TRIHEALTH, INC.
CORPORATE POLICY

TITLE: TriHealth Electronic Mail Email Use	
SECTION: 05	**POLICY NUMBER: IS01.00**
EFFECTIVE DATE: 01/1999	**REVIEWED/REVISED DATES: 02/2001, 01/2004, 09/2007, 01/2011, 11/2012, 05/2017**
AFFECTED AREAS All TriHealth Entities including McCullough-Hyde Memorial Hospital This policy acknowledges that other relevant and applicable policies and procedures exist that have been drafted, approved, and adopted by entities (and departments) within TriHealth and are specific to those departments or entities. Interpretation of these other policies must comply with the principles adopted by Corporate Policy #12_01.00, "Corporate Policies, Development & Implementation".	
POLICY OWNER: Manager, Information Systems Security	
APPROVED BY: **Sr. VP & Chief Information Officer** **Executive VP System Development** **Corporate Policy & Procedure Committee** **President of Health Services & System COO** **President & CEO**	

PURPOSE

The purpose of this policy is to define guideline for the appropriate use of all TriHealth Email systems, specifically all computers, computer networks, Email systems, telecommunication systems, and software developed by or licensed to TriHealth, Inc.

BACKGROUND

√ TJC Std: IM.02.01.03; IM.02.01.01

□ Licensure

□ Regulatory Agencies

□ Other: Electronic Communications Privacy Act of 1986

POLICY/PROCEDURE

TriHealth, Inc. systems, network, and facilities are intended for TriHealth, Inc., business use by employees, physicians, team members and other agents. The use of electronic forms of communication and information exchange is necessary in everyday business affairs. Employees, physicians, and other agents of TriHealth, Inc. may have access to TriHealth, Inc. Email systems to conduct TriHealth business.

The following applies to all Email systems that are:

- Accessed on or from TriHealth, Inc., premises or affiliated sites utilizing TriHealth resources.
- Accessed using TriHealth, Inc., computer equipment and/or mobile devices.
- Used in a manner that identifies the individual with TriHealth, Inc.
- Accessed using non-TriHealth owned devices or accessed from remote locations (not on TriHealth Premises).

This Policy ASSUMES that the disclosure of PHI (Protected Health Information) by fax or Email is done properly pursuant to TriHealth policies #08_HIPAA_01and #05_MR02.00. All TriHealth employees are encouraged to review these policies and/or consult with his/her manager/supervisor if, prior to any release of PHI, there is a question regarding the propriety of the disclosure.

1. TriHealth departments will make reasonable efforts to protect privacy and confidentiality of PHI faxed or emailed to addresses internal or external to TriHealth.

2. All faxes and emails should be limited so that the PHI being disclosed is the minimum necessary to accomplish the intended purpose of the disclosure or request; **EXCEPT** disclosures to another health care provider for treatment purposes. In the case of disclosures to another health care provider for treatment purposes, all PHI that is requested should be disclosed.

Minimum necessary means no more than the specific information needed by the recipient to serve the purpose(s). If a TriHealth employee has a question as to what is being requested, he/she should clarify the request. The minimum necessary standard protects against unsolicited requests for PHI regardless of whether the information is approved for disclosure or not.

TriHealth, Inc. reserves the right to inspect and monitor the use of its Email systems and all other electronic communication systems at any time and without notice to the extent necessary to ensure that Email systems are being used in compliance with the law and with this and other policies. All users of TriHealth Email systems expressly waive any right of privacy for any email sent or received through TriHealth Email systems. TriHealth, Inc. wants the employee or the agent of TriHealth, Inc., to be aware that its

security systems are capable of recording (for each employee or agent of TriHealth, Inc.,) Email messages into and out of its internal networks, and it reserves the right to do so at any time, however is under no obligation to do so. All communications including text and images can be disclosed to law enforcement or other third parties without the prior consent of the sender or receiver.

Only authorized personnel, with a need to know, are permitted to access, view, or possess TriHealth information. It is the responsibility of the data owner to determine which personnel have a need to know.
PHI or sensitive information may be sent utilizing ProofPoint Email encryption service. To use the encryption service, the phrase, "PHISECURE" must appear anywhere in the subject line of the email. The subject line itself is not encrypted and must not contain any PHI or sensitive information. The Email contents and any attachments will be encrypted. Specific instructions on using encryption and recipient retrieval instructions can be found on LinkNet.

Employees may not at any time Email information to themselves at a personal Email account so that the data can be accessed, worked on or retrieved later from a non-TriHealth Email account.

Electronic mail and services should not be used in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system (i.e., chain letters or mass copying of any types of letters that have no business purpose).

TriHealth currently employs filtering software to block Email spam. Users are responsible for keeping his/her Email “inbox” clean of spam. Spam could be any Email that is unsolicited from an outside entity. While the filtering software will block most spam, if a user receives spam Email, the user can drag that Email to the spam folder. This will mark future Email similar to the one that was received as spam. Also, a user has the ability to block Email from a specific user by opening the message and clicking a box labeled “block sender.” It is forbidden for any individual or organization to use any TriHealth computing or network resources for sending or forwarding unsolicited bulk email, also known as “SPAM.”

