

HARDIN COUNTY GENERAL HOSPITAL ACCOUNTING POLICY

Title:
Policy Number:
Regulation:

Effective Date:
Med Staff:
Admin:

I. POLICY

Hardin County General Hospital provides Internet access to provide patient care, aid employees in performing their job duties, and offers Internet access to interested physicians as a job tool. The Internet provides a source of information from which almost every professional discipline represented in Hardin County General Hospital can benefit. Hardin County General Hospital believes use of the Internet can enhance the quality of care delivered, improve productivity, and increase customer satisfaction.

II. DEFINITIONS

1.0 Corporate Information – is information that is available to the staff of Hardin County General Hospital, but is not available to the general public. Information in this area may include strategic planning for Hardin County General Hospital, employee telephone extensions, corporate policies and procedures.

2.0 Encryption – Information that has been encrypted has been rendered unintelligible. The recipient must decrypt the information before the information would have meaning.

3.0 Highly Confidential Information - shall mean psychotherapy notes and the subset of protected health information that is related to:

1. Treatment of mental health and developmental disabilities;
2. Alcohol and drug abuse prevention and treatment;
3. HIV/AIDS testing;
4. Venereal disease(s);
5. Genetic testing;
6. Child abuse and neglect;
7. Domestic abuse of an adult with a disability; or
8. Sexual assault.

Individually Identifiable Health Information - shall mean information that is a subset of health information, including demographic information collected from an individual, and

1. Is created or received by a health care provider, health plan, or health care clearinghouse; and
2. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and
 - a. Identifies the individual, or
 - b. With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Internet or World Wide Web - The term Internet or World Wide Web (WWW or Web) is a collection of web pages that are developed in accordance with the hypertext markup language (HTML) format standard, and may be accessed via Internet connections using a Web browser.

Malware – Malware includes software that was developed for the specific purpose of causing harm to information systems or networks. This includes computer viruses, worms or trojans. Malware can cause information systems to shutdown, provide inaccurate information, or send information to an external unauthorized source.

Protected Health Information - shall mean the subset of individually identifiable health information that is (i) transmitted by electronic media; (ii) maintained in any medium constituting electronic media; or (iii) transmitted or maintained in any other form or medium. "Protected health information" shall not include (i) education records covered by the Family Educational Right and Privacy Act, as amended, 20 U.S.C. §1232g, (ii) records described in 20 U.S.C. §1232g(a)(4)(B)(iv), and (iii) employment records held by a covered entity in its role as employer. (Note that highly confidential information is a subset of protected health information.)

Remote Access Software – Remote access software is software that would allow access to information on the computer, or information that could be available to the user signed on to that computer from a place other than the computer. Information systems that are not in production may use this software for initial setup and installation under the supervision of the Information Technology Services staff. Web-Ex, PCANYWHERE, GOTOMYPC are all examples of remote access software.

Sensitive Information – Information which if improperly disclosed could cause damage to the reputation, privacy, image and/or financial viability of the patient, medical staff, employees, and/or Hardin County General Hospital. Sensitive information includes but is not limited to

1. Individually identifiable health information,
2. Patient billing information,
3. Employee information,
4. Proprietary products and product development,
5. Financial information,
6. Marketing and general business strategies,
7. Anything marked or stated as confidential.

Sexual Harassment – Sexual Harassment in the workplace is unlawful. Sexual Harassment is defined as unwelcome advances, requests for sexual favors and/or other verbal, written, visual or physical conduct of a sexual or sexually suggestive nature by employees, supervisors, management, medical staff, customers, visitors, volunteers, contractors, vendors, agents, or any other person where such conduct is either made in explicit or implicit terms as a condition of employment; used as the basis for employment decisions affecting employees; has the purpose or effect of substantially interfering with an employee's work performance; or creates an intimidating, hostile, or offensive work environment. This may involve the behavior of a person of either sex toward a person of the opposite or same sex.

Spyware – Spyware is software that was developed for the specific purpose of capturing information from the host computer. This may include keystrokes used, websites visited, or information accessed by the user.

Workforce - shall mean employees, volunteers, trainees and other persons whose conduct in the performance of work for a covered entity is under the direct control of such entity, whether or not they are paid by the covered entity. (A covered entity may treat an independent contractor that performs a substantial portion of his/her activities on the premises of the covered entity as a member of its workforce.)

III. RESPONSIBILITY

1.0 Authorized users of Hardin County General Hospital's Internet service – Users of the internet are responsible to use their access for the completion of job duties and in conjunction with the Mission and Values of Hardin County General Hospital. Particular attention should be paid to the values of stewardship and integrity. Users are to use the Internet in a manner that would not

violate federal, state or local laws, including copyright, anti-spam, etc. Users should take care to not expose the Hardin County General Hospital information systems to malicious software, such as malware, spyware, etc.

2.0 Information Technology department – The Information Technology department is responsible to allow access to the internet for members of the workforce who have completed the internet access agreement.

3.0 Management – Department managers, directors, and above are responsible for requesting access to the Internet for their employees. Requests must be made only when not having access to the Internet will prevent the employee from completing their job duties. Requests for Internet access should identify the business need for the requested access.

4.0 Physician Services – Directors and Managers group is responsible for the requesting of access and termination of access for members of the medical staff who purchase Internet services access as part of their service agreement.

IV. EQUIPMENT

1.0 Personal Computer connected to the Hardin County General Hospital network

V. PROCEDURES

INFECTION CONTROL: N/A

1. Need for access to Hardin County General Hospital internet, intranet, and e-mail usage will be determined at hire. If such need is determined access will be provided on an individual basis.

