DEPARTMENT OF THE ARMY
U.S. ARMY MEDICAL DEPARTMENT ACTIVITY
Fort Drum, New York 13602-5004

FD MEDDAC Regulation 25-70 10 May 2007

Information Assurance, HIPAA Security, Computer, Internet and Electronic Mail Usage Policy

1. HISTORY. This is the fourth printing of this publication, all previous editions are obsolete.

2. PURPOSE.

a. Establish procedures and policies for U.S. Army Medical Department Activity (USA MEDDAC and DENTAC) personnel with regard to use of government computer systems and devices (including peripheral devices such as printers, USB drives, stick drives and other removable media drives), Internet access and electronic mail (e-mail).

b. Define the Information Assurance (IA) policies, roles and the user's responsibility with respect to maintaining IA, guarding Protected Health Information (PHI) and maintaining computer security within the mandated parameters of Public Law 104-191, Health Insurance Portability and Accountability Act of 1996 (HIPAA), 21 Aug 96.

3. SCOPE.

a. This policy applies to all permanent, temporary and contract employees; military personnel (attached or assigned); students and volunteers; information and information systems; and networks of the USA MEDDAC, including DENTAC and Veterinary Services (VETCOM) located at Fort Drum, NY and all subsequent MEDCOM supported units on and off Fort Drum, NY, including Watervliet Arsenal Health Clinic and the MEDDAC OB/GYN Clinic located in Watertown, NY.

b. This policy also applies to tenant units such as Health Net, Veteran Affairs, Soldier Readiness Clinic (SRC) activities and Reserve and National Guard Units utilizing our Information systems and/or networked devices.

4. REFERENCES.

a. Department of Defense Directive/Joint Ethics Regulation, DoDD 5500.7R, Standards of Conduct, 30 Aug 1993.

b. DoD 8500.1, Information Assurance, 24 Oct 02.

c. DoDI 8500.2 Information Assurance (IA) Implementation, 6 Feb 03.

d. DoD 5200.2-R, Personnel Security Program, 9 Apr 99.

e. DoD 5200.8-R, Physical Security Program, May 91.

f. Department of Defense HIPAA Implementation, DoD 6025.18-R , Jan 03.

g. Public Law 104-191, Health Insurance Portability and Accountability Act of 1996 (HIPAA), 21 Aug 96.

h. Public Law 99-570, Freedom of Information Act of 1986.

i. Public Law 107-347, (Title III) Federal Information Management Security Act (FISMA) of 2002.

j. Army Medical Department (AMEDD) Health Insurance Portability and Accountability Act (HIPAA) Implementation Guide v. 3, 14 Jun 04.

k. AR 25-1, Army Information Management, 31 May 02.

l. AR 25-2, Information Assurance, 14 Nov 03.

m. AR 40-66 Medical Record Administration and Health Care Documentation, 21 Jun 06.

n. MEDCOM Supplement 1 to AR 40-66, Clinical use of electronic mail in Provider-to-Patient electronic communication, 11 May 05.

o. AR190.13, The Army Physical Security Program, 30 Oct 93.

p. AR 380-5, The Department of the Army Information Security Program, 22 Feb 88.

q. AR 380-53, Information Systems Security Monitoring, 29 Apr 88.

r. AR 380-67, Personnel Security Program, 9 Sep, 88.

s. NARMC Reg 25-54 Information Assurance, 2 Feb, 05.

t. NARMC Workstation Use and Security Policy 05-012.

u. FD MEDDAC Reg 40-45, Protected Health Information and Privacy, 10 Dec 03.

5. GENERAL STATEMENT.

a. NARMC Reg 25-54, Information Assurance, and the NARMC Workstation Use and Security Policy 05-12, will be used to standardize the guideline for the Security Plan for HIPAA security issues and for purposes of a general workstation use guideline for all other IA procedures and policies as they apply to the MEDDAC, DENTAC and VETCOM at Fort Drum, NY.

b. Army Regulation AR 25-2 will provide overall guidance and direction with respect to all other IA issues and concerns. All MEDDAC, DENTAC, and VETCOM users will comply with the elements outlined in AR 25-2, Section 3.3c. "General Users" along with the specific "user requirements" contained in this publication.

c. All references to "systems" include but are not limited to all government computers and terminals, all associated hardware and software, internal and external government networks, Internet via a government gateway, government e-mail accounts and e-mail systems, and other government fielded applications and systems.

d. References to "users" include all personnel that use government systems regardless of their employment status, i.e., military personnel; civilian, contractor and temporary employees; or student.

