Tift Regional Medical Center

Policy & Procedure

	Policy Manual
Effective Date: September 28, 2001 Title: Communication Systems (Email, Voice Mail, Electronic Devices and the Internet)	☐ HIPAA ☐ Infection Control ☐ Departmental ☐ Patient Care Manual ■ Administrative _____ Approval / CEO

Purpose:
The purpose of this policy is to provide guidance on the usage of communication systems at Tift Regional Medical Center including but not limited to email, voice mail, electronic devices and the internet.

Policy:
Tift Regional Medical Center ("TRMC") provides electronic mail, voice mail, electronic devices and Internet access to promote and support its mission. All such communications systems are the property of TRMC and are to be primarily used for business purposes. Highly limited reasonable personal use of the systems is permitted; however, you should assume that these communications are not private. Patient or confidential information should not be sent through the Internet until such time that its confidentiality can be assured.

The Internet access, electronic devices, e-mail, and voice mail are intended for business purposes during business hours.

Employees and others with access to these services must use them responsibly and consistent with their job duties and TRMC's mission.

Along with pagers, printed memos, and other correspondence, voice mail and e-mail comprise the accepted forms of inter-departmental communication.

Employees may not use internal communication channels or access to the Internet at work to post, store, transmit, download, or distribute any proprietary data, trade secrets, or other confidential information. Further, employees may not post, store, transmit, download, or distribute any threatening; knowingly, recklessly, or maliciously false; or obscene materials including anything constituting or encouraging a criminal offense, giving rise to civil liability, or otherwise violating any laws. Additionally, these channels of communication may not be used to send chain letters, personal broadcast messages or copyrighted documents that are not authorized for reproduction; nor are they to be used to conduct a job search or open misaddressed mail.

TRMC's communication systems cannot be utilized to engage in any type of unethical, illegal, or in any conduct which violates TRMC's Code of Ethics or Corporate Compliance Program.

It is each department manager's responsibility to make available and utilize voice mail and e-mail within his/her department. Voice mail and e-mail must be checked periodically throughout the day. These messages must be secure and confidential. Employees without individual computers are required to go to a designated

computer station at least twice-a-week to log-on and read the latest TRMC information sent via e-mail or posted on the employee intranet.

TRMC, as the owner of the systems, reserves the right to, but does not have the duty to, periodically access, monitor and disclose the contents of internal e-mail, Internet e-mail and voice mail messages. TRMC disclaims responsibility for the content of e-mail sent out on the electronic mail system. TRMC does not intend to screen messages in advance and cannot be responsible for their content.

Because computerized information can be vulnerable to unauthorized access, employees must take special care when using e-mail to convey sensitive information of any kind. Routinely deleting documents and limiting the forwarding of messages to other users can help protect but do not assure the privacy of information.

Employees who abuse the communications systems or use them excessively for non-business purposes may lose these privileges and be subject to disciplinary action up to termination.

For complete information, see the complete policy which follows.

Procedure:

Guiding Principles
TRMC's visibility on the Internet is rapidly increasing both inside and outside TRMC.

Not all the dos and don'ts nor every circumstance for using these resources can be addressed specifically. Your best guide to appropriate work-related uses of the Internet and LAN will be your manager. In addition to your manager, employees should also adhere to the guidelines listed below, which relate to the Internet and LAN specifically. Finally, your own common sense and sound business judgment should guide your behavior, both in terms of the content of your usage, as well as the impact of the usage on your own productivity.

Your first obligation is to protect TRMC information assets. Generally, all servers being put on the Internet for access by non-TRMC employees must be approved by TRMC management with appropriate safeguards to protect intellectual property and confidential patient data. All LAN or other network servers must also be approved by TRMC management with appropriate safeguards to protect TRMC intellectual property.

