

NOMIINST 5230.4C  
Code N14  
07 Mar 01

NAVOPMEDINST INSTRUCTION 5230.4C

Subj: ELECTRONIC MAIL (E-MAIL) USE POLICY

Ref: (a) BUMEDINST 5230.14  
(b) BUMEDINST 5230.4  
(c) SECNAVINST 5216.5D

Encl: (1) Electronic Mail (E-Mail) and Freedom of Information/  
Privacy Act Guidance

1. Purpose. To provide policy regarding permissible and prohibited use of electronic mail (e-mail) at the Naval Operational Medicine Institute (NOMI). Violations of the prohibited activities listed in paragraphs 6f(1) through 6f(12) below are subject to administrative and/or disciplinary action, including non-judicial punishment or courts-martial.

2. Cancellation. NAVOPMEDINST Instruction 5230.4B

3. Scope. This instruction applies to NOMI headquarters, its detachments and components.

4. Background. Electronic mail (e-mail) is a tool available within NOMI that can aid the smooth, efficient, and timely conduct of business and allows for the quick query and reporting of information between users without direct person-to-person or telephone contact. It possesses the ability to carry an attached file (i.e., text, graphics, programs, etc.). Per reference (a), e-mail has become a vital means of communication within Claimancy 18. Its many attributes allow users to use it for informal communications in place of telephone calls, or to transmit official correspondence with the same expectation for receipt and action previously accompanying more traditional means of information transfer.

NOMIINST 5230.4C

07 Mar 01

5. Responsibilities. Per reference (b), the Chief, Bureau of Medicine and Surgery (BUMED) has delegated authority to activities within BUMED to maintain e-mail accounts for their commands. Further guidance is provided in enclosure (1).

6. Policy. Per reference (c), e-mail allows individuals and activities exchange information by computer. You may use it for informal communications in place of telephone calls or to transmit formal correspondence within DOD. E-mail at NOMI is designated as "quasi-official" and as such represents only the originator's comments. E-mail users are authorized to communicate directly with other commands and will keep their chain of command apprised of important or far-reaching business conducted by e-mail.

a. Access to e-mail at NOMI is a privilege and not a right of employment; therefore, e-mail privileges may be denied in part or in entirety, as directed by the Commanding Officer.

b. E-mail messages on government computers and networks are government property and not personal property, and the use of government communications systems is subject to monitoring, interception, accessing, and recording. All users of e-mail systems on government computers have no expectation of privacy or confidentiality in their use of government information systems.

c. E-mail messages that contain inappropriate content or attachments (e.g., remarks or images) are considered the same as if spoken or written in a memorandum, and may result in consequences under existing processes concerning sexual harassment, discrimination, and other provisions relating to employee (military and civilian) conduct.

d. E-mail messages may be subject to the Freedom of Information Act (FOIA) or may be considered official records. Further guidance is provided in enclosure (1).

e. E-mail may be used for personal purposes, as long as such use:

(1) Does not adversely affect the performance of official duties.

(2) Does not overburden NOMI's computing resources or network communication systems.

(3) Does not adversely reflect upon the Department of Defense, Department of the Navy, the Navy Medical Department, or NOMI (to include transmitting pornographic materials; racial, ethnic, sexist and indecent/obscene jokes and literature; chain letters; and unofficial advertising).

f. The use of e-mail on government resources for purposes other than those described in paragraphs 6e(1) through 6e(3) above is prohibited. Examples of prohibited use include, but are not limited to, the following:

(1) Illegal, fraudulent, or malicious activities (such as writing, coding, compiling, storing, transmitting, or transferring malicious software codes, to include viruses, logic bombs, worms, and macro viruses).

(2) Partisan political activity, political or religious lobbying or advocacy.

(3) Activities whose purposes are for personal or commercial financial gain, to include chain letters.

(4) Unauthorized fund raising.

(5) Accessing, storing, processing, displaying, or distributing offensive or obscene material (such as pornography and hate literature).

(6) Obtaining, transporting, installing, or using software obtained in violation of the appropriate vendor's patent, copyright, trade secret, or license statement (including shareware).

(7) Participation in chat rooms for uses other than those outlined in paragraphs 6e(1) through (3).

NOMIINST 5230.4C

07 Mar 01

(8) Introducing classified information into an unclassified system or environment.

(9) Gambling, wagering, or placing any bets.

(10) Posting personal home pages on the Internet.

(11) Personal encryption of electronic communication.

(12) Plagiarism; cutting and pasting ideas from the Internet into your own document without giving credit to the author.

g. Violations of paragraph 6f above are subject to disciplinary or administrative action.

7. Action:

a. Directors, Officers in Charge, Department Heads, Division Officers

(1) Ensure policy guidelines contained in this instruction are followed.

(2) Control and monitor access and usage within respective directorates/departments/divisions.

