DEPARTMENT OF THE NAVY
BUREAU OF MEDICINE AND SURGERY
2300 E STREET NW
WASHINGTON DC 20372-5300

IN REPLY REFER TO
BUMEDINST 5239.2
BUMED-M09B6
8 Nov 2007

BUMED INSTRUCTION 5239.2

From: Chief, Bureau of Medicine and Surgery

Subj: PROTECTION OF SENSITIVE, PROTECTED HEALTH INFORMATION (PHI), AND PERSONALLY IDENTIFIABLE INFORMATION (PII) DATA AT REST (DAR) ON MOBILE COMPUTING AND PORTABLE STORAGE DEVICES

Ref: (a) DOD Directive 8100.2 of 14 Apr 2004
(b) DODI 8500.2 of 6 Feb 2003
(c) DOD Memorandum, Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DOD) Global Information Grid (GIG), 2 Jun 2006
(d) DOD Instruction 5200.40 of 30 Dec 1997
(e) DOD 6025.18-R of 24 Jan 2004
(f) DOD 5220.22-M of 28 Feb 2006
(g) SECNAVINST 5239.3A
(h) DOD 8580.02-R of 12 Jul 2007
(i) OMB Memorandum M-01-05, Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy, Dec 20, 2000
(j) OMB Memorandum M-06-20, FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management, July 17, 2006
(k) COMNAVNETWARCOM NORFOLK VA 061635Z Oct 2006 (NOTAL)
(l) OPNAVINST 2100.2
(m)DON CIO WASHINGTON DC 301540Z Nov 2006 (NOTAL)
(n) DON CIO WASHINGTON DC 171952Z Apr 2007 (NOTAL)
(o) SECNAVINST 5211.5E
(p) SECNAV M-5214.1 of December 2005

1. Purpose

a. To establish Navy Medicine policy to protect PHI and PII DAR on mobile computing and portable storage devices consistent with references (a) through (o).

b. To specify the encryption, certification and accreditation parameters to ensure security of the Navy Medicine DAR environment, including mobile devices.

c. To assign responsibilities within Navy Medicine for the evaluation, registration and implementation of secure DAR solutions in protecting Sensitive data, which includes PII and PHI.

d. To enhance the enterprise network capabilities of Navy Medicine through secure application of commercial, standards-based DAR devices, services, and technologies.

e. To establish an incident reporting process in the event of lost, stolen, or compromised Sensitive data. Lost, stolen, or compromised Sensitive data means actual or possible loss of control, unauthorized disclosure, or unauthorized access of Sensitive data where persons other than authorized users gain access or potential access to such information for other than authorized purposes where one or more individuals will be adversely affected. Such incidents are also known as breaches.

2. Background

a. The operational benefits of mobile computing solutions and highly portable, reusable, and removable storage devices are acknowledged. These same benefits introduce significant risks to Navy Medicine information, computers, and networks. Improper use and/or handling of mobile computing solutions and portable storage devices can result in the loss or compromise of Sensitive data.

b. Risk mitigation is always a consideration with the application of new technology. However, risks affecting DAR can be mitigated through the use of secure and properly configured commercially available products.

3. Applicability and Scope

a. Applies to all Navy Medicine personnel, including contractors and volunteers.

b. Applies to all mobile computing devices, including, but not limited to, commercial mobile devices, as defined in references (a) through (o).

c. Applies to any portable storage device that is easily removable and stores data that can be connected to a Navy Medicine network, workstation, or other computing device via cable, universal serial bus (USB), Firewire (IEEE 1394), I-Link, infrared, radio frequency, personal computer memory card international association (PCMCIA), or any other external connection that would allow data to be transferred and removed, per reference (k). Examples of portable devices include, but are not limited to zip drives, floppy diskettes, recordable and re-writeable compact disks (CD), recordable and re-writeable digital video disks (DVD), USB flash digital media devices (thumb drives), memory sticks/cards, pc card storage devices of all types, and mini external hard drives.

4. Policy

a. Data Classification. PHI, PII and all devices upon which either or both forms of information reside must be identified. This includes aggregations of data that would not normally fall under the categorization of PHI or PII independently, but when aggregated they do meet the classification, per reference (n). As data aggregation requirements

and procedures mature, further guidance will be promulgated by the Navy Medicine Command Information Officer (CIO).

b. Physical and Environmental Controls. Physical and environmental controls will satisfy Confidential and Sensitive data requirements. All mobile computing and portable storage devices containing Sensitive data that require removal from the workplace shall be signed in and out with a supervising official designated in writing by senior leadership.

c. DAR Encryption. Any mobile computing or portable storage device containing Sensitive, PHI, or PII DAR will be password protected and encrypted. The cryptography should be National Institute of Standards and Technology (NIST)-certified at Federal Information Processing Standard (FIPS) 140-2 level per references (a) and (b). If the device is not capable of applying this standard, PHI and PII is not authorized on this device.

d. Portable Storage Device Access Controls. All Flash media devices, whether personal or government procured, will be scanned for malicious code immediately upon connecting to a Navy Medicine network and/or workstation. If antivirus scanning software is not configured to automatically scan all files when accessed, procedures must be implemented to ensure personnel manually scan media for malicious code per reference (k).

e. Authentication to Access DAR. Access to DAR requires that PKI authentication and authorization controls are implemented to the extent possible.

f. Disposition of Mobile Computing and Portable Storage Devices. In the event that DAR resides in unencrypted format on the media and devices covered by this instruction, the media will be sanitized per reference (f). Portable storage devices impacted by electronic security violations (e.g., classified spillage) will be surrendered to the command security manager per reference (k).