6. PERSONNEL SECURITY STANDARDS.

a. Personnel requiring access to Army Information Systems (IS) to fulfill their duties must possess the required favorable background investigation or formal access approval (whichever is appropriate for the position), and have a need-to-know as determined by their Supervisor.

b. New users (military, civilian, etc.) requiring access to information systems or networks are required to complete a Technical Activity Request LAN User Identification, MCID-IM FM 674-R. If access to Comprehensive Health Care System (CHCS) is required, the user must complete the CHCS User Access Request, MCID-IM FM 702-R. To comply with HIPAA and DA regulations, both request forms must be approved by the user's supervisor and the user must read the "User Agreement and Checklist" and/or "Security Briefing" and sign the back of each form where indicated.

c. The LAN Request form for new "non-military users" must accompany the Questionnaire for Non-Sensitive Positions, SF 85, or the Questionnaire for Public Trust Positions, SF 85P, to the Physical Security Officer for review. The Physical Security Officer will certify that the SF 85/85P is fully completed or verify the users background investigation status (either in-process or completed) before signing and certifying the LAN account request form for submission to IMD for processing.

d. LAN request forms for "military users" will also be reviewed by the Physical Security Officer, who will verify that the proper investigation has been completed and is on record with Joint Personnel Accounting System (JPAS).

e. Any questions regarding this process can be directed to the Information Assurance Security Officer (IASO) located in IMD.

7. ACCESS CONTROL.

a. Access to the IS and network at MEDDAC and DENTAC is a revocable privilege. All access levels are based on the user's functional duties and their "need-to-know" as determined by their chain of command.

b. All users must receive approval for access from their supervisory chain of command and the necessary background investigation must be in process or completed and verified by the Physical Security Officer before access will be granted to the LAN and/or a government computer and any application running on either the network or the workstations.

c. Illegal or unauthorized activities conducted on workstations or the network, failure to comply with submitting the paperwork for a background investigation, and/or investigations that are returned as unacceptable/incomplete will result in the user's access to all computer devices and the network being revoked.

d. All users are responsible for logging out of or locking their workstation before they leave the office/desk unattended and securing medical records and PHI so that unauthorized persons cannot see, read, take, or copy PHI. However, the current workstation group policy will automatically lock each workstation after 10 minutes of inactivity, excluding KIOSK workstations.

e. All personnel will clear through IMD prior to departing due to termination, resignation, permanent change of station (PCS), change of employment, temporary duty (TDY) deployment longer than 180 days, or other change of status in order to have their LAN and CHCS accounts, Personnel Identification Number (PIN) number and any other MEDDAC/DENTAC or VETCOM network-accessible account held open and/or deactivated. LAN and CHCS accounts which have no activity for 45 working days will automatically be deactivated during periodic access-verification audits.

8. TRAINING.

a. All users will complete initial IA Awareness training by attending the Newcomers' briefing. Annual IA Awareness training is a mandatory requirement and will be accomplished via the Annual Refresher Training (ART).

b. All users will register in the Military Healthcare System's Learning Management System (MHS Learn) on the internet and will complete all required HIPAA privacy and security training for their duty function before they are provided access to their PIN number.

c. LAN and CHCS accounts for users who fail to meet initial and/or mandated annual training requirements for IA or HIPAA as noted in this regulation will be suspended until training requirements are met.

d. Users who are designated as level IT-II will also be required to complete IA Level 1 training. Level IT-1 designation for system administrators and network specialists that support networking equipment or require high-level privileges on systems will also be required to complete IA Level II training.

