIC MEDIA USAGE AND RESTRICTIONS

I. PURPOSE.

To establish the procedures and restrictions for acquiring and loaning South Florida VA Foundation for Research and Education (SFVAFRE) owned computer equipment.

II. POLICY:

The SFVAFRE will purchase and distribute owned portable electronic media devices to approved users and ensure that the devices are used in a manner consistent with SFVAFRE and VA policies and directives regarding the proper use of VA information and equipment.

III. DEFINITIONS:

A. Laptop – A laptop is a portable computer small and light enough to be carried by a typical user and also comes with the ability to operate on battery power. All laptops contain an LCD screen that is not separate from the rest of the unit.

B. Desktop – A desktop computer is a personal computer (PC) in a form intended for regular use at a single location, as opposed to a mobile laptop or portable computer.

C. Portable Electronic Media Device – Electronic devices that can store, transmit, or transfer electronic data and information.

D. Sensitive Information – VA sensitive information is 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 Health Insurance Portability and Accountability Act (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.

E. USB Flash Drive – A USB Flash Drive is essentially NAND-type flash memory integrated with a USB 1.1 or 2.0 interface used as a small, lightweight, removable data storage device. This hot swappable, non-volatile, solid-state device is usually compatible with systems that support the USB version that the drive uses.

IV. RESPONSIBILITIES:

A. The Executive Director, SFVAFRE is responsible for ensuring that any portable electronic media equipment is being used by the appropriate personnel and that the equipment is used in a manner consistent with VA policies and directives.

B. The Information Security Officer (ISO) is responsible for enforcing all policies and procedures while ensuring proper safeguards exist pertaining to the transportation and use of VA sensitive information and VA IT equipment.

B. The Chief of Information Resources Management is responsible for assuring hospital-wide adherence to current VA portable electronic media policies, directives and standards.

C. The Information Resources Management Department (IRM) is responsible for issuing and tracking the portable electronic media.

E. SFVAFRE Employees – Employees who transport and use documents and data on SFVAFRE -issued portable electronic media devices are responsible for requesting and obtaining supervisor and ISO approval for such usage; reading and following the IRM security policies; taking appropriate measures to protect information and equipment; using extreme caution when accessing VA information in open areas or areas where non-authorized persons may see VA information such as airport lounges or hotel lobbies; protecting VA equipment from loss or theft at all times; and immediately reporting any loss of the flash drive to IRM.

V. PROCEDURES:

A. SFVAFRE employees will have an active Work without Compensation (WOC) appointment through Research and Development Service at the Miami VA Healthcare System. SFVAFRE employees are either eligible for short term or long term loans depending upon the reason for the equipment usage and the risk to patient information.

B. VA or SFVAFRE Principal Investigators (PI) who both have active or inactive non-sponsored research projects and maintain an active VA appointment with Research and Development service the Miami VA Healthcare are eligible to request for short term and long

term loans depending upon the reason for the equipment usage and the risk to patient information.

1. Long-term loans of IT equipment must meet the following criteria:
 - a. Executive Director or Approved Special Programs
 - b. Funded Research Project
 - c. IT Specialist in support of SFVAFRE/and VA Research Initiatives
2. Determination of the length of the loan will be assessed based on the following criteria:
 - a. The impact on VA or SFVAFRE data if the loss, theft or damage to IT equipment results in:
 - 1) Data loss of Personal Health Information
 - 2) No patient data – low impact
 - b. IT equipment encryption requirements may influence allowable loan period:
 - 1) Frequent returns needed due to application and use
 - 2) Infrequent returns needed due to application and use
 - 3) Short-term loan required
3. If the application for IT equipment does not meet the necessary criteria and/or if there is insufficient justification of need, SFVAFRE may disapprove of the IT equipment loan.

B. SFVAFRE employees requesting VA Flash drives will submit requests through the Research and Development Service ADPAC.

1. SFVAFRE employees must complete Attachment A, "Request for Issuance of USB Flash Drive" in addition to a footprint with an attached email from the corresponding executive granting approval prior to issue.
 - a. The SFVAFRE employee must be signed by the Administrative Officer, Research and Development or immediate supervisor and by the Information Security Officer.
 - b. The justification needs to include:

- 1) The types of data that will be transported on the flash drive
 - 2) Where the data or documents are being transported to
 - 3) Who the intended audience is for the data or documents
 - 4) The period of time for which the flash drive will be needed
2. If the requested flash drives are to be used to transport sensitive data, as defined by Attachment A, then the applicant must complete Attachment B, "Authorization to transport and utilize VA sensitive information outside protected environments."
 3. The form must be signed by the MVAHS Director or a designee, the Information Security Officer, and the facility's Chief Information Officer.
 4. USB flash drives will be distributed by Information Resources Management.

C. Laptops can be issued by the SFVAFRE – Inventory Control Specialist on a long-term or short-term basis, depending on the loan criteria. An email from the requestor with approval from the corresponding executive (PI) if needed must be attached to the IRMS Footprints request prior to issue.

