



Joint Task Force National Capital Region Medical **INSTRUCTION**

NUMBER 8460.01
NOV 08 2011

J-6

SUBJECT: Electronic Mail (E-mail) Policy

References: See Enclosure 1

1. PURPOSE. This Instruction, in accordance with the authority in References (a) through (d) and the guidance in Assistant Secretary of Defense for Health Affairs Memorandum (Reference (e)), establishes policy and provides guidance to all Medical Treatment Facilities (MTFs) and Centers on the E-mail policy for the Joint Task Force National Capital Region Medical (JTF CapMed) Joint Medical Network.

2. APPLICABILITY. This Instruction applies to JTF CapMed and all Joint MTFs and Centers in the National Capital Region (i.e., Fort Belvoir Community Hospital, Walter Reed National Military Medical Center, and the Joint Pathology Center).

3. DEFINITIONS. See Glossary

4. POLICY. It is JTF CapMed policy that:

a. JTF CapMed shall not transfer classified data, as defined in DoD Directive (DoDD) 8500.01E and DoD Instruction (DoDI) 8500.2 (References (f) and (g)), via unclassified E-mail systems. Classified data transfers shall be performed only on accredited, classified systems.

b. Government office equipment, including E-mail, shall only be used for official purposes, except as specifically authorized in this Instruction. End-users are permitted limited appropriate use of government office equipment for personal use if the use does not interfere with official business and involves minimal additional expense to the government. This limited appropriate personal use of government office equipment must take place during the end-user's non-work time. This privilege to use government office equipment for non-government purposes may be revoked or limited at any time. This personal use must not result in loss of end-user productivity or interference with official duties. Inappropriate personal use is prohibited (see Enclosure 2 for

NOV 08 2011

clarification of what constitutes inappropriate personal use). Moreover, such use should incur only minimal additional expense to the government in areas such as:

- (1) Communications infrastructure costs; e.g., telecommunications traffic.
- (2) General wear and tear on equipment.
- (3) Data storage on storage devices.

(4) Transmission impacts with moderate E-mail message sizes, such as E-mails with attachments smaller than 10 megabytes. Since attachments are a major source of malicious software (malware), attachments of any size on non-official E-mail are discouraged.

c. This policy in no way limits employee use of government office equipment, including E-mail, for official activities.

d. End-users need to ensure that their personal use of Government office equipment is not incorrectly interpreted to represent the agency. If there is an expectation of such an interpretation, a disclaimer must be used, such as "The contents of this message are mine personally and do not reflect any position of the government or my agency."

e. End-users do not have a right, nor should they have an expectation, of privacy while using any government office equipment or system at any time, including using E-mail. To the extent that end-users wish that their private activities remain private, they should avoid using office equipment or systems for personal E-mail. By using government office equipment or systems, end-users imply their consent to disclosing the contents of any files or information maintained or passed through government office equipment. By using office equipment or systems, consent to monitoring and recording is implied with or without cause, including (but not limited to) using E-mail. Any use of government E-mail is made with the understanding that such use is generally not secure, private, or anonymous and may be monitored at any time.

f. End-users need to protect JTF CapMed Joint MTF and Center systems from malware. Users shall be alert to the source of any attachment and shall be alert as to whether they are expecting it. End-users shall be alert for anything that is unexpected or may indicate a virus. Users shall consult with the Information Technology Help Desk in these situations.

g. End-users shall not send or receive copyrighted graphics or documents through E-mail without the owner's permission, unless otherwise permitted under applicable provisions of Federal copyright laws.

h. End-users shall not send or receive illegal or unlicensed software.

i. Use other than as described herein is considered to be misuse of information resources.

j. It is a violation of regulations to use government equipment for personal gain.