9. HIPAA SECURITY COMPLAINTS, INCIDENTS AND/OR VIOLATIONS.

a. HIPAA security incidents are defined as those which involve inappropriate access to, transmission of, or use of electronic protected health information (E-PHI) to include data which is being input, processed, transmitted or at rest as long as it is in an electronic format. HIPAA security incidents will be reported to the HIPAA Security Officer.

b. If the HIPAA incident involves the paper document, medical record or physical release of information from one person to one or more other unauthorized persons or for whom we do not have appropriate authorizing documentation, this would be considered a HIPAA privacy incident and will be reported to the MEDDAC HIPAA Privacy Officer, IAW the additional HIPPA privacy guidance provided in FD MEDDAC Reg 40-45, Medical Services, Protected Health Information and Privacy.

c. All HIPAA complaints and/or incidents will be reported to either the HIPAA Privacy Officer or, if unavailable, the HIPAA Security Officer to determine if a violation of either the Public Law 104-191 or DoD 6025.18-R has occurred. The incident will be logged into the Protected Health Information Management Tool (PHIMT) documentation database, investigated and reported to command IAW FD MEDDAC Reg 40-45. Violators and violations will be subject to the sanctions as stipulated in NARMC Reg 25-54, Section 21. Additional sanctions, summarized in Appendix A of this document, may result from further investigative findings if the case is reviewed by authorities at Health and Human Services.

d. Audits of and unannounced inspections for unsecured PHI, e-PHI and/or IS devices will be conducted during the duty day as well as after hours in order to evaluate the compliance level with respect to maintaining the confidentiality of and securing the availability of patient data, PHI and access to our network. These audits/inspections will facilitate the documentation of our compliance with all HIPAA and Joint Commission (JC) standards for privacy and security and will be coordinated and/or performed by the HIPAA Privacy Officer and/or the HIPAA Security Officer. Inspection outcomes will be reported to the Performance Improvement Committee for forwarding to the Executive Committee for any required administrative action.

e. Other security incidents not involving e-PHI, such as viruses, chain letters, compromised systems, theft of automated equipment, etc,. are further defined in

NARMC Reg 25-54, Section 8. These will be reported immediately to the IMD Helpdesk and the IASO/HIPAA Security Officer.

10. AUTHORIZED USE.

a. Government systems shall be used for official use and authorized purposes only. These resources are provided to conduct government business. Personal e-mail and Internet use of reasonable duration and frequency, which does not adversely affect the performance of the employee or the organization, is permitted. This includes sending and receiving short personal e-mail messages and using systems to access the Internet, provided this access occurs during non-duty hours or authorized breaks.

b. Personal use of the Internet only extends as far as the Internet monitor and filter software will allow. The user will be held responsible to reimburse the government for any personal use telephone and/or e-mail which incurs any additional charges to the government, i.e., long distance tolls or access fees.

11. ELECTRONIC MAIL.

a. There will be no chain letters, spamming, romantic correspondence, or virus propagation actions conducted on government systems. Users that receive e-mail messages thought to be chain letters or spam will report the incident to the IMD Helpdesk. Do not forward the message to IMD unless told to do so. Under no circumstances should a user forward, respond to or “reply to all” for any chain e-mail, hoax or spam e-mail. There are websites devoted to listing various hoaxes, chain letters and viruses in the wild. It is recommended that users check these websites for clarification on any questionable e-mails. The IASO or the IMD Helpdesk can provide additional assistance, if necessary.

b. Accessing commercial or private Internet e-mail accounts from a government system is prohibited, i.e., Hotmail, Yahoo, AOL web mail, etc. All communications to solicit business advertising, other selling activities in support of private business enterprise, or any other use that would reflect adversely on the DoD or which are incompatible with public service are strictly forbidden. Users are authorized to use the government e-mail system for personal use as noted above in Section 10.

c. Outlook e-mail can be used to send patient information, but the message must be encrypted by using your Common Access Card (CAC) card. E-mails that contain Privacy Act information, Sensitive Unclassified (SU) data, For Official Use Only (FOUO), or any HIPAA PHI must be encrypted using your CAC card and should be digitally signed using your CAC card IAW MEDCOM Suppl1 to AR 40-66.