Here are the basic principles to follow when accessing the Internet or LAN:
- Adhere to TRMC's policies.
- Use only services you have authorization to access.
- Always represent yourself as yourself, never as someone else.
- Do not store or send unencrypted TRMC, confidential information, proprietary data or trade secrets.
- Ensure that any software placed on the Internet or LAN complies with applicable licensing agreements and copyrights.
- Always comply with applicable licensing agreements and copyrights when downloading software from the Internet and/or placing it on the LAN.
- Do not post, store, transmit, download or distribute on the Internet or LAN any materials that could be considered inappropriate, threatening, obscene, offensive or disrespectful to others and do not access such material.
- Do not send or forward TRMC internal electronic mail through the Internet to parties outside TRMC.

Use of Online Resources

When an employee connects to the Internet using the TRMC address designations, it should be for TRMC business-related activity only or for other purposes authorized by management. TRMC contractors can use the Internet or LAN for TRMC business purposes to the extent needed to conduct a stated assignment, but usage must be with Tift Regional management approval. A TRMC employee's use of the Internet or LAN for personal reasons may be approved by the employee's manager, if such use is clearly insignificant, does not interfere with or compete with TRMC business or the employee's job, and does not involve any incremental cost to TRMC.

Prohibited Uses

Employees in general should remember that the Internet and LAN are business productivity tools that should enhance their productivity, not detract from it.

Specifically, the Internet and LAN should not be used for:

- Sending or replying to chain letters;
- Distributing or obtaining threatening, obscene, offensive or inappropriate materials;
- Personal gain, profit or advancement of personal views;
- Representing oneself as someone else;
- Engaging in unethical, illegal or any other conduct which violates TRMC's Code of Conduct or Compliance Program;
- Solicitation of other TRMC employees;
- Giving others outside Tift Regional information about or lists of TRMC employees for commercial solicitations or any other purposes;
- When it interferes with your job or the jobs of other employees; or
- When it interferes with the operations of Internet gateways.

Also, employees should avoid accessing material that could embarrass TRMC or could be considered objectionable in the workplace. Examples include Web sites that contain nudity, sexually explicit material, those that advocate illegal activity or intolerance of others.

Your rule-of-thumb should be that if the material is something TRMC would not put in its publications or post in its visitor lobbies, you probably should not distribute or obtain it through the Internet or LAN.

If you still have questions concerning whether or not material is offensive or inappropriate, discuss your concerns with your manager, human resources or call the Compliance Helpline.

Classified Data

Material classified as TRMC Confidential must not be stored or sent on the Internet and must be stored in confidential, password-protected areas on LAN with access allowed based on a need to know, not want to know basis. Management can make exceptions for access to confidential material when data encryption is used or when appropriate contracts are in place with the information recipients. If you receive another company's classified data from the Internet you must comply with that company's requirements for protecting the data either for your own use or placement on LAN. Any questions concerning protection of non-TRMC information should be discussed with your manager or with the Director of MIS.

Login Passwords and Security

Your network LOGIN and password are your entry into the TRMC network, and they must be protected. Please refer to "Password Management" HIPAA Compliance Policy.

Downloading Materials from the Internet

Most information and software that is accessible on the Internet is subject to copyright or other intellectual property right protection.

Materials distributed over the Internet in the form of shareware or freeware often come with requirements or limitations (e.g., some are not to be used for commercial purposes and you cannot charge others for use or distribution; some are subject to having a copyright or attribution notice affixed to each copy; etc.). If such terms are applied, you must read and understand them before downloading the software and make a copy of the terms, if possible. If you think that TRMC will not be able to comply with any of the terms, do not download the material. If you are unsure about the meaning of the restrictive language or have questions about it, request that the Director of MIS review it before downloading or using the material. TRMC employees must seek assistance and approval from TRMC legal counsel before incorporating any material downloaded from the Internet (or any external online service) into LAN or into any product or material that TRMC intends to distribute externally. When downloading software as a courtesy to others, try to do large file transfers during non-peak hours for the server.

Electronic Mail

Electronic mail is the most commonly used facility on the Internet. TRMC maintains an e-mail system to assist in the conduct of its business. The system is not intended to be used for personal business. Also, the e-mail system hardware is TRMC property. All messages composed, sent or received on the system are the property of the TRMC, not the private property of an employee.