NOV 08 2011

k. The JTF CapMed E-mail standard is determined by the Chief Information Officer (CIO) as specified in DoDD 5400.07 (Reference (h)).

l. E-mail messages, like all electronic documents, are considered agency records and are subject to the provisions of DoD 5400.11-R, DoD 5500.7, and DoDD 5500.07 (References (i) through (k)).

m. Many personal E-mail programs now allow "instant messaging" or are Web-enabled, which allows access via any Internet connection. End-users are authorized to use JTF CapMed resources to access Web-enabled personal E-mail services but not the "instant messaging" associated with these programs. Using "instant messaging" via the JTF CapMed network impacts the communication capacity and weakens JTF CapMed network defenses. End-users are not authorized to use JTF CapMed resources to access Web-enabled "instant messaging" without the express written permission of the Designated Approving Authority (DAA). The only authorized "instant messaging" application is via Defense Connection Online.

n. End-users may not use personal E-mail services for official business without the express written permission of the DAA.

o. When using Remote Network Access to send E-mail from a remote location, users must adhere to the provisions of DoDD 8000.01 (Reference (l)).

p. E-mail containing "Sensitive Information" shall be encrypted using a DoD-issued certificate.

q. All official E-mail will be digitally signed with a DoD-issued certificate.

r. The Department of Defense is implementing a Key Management Infrastructure (KMI) to provide engineered solutions for the security of networked computer-based systems. Part of this KMI is a Public Key Infrastructure (PKI) and Public Key Enabling, consisting of products and services that identify an individual and bind that person to an identified public/private key pair. Programs that carry out or support the mission of the Department of Defense require services such as identification, authentication, confidentiality, technical non-repudiation, and access control.

s. Failure to adhere to the provisions of this Instruction may result in termination of access to all JTF CapMed-supported local area networks and in other adverse administrative or disciplinary actions.

5. RESPONSIBILITIES. See Enclosure 2

6. PROCEDURES

NOV 08 2011

a. Ultimate responsibility for keeping the JTF CapMed Joint MTF and Center systems virus-free remains with the end-user. End-users shall be alert for attachments that are unexpected or may indicate a virus. Users shall consult with the Information Technology Help Desk in these situations.

b. The end-user may not introduce any software, including that attached to E-mail, into the JTF CapMed environment without prior approval by JTF CapMed CIO.

7. RELEASABILITY. UNLIMITED. This Instruction is approved for public release and is available on the Internet from the JTF CapMed Web Site at: www.capmed.mil.

8. EFFECTIVE DATE. This Instruction is effective immediately.



SCOTT WARDELL

Executive Director for Administrative Operations

By direction of the Commander

Enclosures

1. References
 2. Responsibilities
- Glossary

NOV 08 2011

ENCLOSURE 1REFERENCES

- (a) Deputy Secretary of Defense Memorandum, “Establishing Authority for Joint Task Force – National Capital Region Medical (JTF CapMed) and JTF CapMed Transition Team,” September 12, 2007
- (b) Deputy Secretary of Defense Approved Action Memorandum, “Civilian and Military Personnel Management Structures for the Joint Task Force National Capital Region – Medical (JTF CapMed),” January 15, 2009
- (c) Comprehensive Master Plan for the National Capital Region Medical, April 23, 2010
- (d) Supplement to the Comprehensive Master Plan for the National Capital Region Medical, August 31, 2010
- (e) Assistant Secretary of Defense for Health Affairs Memorandum, “Military Health System (MHS) Information Assurance (IA) Policy Guidance and MHS IA Implementation Guides,” February 23, 2010
- (f) DoD Directive 8500.01E, “Information Assurance (IA),” October 24, 2002
- (g) DoD Instruction 8500.2, “Information Assurance (IA) Implementation,” February 6, 2003
- (h) DoD Directive 5400.07, “DoD Freedom of Information Act (FOIA) Program,” January 2, 2008
- (i) DoD 5400.11-R, “Department of Defense Privacy Program,” May 14, 2007
- (j) DoD 5500.7-R, “Joint Ethics Regulation (JER),” current edition
- (k) DoD Directive 5500.07, “Standards of Conduct,” November 29, 2007
- (l) DoD Directive 8000.01, “Management of the Department of Defense Information Enterprise,” February 10, 2009
- (m) DoD Instruction 8520.02, “Public Key Infrastructure (PKI) and Public Key (PK) Enabling,” May 24, 2011
- (n) Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer, “United States Department of Defense X.509 Certificate Policy,” February 9, 2005
- (o) Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer, “Key Recovery Policy for the United States Department of Defense,” current edition¹
- (p) Defense Information Systems Agency Information Assurance Support Environment, “External Certification Authority X.509 Certificate Policy,” February 2, 2011
- (q) Chapter 33 of title 44, United States Code
- (r) Defense Information Systems Agency Information Assurance Support Environment, “ECA PKI Program: External Certification Authority Program,” current edition²
- (s) Sections 552 and 552a of title 5, United States Code
- (t) Section 278g-3 of title 15, United States Code
- (u) DoD Directive 5230.25, “Withholding of Unclassified Technical Data From Public Disclosure,” November 6, 1984

