

REFERENCE: AD1.0042 Communication Systems: Use

SCOPE:

This policy applies to Tomball Hospital Authority d/b/a Tomball Regional Hospital ("Tomball, Hospital or TRH") and any other entity or organization in which Tomball or affiliate owns a direct or indirect equity interest of 50% or more. In addition, this policy applies to any individual or entity that uses the facility's Internet connections.

PURPOSE:

This Internet policy is designed to help the employee and members of the Hospital's Medical Staff understand our expectations for the use of the Internet and to help the employee and Medical Staff member use the company's resources wisely.

POLICY:

It is TRH's policy to provide Internet access for official business and for limited personal use as deemed appropriate by the Department Manager and/or Administrative Officer. Employees using TRH's accounts are acting as representatives of TRH. As such, employees should act accordingly so as not to damage the reputation of the organization.

All existing company policies apply to this conduct on the Internet, especially (but not exclusively) those that deal with intellectual property protection, privacy, misuse of company resources, sexual harassment, information and data security, and confidentiality.

While our direct connection to the Internet offers potential benefits, it can also open the door to some significant risks to our data and systems if we do not follow appropriate security discipline. An Internet user can be held accountable for any breaches of security or confidentiality resulting from their use of the company's Internet connection.

PROCEDURE:

The User Access form (available as a WORD template - User Access form) must be signed by the employee and approved by the employee's Department Manager and/or Administrative Officer in order to continue or to gain access to the Internet.

- a. The signed/approved agreement must be submitted to Information Systems for processing.
- b. Information Systems will maintain the user access from until the user is no longer an employee of TRH.

The User Access form will provide acknowledgement of the following information:

- a. The employee's computer password is his/her own individual, personal code for gaining access into the Internet.
- b. The employee is responsible for notifying Information Systems in the event that his/her password is lost or its confidentiality has been breached, so that he/she may take appropriate action.

- c. If the employee shares his/her code, uses someone else's code, makes an effort to acquire other codes, or fails to comply with the above hospital policies, the employee will be committing a breach of hospital policy.
- d. TRH reserves the right to audit any and all activity an employee conducts while using the Internet service.
- e. TRH reserves the right to inspect any and all files stored in private areas of our network in order to assure compliance with policy.
- f. Any violation to policy will result in discipline up to and including termination.
- g. The terms of this policy and agree to abide by them.

Medical Staff Usage

Members of the Medical Staff may have access to the internet on Hospital's campus for professional use as it relates to patient care, medical research and for other uses as deemed appropriate by Hospital's Administrative team and/or Information Systems provided that:

1. Such access is provided from within the facility or remotely through a protected method such as a VPN and is readily available to such physicians
2. Such access does not permit physicians access to restricted Hospital Information;
3. Notices are posted at the relevant terminals advising that the access is for use related to the delivery of medical services at the facility only (e.g. research and review of relevant periodicals, studies and other clinical information);
4. Such internet access is offered to all medical staff members without regard to the volume or value of referrals or other business generated by the physician for the Hospital;
5. Such access is reasonably related to the provision of, or facilitates the delivery of, medical services at the Hospital;
6. Such access is not offered or provided in exchange for the referral of business that is paid for by federally-funded payers; and
7. Any remote access from outside the Hospital is only for the purpose of accessing Hospital medical records or information or to access patients or personnel who are on the Hospital campus.

Audits will be conducted of the use of the medical staff and any inappropriate use by the physician, or their office staff, may result in the termination of the internet service.

Malicious and Inappropriate Software

The introduction of viruses, or malicious tampering with any computer system, is expressly prohibited. Files that are downloaded from the Internet must be scanned with virus detection software before installation or execution. All appropriate precautions should be taken to detect for a virus and, if necessary, to prevent its spread. The

display of any kind of sexually explicit image or document on any of our computer systems is a violation of our policy on sexual harassment. In addition, sexually explicit material may not be archived, stored, distributed, edited or recorded using our network or computing resources.

Cyber law

Unless otherwise noted, all software on the Internet should be considered copyrighted work. Therefore, employees are prohibited from downloading software and/or modifying any such files without permission from the copyright holder. Any infringing activity by an employee may be the responsibility of the organization. Therefore, this organization may choose to hold the employee liable for their actions. Employees shall not place company material (copyrighted software, internal correspondence, etc.) on any publicly accessible Internet computer without prior permission. The organization's Internet access and computing resources must not be used to violate the laws and regulations of the US or any other nation, or the laws and regulations of any state, city, province, or the local jurisdiction in any material way.

Confidentiality

The Internet does not guarantee the privacy and confidentiality of information. Sensitive material transferred over the Internet may be at risk of detection by a third-party. Employees must exercise caution and care when transferring such material in any form. The truth or accuracy of information on the Internet and in email should be considered suspect until confirmed by a separate (reliable) source.

Alternate Internet Service Provider connections to TRH's internal network are not permitted unless expressly authorized and properly protected by a firewall or other appropriate security device(s). The Director of Information Systems must authorize the connection prior to implementation.

ENFORCEMENT:

Failure to adhere to the terms of this policy will be referred to the Hospital's Director of Information Systems or his/ her designee, the Legal Services Department and/or the appropriate administrator and shall result in appropriate human resources action up to and including termination. Failure to adhere to the terms of this policy will also be a factor in determining individual performance evaluations.

TOMBALL REGIONAL HOSPITAL
SUBJECT: **INTERNET: USAGE AND ACCESS**
IMPLEMENTED: 05/00
REVIEWED:
REVISED: 05/03, 08/07, 07/09

POLICY
EXPIRES: 08/10
PAGE 4
CI1.0007.008

CI1.0007.008 **INTERNET: USAGE AND ACCESS**

COMPLIANCE: All Departments