1. A long-term loan is defined as one year.
2. A short-term loan can be for any time frame less than 90 days.
3. Upon completion of the loan period, the laptop must either be returned to SFVAFRE or a request for extension submitted.
4. Long-term Loan Criteria:
 - a. Laptops are issued on a long-term basis to PI(s) and research staff involved with research project and who performs direct VA patient care during normal business hours at locations other than their assigned designation. For example, the non-sponsored clinical trials, VA Cooperative Study Projects, Clinical Science Research and Development Merit Reviews.
 - b. Special projects/programs involving direct patient care will be evaluated on a case-by-case basis for long-term loans.
 - c. Laptops are not issued on a long-term basis strictly for telecommuting purposes.
5. Long-term Application Process:

- a. If the individual feels their circumstance meets these criteria, they must make the request with the justification of how their request fulfills the necessary criteria directly to the Executive Director, SFVAFRE.
6. Short-term loans of laptops can be used for travel, training purposes and presentations. The laptops are available on a first come, first serve basis.
7. The justification for the laptop must contain the following information:
 - a. The types of data that will be transported on the laptop
 - b. Where the data or documents are being transported
 - c. Who the intended audience is for the data or documents
 - d. The period of time for which the laptop will be needed
8. If the laptop user intends to access or transport VA sensitive information on the laptop, the user must complete Attachment B, "Authorization to transport and utilize VA sensitive information outside protected environments."
9. VA sensitive information is not to be stored on the laptop for longer than the user is going to use it. If the VA sensitive information is accessed regularly by the user, it should be stored on the VPN network.
10. All laptops must be kept current with operating system patches and virus protection updates. SFVAFRE recalls all laptops on a regular basis to perform maintenance and install updates, operating system patches, and virus protection. If an individual is issued either a long-term or short-term laptop, the individual is required to return said laptop immediately upon request.
11. The employee is responsible for returning the laptop in the same condition it was issued: no additional software, hardware and no damage.

VI. OTHER:

None

VII. REFERENCES:

VA Handbook 6500, Information Security Program Handbook

MCPM-IRMS-05-09, Computer and Portable Electronic Media Usage and Restrictions

VIII. RESCISSION:

None

IX. FOLLOW-UP RESPONSIBILITY:

Executive Director, SFVAFRE

X. This Policy Memorandum will remain in effect until December 31, 2011.



Luis Gonzalez, MHA
Executive Director, SFVAFRE

Attachments: 2

MIAMI VA HEALTHCARE SYSTEM
MIAMI, FLORIDA

MEDICAL CENTER POLICY MEMORANDUM
NO.....IRMS-05-09
ATTACHMENT A

July 8, 2009

**Department of
Veterans Affairs**

Memorandum

Date: <date signed>

From: <Requestor's Title>

Subj: Request for Issuance of USB Flash Drive

To: Field Information Security Officer

Thru: <Requestor's Immediate Supervisor>

1. In order to accomplish my duties, I request a USB Flash Drive to store, transport and utilize VA information. My personal information follows:
<Requestor's Full Name>
<Title>
<Home Address>
<City, State, Zip>
<Home Phone number>
2. Justification for the use of this item (include what type of information will be most commonly stored on the drive):
3. I require the following:
 - 1 Gigabyte capacity – no further justification necessary
 - 2 Gigabyte capacity – please justify this requirement below

4. I acknowledge that if I plan to store, transport and utilize VA sensitive information outside a protected environment (as determined by OI&T staff), I must obtain approval from my local Director or his/her designee.

<requestor signature>

Required Concurrence and Approval

Approved / Disapprove

<first name last name>

Date

Immediate Supervisor

Concur / Do Not Concur

Carl Lindsey
Information Security Officer

Date

MIAMI VA HEALTHCARE SYSTEM
MIAMI, FLORIDA

MEDICAL CENTER POLICY MEMORANDUM
NO.....IRMS-05-09
ATTACHMENT B

July 8, 2009

Department of
Veterans Affairs

Memorandum

Date: <date signed>

From: <Requestor's Title>

Subj: Authorization to transport and utilize VA sensitive information outside protected environments

To: Field Information Security Officer

Thru: <Requestor's Service/Department Chief>

1. In order to accomplish my duties, I require the capability to store, transport and utilize VA sensitive information outside protected environments, as defined by VA Directive 6504. VA information refers to all information, either electronic or paper-based. My personal information follows:

<Requestor's Full Name>

<Title>

<Home Address>

<City, State, Zip>

<Home Phone number>

2. Justification for the removal of VA sensitive information outside of protected environments (include where and how information will be used):

3. The sensitive information, as defined in VA Directive 6504, I intend to store, transport and utilize includes (check all that apply):

- Individually identifiable medical, benefits or personnel information
- Information that can be withheld under the Freedom of Information Act
- Financial information
- Research information
- Investigatory information
- Commercial information
- Quality assurance information

- Law enforcement information
- Information that is confidential or privileged in litigation
- Information that could adversely affect the national interest or conduct of federal programs

4. The timeframe I will store, transport and utilize VA sensitive information outside protected environments is:

- 30 days
- 180 days
- One Year

5. I acknowledge that the above statements are accurate and are in compliance with VA Directives 6601 and 6504, Removable Storage Media and Restrictions on Transmission, Transportation and Use of, and Access to, VA information outside protected environments.

6. I acknowledge this document requires renewal upon expiration of the approval timeframe requested above.

<requestor signature/Title> Date

Required Concurrence and Approval
Approved / Disapprove

<Requestor's Service/Dept. Chief> Date

Concur / Do Not Concur

Date

Information Security Officer

Concur / Do Not Concur

Date

Facility Privacy Officer