¹ Available on the SIPRNet: <http://iase.disa.rel.smil.mil/pki/pki-guidance.html>

² Available at: <http://iase.disa.mil/pki/eca/>

NOV 08 2011

ENCLOSURE 2RESPONSIBILITIES

1. COMMANDER, JTF CAPMED (CJTF). The CJTF shall designate the CIO.

2. JOINT MTF COMMANDERS AND CENTER DIRECTORS. Joint MTF Commanders and Center Directors shall ensure that the provisions of this Instruction, References (a) through (l), and DoD Instruction 8520.02; United States Department of Defense X.509 Certificate Policy; Key Recovery Policy for the United States Department of Defense; External Certification Authority X.509 Certificate Policy; and Chapter 33 of title 44, U.S.C. (References (m) through (q)) are implemented.

3. INFORMATION MANAGEMENT AND INFORMATION TECHNOLOGY (IM/IT) DEPARTMENT. The IM/IT department shall:
 - a. Develop E-mail security policies, standards, and procedures.

 - b. Ensure E-mail use complies with applicable security laws, guidelines, regulations, and standards, both internal and external. That includes, but is not limited to, public laws and the JTF CapMed, the General Services Administration, and the Office of Management and Budget publications.

 - c. Make decisions on and assist end-users with security safeguards for E-mail use.

 - d. Advise and assist management on appropriate administrative action(s) if misuse occurs.

 - e. Manage the JTF CapMed E-mail system under the direction of JTF CapMed CIO's office.

 - f. Protect the network from malware.

 - g. Establish and keep current internal lists and other internal addresses, including deleting the mailboxes of end-users who have departed the JTF CapMed or those who have violated the provisions of this Instruction.

 - h. Support the JTF CapMed E-mail end-users.

 - i. Monitor the use of electronic communications to ensure adequate performance and proper use, as approved by the CIO.

 - j. Use or disclose information obtained during the monitoring process only as required in the performance of official duties.

NOV 08 2011

k. Notify the end-user, the end-user's manager, and IM/IT of any problem concerning the end-user's conduct in accessing and using E-mail.

l. Revoke lost or stolen DoD certificates.

m. Provide and maintain the hardware and software necessary to send encrypted and digitally signed E-mail.

n. Recover key encryption certificates in accordance with Reference (o).

4. END-USERS

a. End-users shall:

(1) Check for messages regularly.

(2) Dispose of messages (which may include filing, archiving, or deleting) before mailboxes become too full to receive additional correspondence, keeping in mind that E-mail is subject to the provisions of References (h) and (i). The mailbox limit will be adjusted as JTF CapMed resources dictates. Users will receive a warning notification prior to reaching the set limit. This includes such boxes as the inbox, sent items, deleted items, etc.

(3) Use the E-mail system only for its intended purpose and protect the security of information in accordance with References (f) through (l).

(4) Locate Internet addresses of intended message recipients. There is no comprehensive on-line directory of addressees available.

(5) Provide their Internet address to those who wish to send them messages.

(6) Be alert for unexpected attachments or those that may contain a virus.

(7) Dispose of unsolicited messages, such as advertisements, chain letters, jokes, etc., in accordance with the provisions of Reference (j). Further distribution of these types of messages is rarely consistent with Reference (j).