(3) Ensure personnel within their respective directorates/departments/divisions complete the check-out process with Management Information Department (MID) to terminate e-mail accounts upon their departure from the command.

b. Head, Administrative/Personnel Management Department. Ensure departing personnel report to MID to terminate e-mail accounts.

c. Head, Information Management/Technology Department.

(1) Coordinate with Network Security Manager and Information Security Officers, to ensure new account holders are

properly trained and equipped to operate the e-mail systems at NOMI in an effective and efficient manner.

NOMIINST 5230.4C  
07 Mar 01

(2) Construct an audit trail providing the account holder's (e-mail originator's) name, and the date and time e-mail messages depart the originator's individual mailbox, maintaining all audit files indefinitely.

(3) Terminate inert accounts that have not been active for a period of 3 months or more.

(4) Configure NOMI's Message Transport Agent (MTA) so that oversized e-mails are placed in a deferred queue for attempted delivery during off-peak periods.

(5) Configure e-mail systems to accommodate interagency and extra-governmental exchanges of e-mail up to 5 megabytes.

d. All E-Mail Users

(1) Check e-mail account for incoming messages at minimum of twice daily for each day the user is present at the command.

(2) Avoid sending e-mail attachments in multiple formats.

(3) Beware of software and other files downloaded from the Internet and scan all software and executable files that are received as attachments for computer viruses.

(4) Promptly delete undesired e-mail messages.

(5) Report to Network Security Manager to terminate e-mail account(s) upon permanent departure from NOMI.

/s/

J. H. FAHEY

Distribution:  
List A



ELECTRONIC MAIL (E-MAIL) AND FREEDOM OF  
INFORMATION/PRIVACY ACT GUIDANCE

1. Users of the e-mail system should be aware that this new method of communication is not exempt from the Freedom of Information Act (FOIA), 5 U.S.C. Section 552 (1982 & Supp. IV 1986) or Privacy Act, 5 U.S.C. Section 552a (1982 & Supp. IV 1986). Problems may arise due to the ease and informality of the system, coupled with permanence not readily apparent.

2. It must be noted that e-mail is never truly private. E-mail users have no expectation of privacy or confidentiality in their use of government information systems per paragraph 6b of the basic instruction. System Administrators and operators may have access to stored e-mail messages on the server or computerized workstations, if system problems exist.

3. The e-mail system aids rapid transmission of information among commands. The user accesses the system via an individualized password and may then send or receive messages through a centralized computer network. Incoming messages are stored as follows:

a. Exchange Server E-Mail. Microsoft Exchange is the Primary e-mail system in use at NOMI. E-mail on an Exchange server is stored on the server by default but may be offloaded to the user's local hard drive. Any files offloaded will not be included in the nightly backup of the Exchange server files. After reading messages, the recipient may delete them, store them within personal folders created in the e-mail client on the computerized workstation, or store them in a printed form. It is the recipient's responsibility to purge deleted messages from their workstation.

b. Defense Information Systems Network E-Mail. Incoming e-mail messages are temporarily stored in the central e-mail server until retrieved. Retrieved messages are then stored in the recipient's local computer. After reading messages, the recipient may delete them, store them within personal folders created in the e-mail client on the computerized workstation, or store them in a printed form. It is the recipient's responsibility to purge deleted messages from the computerized workstation, which is manually accomplished through the e-mail client's software configuration.

4. FOIA provides any person a right of access to all information maintained by federal agencies, unless exempted by the statute. FOIA applies to information stored in any form, including paper, ADP storage media, and computer printouts. E-mail transmissions are subject to FOIA from the moment they are created until they no longer exist. Hard copies of e-mail messages also fall under FOIA.

5. The Privacy Act provides individuals a right of access to records pertaining to themselves, while barring disclosure to others in the absence of an exemption. The Act only applies to records filed and retrieved by an individual's name, social security number, or other personal identifier. While messages on the e-mail system are usually not subject to the Privacy Act, since they are filed and retrieved by sequential number, the Act may apply if the recipient stores the message, either in the computer or in paper form, by an individual's name or personal identifier.

6. An important aspect of any communications system is security. All e-mail users should ensure that access to the system is limited to those with authorization. Unauthorized disclosures may violate the Privacy Act or waive otherwise applicable FOIA exemptions.

7. In those instances where disclosure of e-mail communications is not desired, the following procedures are recommended:

a. Promptly delete e-mail messages you do not desire to retain. Remember that e-mail is retained in the e-mail folder until it is affirmatively deleted. Reading an e-mail message will not delete it. In addition deleted messages are stored in a deleted items folder. Only after they are removed from the deleted items folder is the message fully purged from the system.

b. Do not retain hard copies of e-mail. Be aware that filing messages by an individual's name or personal identifier may bring the e-mail message within the purview of the Privacy Act.

c. When communicating sensitive information, consider using the telephone in lieu of e-mail. Conversations are not subject to FOIA or the Privacy Act, although notes taken during a conversation may be.

8. In summary, when information transmitted by e-mail is retained in any form, it should be treated as any other official government record.