12. MONITORING.

a. Use of any DoD computer system constitutes consent to monitoring IAW AR 380-53 and AR 25-2. Government systems are the property of the U.S. government and

can be searched at any time without a user's permission. Users should be aware that information placed on a government system is subject to monitoring and users have no expectation of privacy.

b. IMD has software and systems in place that monitor and record all Internet and e-mail usage. These systems are capable of recording and monitoring each worldwide web/file transfer protocol (WWW/FTP) site visit, chat session, newsgroup, e-mail message, stored files, and file transfer. Supervisors and section chiefs have the ability to request an assessment of any subordinate users' internet activity, if they suspect performance issues or abuse.

c. At any time and without prior notice, Army supervisors and management, under lawful authority, reserve the right to examine all electronic mail and files stored on MEDDAC IS and supported systems IAW AR 25-2, Chapter 4, Section 1 paragraph 4-5t. Management searches, in the absence of the user, are permitted subject to the guidelines stipulated and IAW NARMC Reg 25-54, Section 17.

d. Periodically, all systems are scanned to check system configurations, IA vulnerability status, to verify that systems have not been compromised by viruses or other peer-to-peer applications, and to validate that only government authorized applications are installed on all government systems. Unauthorized files found on government computer systems will be deleted without notice and reported.

13. UNAUTHORIZED USE.

a. Government computer systems will not be used in any way that would interfere with official duties, undermine readiness, or reflect negatively on the DoD or the U.S. Army. AR 25-2, Chapter 4, Section 1 paragraph 4-5a outlines specifically prohibited activities that users will adhere to with respect to Army network access.

b. Government computer systems shall not be used to conduct any type of personal commercial business or used in any way that violates federal/state laws or regulations, DoD, or Department of the Army (DA) regulations, policies, or directives. Fundraising or advertising for any non-government purpose is not authorized.

c. Jokes, quotes, romantic correspondence, or derogatory correspondence of racial, ethnic, sexual, political, or religious origin are prohibited.

d. Derogatory communications against the Commander in Chief, U.S. policy, U.S. government agencies, or U.S. Army leadership are not authorized on government systems.

e. "Hacker" or "cracker" type software or actions will not be run on or against government systems.

f. Users are not authorized to install any software, freeware or shareware on government systems.

g. Users are not authorized to download any applications, programs, or graphics to government computers.

h. All software applications, programs, or graphics must be requested via CAPR, IM FM 663, and submitted to IMD for approval. Only the Automation Helpdesk will install and configure computer software to be executed on government systems.

i. Absolutely no privately-owned computers, hard drives, laptops, or personal electronic devices will be connected to MEDDAC, DENTAC or VETCOM systems or the MEDDAC network.

j. Stick drives, thumb drives and jump drives are only authorized if purchased by the government and for files which do not contain any privacy data or PHI data that can be identified and linked to a specific patient. The use of these types of drives is on a case-by-case basis and must be reviewed by the IASO or the IAM before purchasing the drive unit. User will sign the USB Thumb Drive User Agreement.

k. Accessing Internet sites that have motion graphics, video and/or audio or that include Internet radio, video and/or streaming data sites overburden the network and are not authorized.

l. The following types of software and specific programs represent a major security threat to our computer network and are also **strictly forbidden.** This is not an all-inclusive list:

(1) Peer-to-Peer or file sharing software such as Napster, Zazaa, Gnutella, WinMX, Bottorrent, LimeWire, Kazaa, Ares, or Morpheus.

(2) MP3 files – any music illegally downloaded form the Internet.

(3) Chat software: This includes ICQ, Yahoo Messenger, AIM, Paltalk, Eyeball and mIRC. The only chat application that is currently authorized is AKO-Chat which is facilitated via the AKO website and requires user authentication.

(4) Game software, including standard Microsoft games are not permitted on government equipment IAW AR 25-1.

(5) Remote Administration Software (GoToMyPC, Radmin, Remote Anywhere, Remote Desktop, etc.): Only the Automation Helpdesk is permitted to use remote access software for the purpose of assisting the users with computer hardware/software performance or training issues.

(6) FTP Software (BulletProof FTP, Cute FTP, FTP Explorer, FTP Voyager, File Dog FTP and WS FTPro): If your function requires an FTP client, the Automation Helpdesk will provide the installation you need in order to do your function. All other installs of FTP client software are forbidden.