(8) Refrain from any practices that might jeopardize, compromise, or render useless any JTF CapMed Joint MTF or Center data, system, or network.

(9) Be individually responsible and liable for any disclosures of personal information if the employee chooses to send such information through an electronic communications system provided by the JTF CapMed Joint MTFs or Centers or the Federal Government.

(10) Not send classified information through non-classified network (i.e., NIPRNet). All classified data transfers shall be performed only on accredited, classified systems (i.e., SIPRNet).

NOV 08 2011

(11) Information subject to References (h) and (i) shall be appropriately marked "For Official Use Only" if transmitted electronically.

(12) Refrain from any activities that could congest or disrupt an electronic communications system provided by the JTF CapMed Joint MTFs or Centers or the Federal Government.

(13) Refrain from any inappropriate personal uses.

(14) Store important E-mail messages according to disposition instructions.

(15) Encrypt E-mail containing "Sensitive Information."

(16) Digitally sign official E-mail.

(17) Regularly check the JTF CapMed Intranet for updated procedures.

(18) Immediately report any loss, theft, or misuse of DoD certificates to their supervisor, the Office of Security, and the PKI representative or Verification Official.

(19) Inform persons outside of the Federal Government with whom they wish to communicate via digitally signed and/or encrypted E-mail of the requirement to obtain a digital certificate from one of the Department of Defense's recognized External Certificate Authorities (ECA) (see ECA PKI Program: External Certification Authority Program (Reference (r))).

(20) Request for restoring key encryption certificates will be sent by a digitally signed email or in person to the appointed Key Recovery Agent(s) or Key Recovery Officials.

b. End-users shall not:

(1) Participate in any personal use that could cause congestion, delay, or disruption of service to any Government system or equipment. For example, greeting cards, video, sound, or other large file attachments can degrade the performance of the entire network. "Push" technology, such as Pointcast on the Remote Network Access, Real Audio, and other continuous data streams would also degrade the performance of the entire network and could be considered an inappropriate use.

(2) Use the Government systems as a staging ground or platform to gain unauthorized access to other systems, unless mission makes it necessary.

(3) Create, copy, transmit, or retransmit of chain letters or other unauthorized mass mailings, regardless of the subject matter, unless mission makes it necessary.

NOV 08 2011

(4) Use Government office equipment for activities that are illegal, inappropriate, or offensive to fellow end-users or the public. Such activities include, but are not limited to, hate speech or material that ridicules others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation.

(5) Create, download, view, store, copy, or transmit sexually explicit or sexually oriented materials, unless mission makes it necessary.

(6) Create, download, view, store, copy, or transmit materials related to gambling, weapons, terrorist activities, and any other illegal activities or activities otherwise prohibited, etc., unless mission makes it necessary.

(7) Participate in commercial purposes, support "for-profit" activities, or support other outside employment or business activities (e.g., consulting for pay, sales, or administration of business transactions, or sale of goods or services).

(8) Engage in any outside fund-raising activity, endorsing any product or service, participating in any lobbying activity, engaging in any prohibited partisan political activity, or personal use to sell at-no-cost personal items such as "tickets" or "vacation rentals."

(9) Engage in posting agency information to external newsgroups, bulletin boards, or other public forums without authority. This includes any use that could create the perception that the communication was made in one's official capacity as a Federal Government end-user, unless appropriate agency approval has been obtained, or any use that is at odds with the agency's mission or policies.

(10) Engage in any use that could generate more than minimal additional expense to the government.

(11) Engage in the unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information, including computer software and data that includes privacy information, copyrighted, trademarked, or material with other intellectual property rights (beyond fair use), proprietary data, or export controlled software or data, unless mission makes it necessary and as otherwise authorized under applicable law and regulation.

NOV 08 2011

GLOSSARYDEFINITIONS

certificate. A digital representation of information that, at a minimum, identifies the certificate authority issuing it, names or identifies its subscriber, contains the subscriber's public key, identifies its operational period, and is digitally signed by the certification authority issuing it.