When using the e-mail system, keep the following guidelines in mind.

• All TRMC employees who have e-mail are responsible for any communication sent to them via e-mail.

• Employees should not automatically forward e-mail to an Internet site - this includes forward files. Also, don't use auto-reply functions such as IAMAWAY or DELEGATE for replying to Internet mail (this can cause major problems for mailing lists and is considered bad form on the Internet).

• You should not send unsolicited advertising via e-mail. This means that if people use your Web site and you record their address, you shouldn't use this for sending out advertising. Only send e-mail advertising to those users who specifically request it.

• E-mail may not be used to solicit for commercial ventures, religious or political causes, outside organizations or other non-job-related solicitations.

• The e-mail system is not to be used to create offensive or disruptive messages, such as those that contain sexual implications, racial slurs, gender comments or any other comment that offensively addresses someone's age, sexual orientation, religious or political beliefs, national origin or disability.

• The e-mail system is not to be used to send (upload) or receive (download) copyrighted materials, trade secrets, proprietary financial information or similar materials without prior authorization.

• The confidentially of any message should not be assumed. Even when a message is erased, it is still possible to retrieve and read that message. Further, the use of passwords for security does not guarantee confidentiality. All passwords must be disclosed to Tift Regional or they are invalid and cannot be used.

TRMC reserves the right to review, audit, intercept, access and disclose all messages created, received or sent over e-mail for any purpose. The contents of electronic mail, properly obtained for legitimate business purposes, may be disclosed within TRMC without the permission of the employee. TRMC disclaims responsibility for the content of e-mail sent out on the electronic mail system. While TRMC reserves the right to discipline any user for inappropriate use of the e-mail system, it does not intend to screen messages in advance and cannot be responsible for their content.

• Notwithstanding TRMC's right to retrieve and read any e-mail messages, such messages should be treated as confidential by other employees and accessed only by the intended recipient. Employees are not authorized to retrieve or read any e-mail messages that are not sent to them. Exceptions require prior approval by the employee's manager.
• Employees should not use a code, access a file or retrieve stored information unless authorized to do so and they should not attempt to gain access to another employee's messages without the latter's permission.
• Any employee who discovers a violation of this policy should notify human resources.
• TRMC intends to honor the policies set forth here but reserve the right to change them at any time as required under some circumstances.
• E-mail which is necessary to maintain for record-keeping requirements or documentation must be printed in hard copy form and filed in the appropriate hard copy file. All e-mails must be deleted within three months or moved to a folder and deleted from the in-box and deleted items box.

Because computerized information can be vulnerable to unauthorized access, employees must take special care when using e-mail to convey sensitive information of any kind. Routinely deleting documents and limiting the forwarding of messages to other users can help protect but not assure the privacy of information. Most e-mail documents are subject to discovery in legal proceedings to the same extent as hard copies. By transmitting a message via e-mail, a user may in fact be deemed to have waived certain confidentiality protections that would otherwise be available. In addition, highly sophisticated technologies for salvaging records can frequently make even "deleted" records available for inspection.

Voice Mail
The Voice Mail system provided for use by TRMC employees is the property of TRMC. All TRMC employees are responsible for any communication sent to them via voice mail. They should be responded to and deleted weekly. Limited personal use of the system is permitted; however, you should assume that these communications are not private. The Voice Mail system should not be utilized to engage in any type of unethical, illegal or in any conduct which violates TRMC's Code of Ethics or Corporate Compliance Program. TRMC, as the owner of the system, reserves the right to, but does not have the duty to periodically access, monitor and disclose the content of voice mail.

Electronic Devices
All electronic devices (phones, ipods, mp3 players, etc) that are not issued to an employee by TRMC must always be turned off and stored off your person out of sight during normal business hours.

Discipline
Any employee who violates this policy or uses the communication system for improper purposes shall be subject to discipline, up to and including termination. If necessary, TRMC will advise appropriate legal officials of any illegal violations.

Review/Revise History:
February 2010 (Replaces "*Usage of Communication Systems (Email, Voice Mail, and the Internet*")
August 2012