(7) Alternate E-mail: Yahoo, Hotmail, AOL, other WEB-Mail sites, etc.

(8) Streaming audio and video for any purpose unless authorized and configured by Automation Helpdesk to support a valid governmental business requirement.

14. UNAUTHORIZED WEBSITES.

a. Unauthorized sites, resources and activities include but are not limited to areas or actions that involve gambling, hacking, cracking, sexually explicit and nudity, hate groups, extremist groups, chain letters, unofficial advertising, web-mail systems and general internet chat capability, soliciting, illegal activities, classified materials, or uses incompatible with public service. These various categories and sites are blocked at our location by DA provided Security Suite tools.

b. While performing official duties, if you are blocked from a legitimate website that is needed for successful completion of your mission, notify the Automation Helpdesk at 772-5233, and the IASO and/or the Network Specialist will evaluate the site for use.

15. COMPUTER ANTI-VIRUS PROTECTION.

a. Users will scan any removable media containing files prior to opening the file on their workstation or laptop.

b. E-mail messages containing attached files must have the attachment saved to the hard drive and scanned using Symantec Anti-Virus (AV) before being opened, transmitted or processed. If the attachment is reported as infected with a virus after scanning, the user will report it to IMD. Do not forward the message/file to IMD unless told to do so.

c. Users will not broadcast virus-warning messages. The IASO, when necessary, will broadcast these alerts.

d. DoD civilian employees and military service members are authorized and required to download a desktop security solution (Symantec or McAfee) for their home computer from the approved DoD website containing the DoD approved enterprise license AV agreement. This is especially important if users work on government-related documents on their home computer. These documents must not contain any SU, e-PHI, or FOUO material. Desktop support is provided by the DoD download site and will not be provided by the MEDDAC IMD Helpdesk. At this time, contractors are not authorized this access.

16. SU, FOUO, PRIVACY ACT, HIPAA, CLASSIFIED INFORMATION.

a. MEDDAC systems are not accredited for classified information. Classified information can not and will not be processed on MEDDAC systems, even if this information is stored on a removable disk.

b. Sensitive Unclassified (SU) data is presently the highest level authorized on MEDDAC systems.

c. You must use your CAC card to encrypt and/or digitally sign Outlook e-mail messages to transmit the following type of data to others who have a need to know on the AMED domain:

(1) Sensitive Unclassified (SU)

(2) For Official Use Only (FOUO)

(3) Privacy Act Information

(4) Electronic Protected Health Information (e-PHI HIPAA) data

17. SECURITY.

a. Users will safeguard login identifications and passwords. Any suspected password compromise will be reported immediately to the IASO.

b. CHCS passwords and access information will be released only to the user as he/she must sign for their access to that system.

c. Passwords and access information will not be shared or given to anyone other than the user unless specifically authorized by the IASO. Only the user to whom a computer account was issued is authorized to use the account. Failure to comply with this requirement will result in the account password being force-changed the first occurrence. Any subsequent occurrence that breaches our security level will be communicated to the user's supervisor chain for counseling; it may result in the account being disabled, and the user may be required to take refresher IA Awareness and/or HIPAA Security Training and/or will result in applicable sanctions as noted in Section 18 and/or Appendix A of this regulation.

d. Computers will not be left unattended by a user while they are logged into the system (this applies to the LAN, CHCS and/or Health e-forces). The user must log out or lock the workstation, and/or secure the room where the computer is located and secure any medical records or PHI to prevent unauthorized access.

e. Periodic notifications, warnings and guidance will be included in the MEDDAC Daily Update or posted to the IMD LAN & User Issues Outlook Public Folder. Some

notices may also be sent to the Drum Users Group to provide timely notices on new developments of interest to our user base.

18. SANCTIONS.

a. HIPAA electronic violations: These will be investigated by the HIPAA Security Officer, in conjunction with the HIPAA Privacy Officer and the HIPAA Compliance Officer, as necessary. If violations are identified, the policy offenders will be subject to HIPAA sanctions as outlined in NARMC Reg 25-54, Section 21, and at the MEDDAC Commander's discretion. The Federal Regulation Sanctions for HIPAA violations are provided in APPENDIX A of this document for reference.

b. NARMC Reg 25-54, 21. System of Sanctions states:

(1) This section is provided as a guideline for administrative or disciplinary actions associated with violations of IA policies. All personnel are subject to any of the actions stated below. The Chain of Command and supervisory channels maintain primary responsibility over the application of administrative and disciplinary actions.