CIO. The senior official appointed by the CJTF who is responsible for developing and implementing information resources management in ways that enhance the JTF CapMed mission performance through the effective, economic acquisition and use of information.

DAA. The official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with designated accrediting authority and delegated accrediting authority.

E-mail. A means of communication that uses computer-to-computer data transfer technology, normally as textual messages or attached files.

end-user. A JTF CapMed employee or contractor who uses computer hardware or software to perform work-related tasks.

end-user non-work time. Times when the end-user is not otherwise expected to be addressing official business. End-users, for example, may use Government office equipment during off-duty hours, such as before or after a workday (subject to local office hours), lunch periods, authorized breaks, or weekends or holidays (if the employee's duty station is normally available at such times).

ECA. The Department of Defense has established the ECA program to support the issuance of DoD-approved certificates to industry partners and other external entities and organizations. The ECA program is designed to provide the mechanism for these entities to securely communicate with the Department of Defense and authenticate to DoD Information Systems.

hardware token. A portable, user-controlled, physical device used to generate, store, and protect cryptographic information, and to perform cryptographic functions.

Internet. The loosely connected worldwide collection of computer systems that uses a common set of communications standards to send and receive electronic information.

key recovery. The capability for authorized entities to retrieve keying material from a key backup or archive.

key recovery policy. A named set of rules that specify the conditions under which key recovery information must be created and conditions under which and to whom escrowed keys may be

NOV 08 2011

released; it also indicates who are allowable Key Recovery Agent(s) and Key Recovery Officials and how escrowed keys must be maintained.

JTF CapMed environment. Any computer, media, or network used by JTF CapMed users.

personal use. Activity that is conducted for purposes other than accomplishing official or otherwise authorized activity. End-users may make limited use under this policy of Government office equipment to seek employment in response to Federal Government downsizing or communicate with a volunteer charity organization.

PKI. The framework and services that provide for the generation, production, distribution, control, accounting, and destruction of public key certificates.

privilege. In the context of this policy, privilege means that the Executive Branch of the Federal Government is extending the opportunity to its end-users to use Government property for personal use in an effort to create a more supportive work environment. However, this policy does not create the right to use Government office equipment for non-Government purposes. Nor does the privilege extend to modifying such equipment, including loading personal E-mail software or making configuration changes. Government office equipment, including the E-mail system, includes, but is not limited to, personal computers and related peripheral equipment and software, office supplies, Internet connectivity, and access to Internet services and E-mail.

Public Key Enabling. The incorporation of the use of certificates for security services such as authentication, confidentiality, data integrity, and nonrepudiation. Public Key Enabling involves replacing existing or creating new user authentication systems using certificates instead of other technologies, such as user identification and password or Internet protocol filtering; implementing public key technology to digitally sign, in a legally enforceable manner, transactions and documents; or using public key technology, generally in conjunction with standard symmetric encryption technology, to encrypt information at rest and/or in transit.

record. As defined in Reference (l), the term includes: all books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value or data in them. Is made or received by an agency of the U.S. Government under Federal law or in connection with the transaction of agency business.

Sensitive Information. Information the loss, misuse, or unauthorized access to or modification of could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, U.S.C. (Reference (s)), but which has not been specifically authorized under criteria established by Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy (section 278g-3 of title 15, U.S.C. (Reference (t))). This includes information in routine DoD payroll, finance,

NOV 08 2011

logistics, and personnel management systems. Sensitive information sub-categories include, but are not limited to, the following:

For Official Use Only. In accordance with Reference (h), DoD information exempted from mandatory public disclosure under section 552 of Reference (s).

Privacy Data. Any record that is contained in a system of records, as defined in Reference (s), and information the disclosure of which would constitute an unwarranted invasion of personal privacy.

Unclassified Technical Data. Data that is not classified, but is subject to export control and is withheld from public disclosure according to DoDD 5230.25 (Reference (u)).

Proprietary. Information that is provided by a source or sources under the condition that it not be released to other sources.

support. Diagnosing and resolving problems regarding operating and using E-mail.