

Title: E-Mail/Internet Policy

Statement of Purpose: To provide guidelines for the use of E-Mail/Internet.

Text:

- I. Policy
  - A. Network systems and services shall be used in ways consistent with overall hospital policy.
  - B. Network systems and services will be used for mission-related purposes, including the carrying out of day-to-day hospital operations.
  - C. Network systems and services shall not be used in a way that is disruptive to the operation of the hospital or offensive to others.
  - D. The use of network systems for transmission of information disparaging to others based on race, origin, sex, sexual orientation, age, disability, religion, or political causes, or outside organizations, or personal gain (as in the use of "chain letters") is prohibited. Use of network systems in this manner shall result in disciplinary action, up to and including immediate termination.
  - E. Users shall adhere to confidentiality and release of information policies as defined in Administrative Policies, Information Security and Administrative Policies , Release of Patient Information/Access to Medical Records.
  - F. Confidentiality of electronic communications services can not be guaranteed. All communications are assumed to be unsecured. Use the postcard rule: "Don't send anything you wouldn't put on a postcard."
- II. Procedure
  - A. Authorization will be granted to personnel who require access to network systems and services for reasons that include, without limitation:
    1. Retrieving business-related information
    2. Trouble-shooting hardware and software problems
    3. Preventing unauthorized access and system misuse
    4. Assuring compliance with software copyright and distribution policies.
  - B. Confidential information shall not be transmitted or forwarded to:
    1. Outside companies or individuals not authorized to receive such information
    2. Hospital users who have no business reason for such information at the present time
    3. Healthcare information which identifies the patient, physician, or employee shall not be transmitted via the Internet.
  - C. Your Health System users shall not attempt to gain access to any e-mail messages not addressed to them. Normal disciplinary processes related to privacy and confidentiality shall apply, up to and including termination.
  - D. Use of network systems is a privilege which may be revoked at any time for inappropriate use or misconduct.
    1. All users shall be responsible for complying with the guidelines contained in this policy and Human Resources policy addressing ethical standards and conflicts of interest.
    2. Violation shall result in revocation of network systems privileges and any other applicable actions described in Human Resources policy addressing disciplinary procedures.
  - E. Monitoring will occur when there is evidence that a user is involved in activities that are prohibited by law, that violate hospital policies, that may jeopardize the integrity or viability of the hospital's network systems, or that violate this policy and guidelines.
  - F. As technology for communication and information processing evolves, the hospital will continue to examine and refine its information management policies.
  - G. Users may use hospital network systems to access the following approved Internet services: e-mail
    1. World Wide Web
    2. Gopher
    3. Telnet.
    4. Internet services which are not approved for use through hospital network systems include the following:
      - a. Newsgroups
      - b. Internet Relay Chat (IRC)

- c. Internet phone
  - d. on-line gaming
  - e. Multi User Domain/Dungeon (MUD).
  - f. Use of these non-approved services shall result in revocation of network systems access privileges and any other applicable actions described in Human Resources policy addressing disciplinary procedure.
5. The following guidelines apply to general Internet access:
- a. Users may use the Internet for professional activities and career development. Users may use the Internet to connect to resources that provide information relating to career and education activities, and participate in reading electronic mail discussion groups on professional topics.
  - b. Users shall conform to the standards of conduct and specific rules of etiquette when accessing the Internet. Users shall use their access to the Internet in a responsible and informed way, conforming to network etiquette and courtesies. Use of the Internet encompasses many different interconnected networks and computer systems. Many of the systems are provided free of charge by universities, public service organizations, and companies, and each system has its own rules and limitations. Specific inappropriate conduct includes but is not limited to:
    - 1) Use of the Internet for unlawful activities;
    - 2) Use of the Internet for commercial activities not related to the organization;
    - 3) Activities that interfere with the ability of other users to effectively use the network;
    - 4) Violations of computer system security;
    - 5) Any communication which violates any applicable laws and regulations;
    - 6) Violation of copyright law.
  - c. Users may download files from the Internet if not otherwise prohibited. These files must be scanned for a virus using an antivirus program provided by MIS. Since only a small, uniform amount of system disk space is allotted to each user to hold files and electronic mail, stored information shall be kept to a minimum.
  - d. All users should receive training on Internet basics before using it, This includes information about electronic mail; telnet; anonymous ftp; use of listservs, mailing list, and discussion groups; use of Internet search engines; and features of Internet browsers.
6. The following guidelines apply to using email:
- a. No spamming or sending of bulk email.
  - b. No mail bombs, flames, or similar kinds of mail.
  - c. E-mail listservs/list subscriptions should be limited to those actually read. All files not read or no longer needed should be deleted.
  - d. File attachments that are sent via Internet should be smaller than 5MB to comply with size limitations on other systems, (This may still be too large for some systems).
  - e. The use of broadcast mail (sending the same note to groups of employees or students) will be selectively used for compelling mission-related or business reasons only.
7. The following guidelines apply to use of the World Wide Web:
- a. Web sites providing sexually explicit content shall not be visited.
  - b. Be judicious when it is necessary to fill out an on-line form, i.e., to register to use a specific web site.
  - c. Use of the World Wide Web should be limited to mission-related or business reasons and should not disrupt the workplace.
8. The following guidelines apply to use of File Transfer Protocol (FTP):
- a. Illegal copies of software shall not be obtained.
  - b. Licensed software shall not be distributed to others.
  - c. Attach only to systems for which an authorized login has been obtained.
9. The following guidelines apply to the use of Telnet:
- a. Login should be limited only to those systems for which an authorized login has been obtained.
  - b. Login as a "system administrator" or "supervisor" shall not be attempted unless the user is the authorized "system administrator" or "supervisor" for that system. This is considered a break-in attempt.

10. Suspected violations of this policy and guidelines should be reported to Security who will then contact the Risk Management Department. Risk Management will direct further action.

Affected Departments: All departments with email/Internet capabilities

Responsible Parties: All email/Internet users

JCAHO Standard: IM.2, IM.4