(2) The system of sanctions is divided into two areas as follows:.

(a) Access penalty. Access to an information system or network may be affected per the DAA discretion for noted policy violations. Some of the more common access penalties include but are not limited to:

- A temporary suspension or permanent revocation of access privileges to an information system or network.

- Mandatory participation in remedial IT security training.

- Temporary suspension or permanent revocation of IT clearance.

- Loss of access to or use of other new or emerging IT technologies.

(b) Applicable administrative or disciplinary actions as per published regulatory guidance. Some of the more common penalties include or can be found but are not limited to:

- Verbal and/or written counseling.

- Punishment under the Uniform Code of Military Justice (UCMJ).

- Punishment under the Civilian Personnel Table of Penalties (AR 690-700, Chapter 751).

- Contractor personnel could be subject to immediate removal.

- Applicable sanction penalties under the HIPAA Act of 1996.

- Criminal prosecution under several U.S. Codes including U.S.C. 1030 and U.S.C. 506.

(3) A combination of sanctions can be imposed for committed violations. As a general rule, an access penalty will be imposed by the DAA through the IASO when and where deemed appropriate. The chain of command and supervisory channels has responsibility over administrative and disciplinary actions.

(4) Personnel found to be in violation of any of the guidelines mentioned in this regulation will receive written notification from the local IASO. The IASO will also report violations to the individual's supervisory channel and/or chain of command.

(5) Suspected (HIPAA Security) violations will be informally investigated by the IASO.

(6) Upon notification of a violation, supervisors are required to submit an action taken statement in writing to the IASO within 7 days of receipt. The actions-taken statement may be made via e-mail to the IASO or in the form of a formal memorandum addressed to the Director of Information Management or Chief, IMD (ATTN: IASO).

(a) Personnel are entitled to appeal administered penalty as per local polices and procedures.

(b) Records of violations and actions taken will be maintained by the IASO.

19. RESPONSIBILITIES.

a. This policy is punitive in nature. Military violators of these procedures are subject to punishment under the Uniform Code of Military Justice (UCMJ), Article 92, "Disobeying a Lawful Order." Any civilian employee violating this policy may also be subject to disciplinary action. Military and civilian violators are both subject to disciplinary procedures pursuant to the Joint Ethics Regulation, DoDD 5500.7R.

b. Supervisors must ensure that all users have read and understand this policy. Supervisors have the authority and the responsibility to monitor usage of communications systems and other resources to ensure this policy is followed. Supervisors have the authority to limit, restrict or revoke all use of communication systems and resources for abuse of the above noted restrictions.

20. REPORTING: Violations of this regulation, compromised computers and/or security incidences should be reported to the IASO and/or the Chief, Information Management.

APPENDIX A

HIPAA Sanctions and Penalties as defined by the HIPAA and DoD Regulations, References a, b, and c.

Civil Penalties:

Monetary	Prison Time	Offenses
$100	NA	Single violation of a provision (multiple penalties for violating multiple provisions).
$25,000	NA	Multiple violations of an identical requirement made during the calendar year.

Criminal (maximum) Penalties:

Monetary	Prison time	Offenses
Up to $50,000	Up to one year	Wrongful disclosure of individually identifiable health information.
Up to $100,000	Up to five years	Wrongful disclosure of individually identifiable health information committed under false pretenses.
Up to $250,000	Up to ten years	Wrongful disclosure of individually identifiable health information committed under false pretenses with intent to sell, transfer, or use for commercial advantage, personal gain, or malicious harm.

The proponent of this publication is the Information Management Division. Send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) to Information Management Division, U.S. Army Medical Department Activity, 11050 Mount Belvedere Blvd, Fort Drum, NY 13602-5004.

FOR THE COMMANDER:

LAWRENCE P. NOLAN
LTC, MS
Chief of Staff

DISTRIBUTION

A