Email must not be used for knowingly transmitting or sending any communications of a discriminatory or harassing nature, or which are derogatory to any individual or group, obscene or X-rated communications, or are of a defamatory or threatening nature, or of any offensive messages, including offensive comments about race, gender, disabilities, age, sexual orientation, pornography, religious beliefs, or national origin; or for "chain letters," or for solicitation, or for any other purpose which is illegal or against TriHealth, Inc., policy or contrary to the interest or values of TriHealth, Inc. Employees who receive any emails with such content from any TriHealth employee or agent of TriHealth must report the matter to his/her manager and/or supervisor immediately.

No Email may be sent that attempts to hide the identity of the sender, or represents the sender as someone else or from another company. Employees or agents of TriHealth, Inc. are advised to use Email with the same awareness as they would use with a more permanent communication medium such as a memorandum or letter. Blind carbon copy (Bcc:) should not be used for TriHealth business. Blind carbon copy suggests inappropriate activity. Email conversations should be kept to thoughts that would normally be expressed to the recipients in person and kept at a minimum.

TriHealth does not maintain archives of Email. Items in the Microsoft Outlook "Deleted Items" and "Sent Items" folders are removed automatically after60 days. Emails in the Microsoft Outlook "Personal Folders" are saved in the user's home directory until the user actually deletes the Email.

Copies of Email may not be kept in ".PST" files that are stored on any workstation, laptop, PC, or portable device. All copies of Email must be stored in the users "H" drive or "home directory."

Email messages are not to be considered secure especially those sent to or from external parties. All TriHealth employees should be made aware of the security risks associated with Email as part of the TriHealth Security Awareness and Training Program (08_HIPAA13.00).

Under no circumstances may personal Email accounts be used for TriHealth business (i.e. Yahoo Mail, AOL, Hotmail, Gmail, etc.). Employees and agents of TriHealth may not send or reply to emails using personal Email accounts to conduct TriHealth Business, especially if the Email contains PHI and / or sensitive information. These types of Email are not secure.

Anyone obtaining electronic access to other companies' or individuals' materials must respect all copyrights and may not copy, retrieve, modify or forward copyrighted materials except as permitted by the copyright owner. Email containing trade secret/proprietary information may not be forwarded without the permission of the sender. Users must treat all Email attachments with caution. Users should always question the validity of the attachment, especially if it was not expected. Users should understand the risks of viruses and worms, and how they can use the internal address book to masquerade as a valid email from a known sender. Users should delete any Email that is considered to be malicious. Technology and processes are in place for blocking dangerous attachments and links. The technology is no substitute for individual vigilance on opening email and attachments or clicking links that are suspicious. .

Users should be aware of virus hoaxes. Email messages can falsely warn the user about a virus and then give potentially system-damaging advice on how to remove it.

Awareness training will be provided for new employees through a combination of Human Resources orientation and security awareness articles on LinkNet.

Communications on suspicious email awareness will be sent to users on a periodic basis.

Content filtering of Emails is used at TriHealth. The local administrator is responsible for a periodic maintenance or update of this word list used for filtering. The Email filtering engine is capable of scanning for malicious code.

Employees or agents of TriHealth, Inc. should use good judgment in forwarding Email to any other person or entity. When in doubt, request the sender's permission to forward the message. All messages written by others should be forwarded "as-is" and with no changes, except where edits are clearly indicated. With the tremendous growth rate of dangerous viruses, it is important to be aware of the source of the message. Do not open attachments from unknown sources; when in doubt; escalate to the Customer Support Help Desk and/or Information Systems Security.

All communications sent by employees or agents of TriHealth, Inc., must comply with this and other company policies. Employees or agents of TriHealth, Inc., may not disclose any confidential or proprietary company information. Email is not a secure form of communication and is used at sender's risk. All disclosures of Protected Health Information (PHI) sent via Email must conform to the guidelines set forth in the Transmitting Protected Health Information (PHI) Via Facsimile or Electronic Mail (Email) Policy (#08_HIPAA05.00).

Email signatures for new messages are to be standardized across TriHealth, Inc. A standard, consistent and clean email signature will present a professional appearance for the TriHealth brand. The signature is designed to maximize contact information, promote TriHealth.com, and reinforce the TriHealth brand both internally & externally.

Standard email template:

--

Your Name | Your Title

Office 513 123 1234 | Cell 513 123 1234 | Fax 513 123 1234

your_email@trihealth.com

Your Location

Facility Address, City, OH #Zip#

TriHealth.com | Facility Main Phone

Instructions on creating the email signature can be found on LinkNet or at TriHealth.com/Employee Signature.

All requests for exceptions and changes to the standard email format must be submitted in writing to TriHealth Marketing Communications and approved by the Executive Director of Marketing Communications.

Additionally, no page templates, backgrounds, font changes or other customizations may be made from the Outlook defaults.

See Email Etiquette on LinkNet, New to Email, for additional Email usage guidelines.

ANY EMPLOYEE OR AGENT OF TRIHEALTH, INC. FOUND TO HAVE VIOLATED THIS POLICY, BREACHED CONFIDENTIALITY OR ABUSED THE PRIVILEGE OF TRIHEALTH, INC., ACCESS TO INFORMATION TECHNOLOGY RESOURCES WILL BE SUBJECT TO THE PERFORMANCE COUNSELING POLICY.

OTHER AREAS/POLICIES OR PROCEDURES OF REFERENCE

Access to TriHealth Information Technology Resources
Software Copyrights
Internet/Intranet Acceptable Use
HIPAA: Transmitting Protected Health Information (PHI) Via Facsimile or Electronic Mail (Email)