5. Incident Reporting. All Navy Medicine activities will implement incident response plans to address the loss, theft, or compromise of Sensitive data per references (m) through (o). For reporting purposes, the process outlined below will be utilized when there is a breach of PII or PHI:

a. Within **1 hour** of the discovery or suspicion of the loss, affected activity will notify via a single e-mail the following privacy officials and agencies of the known or suspected loss:

(1) The Department of the Navy Chief Information Officer (DON CIO) Information Assurance, Identity Management and Privacy Team, e-mail: don.privacy.fct@navy.mil, telephone: (703) 601-0120 or (703) 602-6882.

(2) The Navy Privacy Act Officer (DNS-36), e-mail: privacy@ogc.law.navy.mil, telephone: (202) 685-6545, and the Chief of Information (CHINFO), e-mail: chinfo.dutyoffic.fct@navy.mil, telephone: (703) 697-5342.

(3) Copy to: the Navy Medicine Command Information Officer (CIO) Privacy and Security Team, e-mail: rick.mccarthy@med.navy.mil, telephone: (202) 762-0037 or (202) 762-0384.

(4) Contact the local Naval Criminal Investigative Service (NAVCRIMINVSERV) office or Marine Corps Criminal Investigation Division (CID).

(5) Contact the local Staff Judge Advocate (SJA) or Office of General Council (OGC).

b. The e-mail should include the following information:

(1) Component/organization involved;

(2) Date of incident, the number of individuals impacted, and whether they are government or private citizens (if both, provide percentage of each);

(3) Brief description of incident, including circumstances of the breach, information lost or compromised, and if the information was encrypted and/or password protected.

c. Within 24 hours, activities will submit the following information via e-mail to the points of contact listed in 5a above:

(1) Documentation regarding remedial efforts, including any notification made to the individuals whose information was compromised;

(2) Description of actions the activity is taking to prevent future recurrence.

d. When applicable, issue OPREP3 per OPREP3 reporting procedures.

e. Provide letter or digitally signed e-mail notifying those individuals affected within 10 days per reference (o). If unable to provide notification within 10 days, notify DNS-36 why notification was not made and what actions are being taken to complete the notification process.

f. When affected personnel cannot be located or directly contacted, establish a toll-free number (i.e., call center) to allow impacted individuals the opportunity to obtain additional information regarding the loss.

g. Send lessons learned via e-mail to DNS-36 within 30 days of the incident.

6. Responsibilities. Navy Medicine personnel will implement the guidance set forth in this instruction within their organizations.

a. The Navy Medicine CIO will:

(1) Provide strategic oversight and policy development for the secure application of commercial DAR technology throughout Navy Medicine.

(2) Ensure compliance with the DAR technology requirements of references (a) through (o) and related policies, procedures, standards, and guidelines.

(3) Report on enterprise DAR issues to the Chief, BUMED.

b. Each Regional Information Systems Officer (RISO) will:

(1) Monitor compliance of activities within their Area of Responsibility (AOR) with this Instruction.

(2) Report compliance progress and issues to the Navy Medicine CIO.

c. Navy Medicine Support Command will:

(1) Provide technical guidance and support to all Navy Medicine activities.

(2) Provide a DAR execution strategy or solution for the enterprise.

d. Commanding Officers will:

(1) Establish a waiver process for situations in which this instruction could adversely affect the operations of Navy Medicine, and approve all applicable waivers.

(2) Designate in writing a supervisory official for signing in and out of DAR devices.

(3) Ensure the local Command Security Policy Manual is updated with the requirements of this instruction, as appropriate.

e. Each Navy Medicine Information Systems Officer (ISO) or equivalent senior information assurance official will:

(1) Inventory the location of all electronic PHI and PII within the activity.

(2) Inventory all mobile computing and portable storage devices within their area of responsibility that are capable of storing PHI, PII, or Sensitive DAR.

(3) Upon request, provide to the Navy Medicine CIO, via the Regional Information Systems Officer (RISO), specific implementation timelines for legacy system compliance with this instruction.

f. Each Navy Medicine activity Information Assurance Manager (IAM), also known as the Information Systems Security Manager (ISSM), will:

(1) Ensure that DAR security requirements specified in this instruction are integrated into all systems under their cognizance.

(2) Create appropriate waivers under the direction of the ISO where this instruction could adversely affect the operations of Navy Medicine. The waiver process should include risk analysis and risk mitigation procedures. Any technical, physical, or administrative controls implemented that deviate from the recommendations of this instruction must provide equal or greater protection to PHI and PII DAR on mobile computing and portable storage devices.

7. Report. The report contained in paragraph 5 is exempt from reports control by Part IV, paragraph 7n of reference (p).

A. M. Robinson, Jr.

A. M. ROBINSON, JR.

Distribution is electronic only via the Navy Medicine Web site at:
http://navymedicine.med.navy.mil/default.cfm?seltab=directives