2. A copy of the Internet Access and Usage Policy will be provided to anyone Internet access has been requested for. The Internet Access Agreement form must be completed and returned as the written acknowledgement, stating that the user has read the policy, before access will be granted.

3. The following general guidelines identify acceptable use of the Internet when accessed through the

Hardin County General Hospital Internet connection:

3.1 Employees are accessing information to meet the requirements of their jobs. If the information will include patient identifiable information.

3.2 Participate in on-line group activities such as discussion groups that have a direct relationship to the user's job.

3.3 Authorized Internet users may access the Internet for non-job-related information provided
A. The access is done on the employee's personal time (before and after work, lunch breaks, or on days off).

B. Use of the equipment and/or Internet access does not interfere with normal Hardin County General Hospital operations, and

C. These policy guidelines are followed.

3.4 Managers will determine when their employees may use the Internet for personal use, as long as the personal use does not interfere with normal Hardin County General Hospital operations, and these policy guidelines are followed.

3.6 Authorized Internet users are not permitted to engage in the following activities at any time using Hardin County General Hospital equipment or facilities, or when using a Hardin County General Hospital Internet Address:

A. Access, download, print or anyway retrieve information that would be in violation of the Sexual Harassment policy.

- B. The use is contrary to the Hardin County General Hospital mission and values,
 - C. Engage in activities which would violate federal, state, or local laws.
 - D. Engage in personal commercial activities on the Internet, including offering services or merchandise for sale.
 - F. Send or receive information considered sensitive under the Confidentiality of Sensitive Information policy.
 - G. Allow access to a computer through the internet on the Hardin County General Hospital network through a remote access software.
- 4.0 Individuals using Hardin County General Hospital equipment to access Internet are subject to having activities monitored by the Information Technology Services department. Use of this system constitutes consent to monitoring.
- 5.0 Limited Information Technology Services personnel shall have unrestricted access to Internet and related information stored on corporate owned equipment. This access is required for reasons that include retrieving business-related information, trouble-shooting hardware and software problems, preventing unauthorized access and system misuse, assuring compliance with software copyright and distribution policies, and complying with legal and regulatory requests for information.
- 6.0 Use of sensitive information on the Internet
- 6.1 Employees of Hardin County General Hospital must use extreme caution when using the Internet in conjunction with sensitive information.
- 6.2 Employees may only transmit or retrieve information which has been approved by the director of the department, the Privacy Officer or his designee, and the Security Officer or his designee.
- 6.3 Transmission of sensitive information over the internet is only acceptable if the following encryption protections are used:
- A. Acceptable encryption algorithms include:
 - 1) Symmetric: Triple DES with 112 bit key
 - 2) Asymmetric: 1024 bit key (e. g. RSA)
 - 3) Elliptical Curve: 160 bit key
 - B. Encryption may be
 - 1) Hardware-based: Symmetric password “private” key devices such as link-encryptors
 - 2) Software-based:
 - a) Secure Sockets Layer (SSL) implementations at a minimum SSL level of version 3.0, standard commercial implementations of PKI, or some variation thereof, implemented in the Secure Sockets layer
 - b) S-MIME for encryption in the e-mail layer
 - c) Offline encryption/decryption of files at the user sites which are then attached to or enveloped (tunneled) within an unencrypted header and/or transmission
 - C. The recipient of the information has signed a nondisclosure statement, business associate language was included in the contract with the recipient, or the release is an allowable release as defined by the Health Insurance Portability and Accountability Act of 1996.
- 7.0 Tracking Abuse
- 7.1 Information Technology Services may perform random audits of visited Internet web sites. Suspected abuse will be investigated and brought to the attention of the Senior Management member responsible for the area where the incident occurred, along with copies of trace reports showing the web sites accessed. Abuse by physicians from hospital workstations will be brought to the attention of the Hospital Administrator.

7.2 Suspected abuse.

A. If an Internet user suspects that the security of their user account was breached, refer the Information Technology Services Password policy and request a new password.

B. If a internet user is suspected of breaching this policy, the following steps must be completed:

1) In the event that there is a suspected breach of this policy, the breach is to be reported to the Information Technology Services Compliance and Quality Assurance department. The report must be specific as to what type of abuse is suspected, the time frame the abuse occurred, and other specific details that will target the investigation.

2) The incident will be reviewed, and based on the situation, the Systems Administrator and CEO will give approval for specific review of the Internet access account, which is suspected of abuse.

3) The staff who is reviewing the internet access log will review only those sites accessed in the suspected time frame, suspected subject, and suspected internet user(s). Any Internet sites that are found to support the abuse will be forwarded to either the Systems Administrator and CEO.

8.0 Penalties for violations of this policy.

8.1 Employees.

A. Violation of the Internet Access and Usage policy will lead to the Improvement Counseling process and possible suspension of Internet access privileges.

B. Per the Improvement Counseling policy, Hardin County General Hospital management reserves the right to modify the improvement-counseling schedule to reflect extreme circumstances.

C. See Improvement Counseling policy for further information. (Policy number FR-HR-401)

8.2 Non-employees.

A. The Non-employees include all persons who are considered part of the workforce, but are not an employee of Hardin County General Hospital or are accessing the internet though the MSO arrangement with a doctor's office or clinic. This group includes volunteers, members of the clergy, physicians, contract employees, student trainees, interns, contractors, temporary employees, etc.

B. Hardin County General Hospital management reserves the right to modify the improvement counseling schedule to reflect extreme circumstances

C. Violation of this policy may also be a violation of federal or state law. Incidents may be reported to the appropriate law enforcement agencies.

VI. DOCUMENTATION

1.0 Internet access agreement signed by the user who will receive Internet access