Methodist College UnityPoint Health	Page # 1 of 5	Section: A	Policy #: A-69
	Approval: Dr. K.Q.A.		Date: 08/15 Review by: 08/18
	Date Revised: 08/15		
	Policy/Revision Submitted by: Dr. Matthew Hertzog		

SUBJECT: **Electronic Messaging**

I. POLICY:

All electronic messages created, sent, or retrieved from or through the College or the UnityPoint Health system in the course of patient care at UnityPoint Methodist-Proctor, payment for College operation, or research conducted at any UnityPoint Health affiliate, are the property of UnityPoint Health and/or the College. Users of the College/UnityPoint Health systems should have no expectation of or right to privacy in any type of electronic message. All use of electronic messages must comply with the College electronic messaging procedures and rules wherefore mentioned.

II. GENERAL INFORMATION:

DEFINITION: Electronic messages include e-mail, text messages, instant messages, and all other types of digital communications messages that travel through telecommunications networks.

BACKGROUND: The purpose of this policy is to:

- Protect the College, its personnel, its students, and its resources from the risks associated with the use of electronic messages.
- Define appropriate rules for secure use of electronic messaging systems, including access and use from home or other secure external locations.
- Describe the expectations of professional conduct associated with the use of the electronic messaging systems.

POLICY RULES:

1. Purpose of Electronic Messaging Systems. The College's electronic messaging systems (i.e. email) and all electronic messages passing through or stored within the systems are the property of the College and UnityPoint Health and should be used as a business tool to facilitate communications and to exchange information needed in the performance of college related duties. The electronic messaging systems are to be used for appropriate college purposes.

2. User Privacy and Monitoring. The College and/or UnityPoint Health reserve the right to monitor and/or access electronic communications sent to or received from any internal or external source in specific instances in which there is good cause. Good cause shall include, but not be limited to, the need to protect system security, fulfill College and/or UnityPoint Health obligations, detect

wrongdoing, comply with legal process, or protect the rights or property of the College.

Monitoring of electronic communications will be conducted by the College's IT Department in conjunction with UnityPoint Health's Information Protection Department after consultation and approval from the UnityPoint Health General Counsel's Office and the College's Human Resources Department.

2.1 Electronic communications might be forwarded, intercepted, printed, and stored by others. Thus, unless secured following the College's encryption standards (in conjunction with UnityPoint Health's system policies), electronic communications should only be used for communications that would be appropriate to enter into the public record.

2.2 Electronic communications may be discoverable in the event of litigation. As with any type of business communication, users are expected to conduct themselves in a professional manner.

2.3 Electronic communications content is occasionally visible to IT staff engaged in routine testing, maintenance, and problem resolution. IT staff assigned to carry out such assignments will not intentionally seek out and read, or disclose to others, the content of electronic messages, unless in the course of performance of this Policy, IT staff becomes aware of information that violates this Policy, then IT staff may report the violation(s) pursuant to this Policy.

2.4 College related e-mail messages remaining in terminated user accounts may be transferred to other users if approved by the College's Director of Information Technology and/or the Director of Human Resources.

3. Rules for Electronic Messaging. Users of the electronic messaging systems are responsible for the following:

3.1 Keeping e-mail, as well as network passwords confidential.

3.2 Refraining from setting an automatic forwarding rule that sends all e-mails to an external e-mail account.

3.3 Identifying the sender clearly and accurately. E-mail users are responsible for all communications originating from their e-mail accounts, including the content of all text, audio, or images sent over the UnityPoint Health e-mail system. No e-mail may be sent that hides the identity of the sender or represents the sender as another person, unless authorized by that person.

3.4 Respecting and maintaining the integrity of the original e-mail author.

3.5 Taking reasonable precautions to avoid introducing viruses and other types of malicious software (malware) in the UnityPoint Health networks and systems. Such precautions include, but are not limited to, the following:

3.5.1 Users should not open any unexpected e-mail messages with attachments. If the validity of such e-mail messages and attachments cannot be obtained from the sender, the user is required to contact the College's IT Department for assistance. Under no circumstances should the user forward the email to any other College or UnityPoint Health user.

3.5.2 Users should not click on links within e-mail messages coming from unknown senders, or messages that seem uncharacteristic from known senders.

3.6 Adhering to Policy A.IT.09, Remote Access, when accessing the College/ UnityPoint Health e-mail system from home or other secure external locations.

3.7 Submitting spam e-mails (unsolicited/unwanted commercial e-mails) received in your inbox to the College IT Department for analysis.

3.8 No confidential patient information is to be sent via e-mail. Under no circumstances should patient identifiable information be included in any email sent from student users.

For Text Messages

3.9 Clear text (un-encrypted) sensitive information, such as protected health information or student identifiable information may not be sent within text messages.

For Other Types of Electronic Messages

Methodist college of UnityPoint Health students must follow the rules as applicable to the technology and according to the guidance provided by the College IT Department.

4. Rules for Electronic Messages with Protected Health Information.

4.1 All College electronic message communications must comply with College policies and must not disclose any confidential or proprietary information unless permitted by this College policy.

4.2 Authorized College and UnityPoint Health personnel will regularly perform checks to ensure electronic messaging rules are being correctly applied and consistently followed.

5. Prohibited Uses of Electronic Messages. Electronic messages must never be used in any of the following ways:

5.1 To send patient information, sensitive College or UnityPoint Health information, or confidential information outside of UnityPoint Health via electronic messages.

5.2 For any purpose which is illegal, against College or UnityPoint Health policy, or contrary to the best interest of the College.

5.3 To engage in any communication that is threatening, defamatory, obscene, offensive, abusive, sexually explicit, libelous, or harassing.

5.4 To copy or transmit any document, software, or other information protected by copyright and/or patent law, without proper authorization by the copyright or patent owner.

5.5 For charitable, non-charitable, or commercial solicitation or business interests unrelated to the College or UnityPoint Health.

5.6 To forge electronic messages.

5.7 To disrupt or disable the electronic messaging systems.

6. Violations.

6.1 Violations of this Policy will be reported to the appropriate College managers, the College Director of Information Technology, the College President, and the College's Director of Human Resources according to the College's IT Department's electronic messaging monitoring procedures.

6.2 Inappropriate use of electronic messages or systems may result in disciplinary actions at the department level, immediate revocation of access to the electronic messaging systems, and/or dismissal from the College.

6.3 Criminal misconduct in the use of electronic messaging systems may be disclosed to the appropriate authorities and may result in prosecution under local, state, or federal law.

6.4 Any suspected violations of this Policy should be reported to the College's Director of Information Technology and/or the appropriate manager.