 <b>Methodist College</b> <b>UnityPoint Health</b>	<b>Page # 1 of 1</b>	<b>Policy #: S-82</b>
	<b>Approval:</b> <i>Dr. Deborah R. Garrison</i>	<b>Date: 07/2008</b> <b>Review by: 07/2020</b>
	<b>Date Revised: 07/08, 03/12, 8/15, 07/17</b>	
	<b>Policy/Revision Submitted by: Dr. Pam Ferguson</b>	
	<b>Location: FH, SH</b>	
<b>SUBJECT: Client Confidentiality</b>		

**I. POLICY:**

Through the various educational experiences, nursing students are privileged to confidential information.

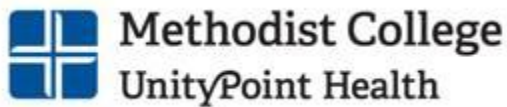
**II. GENERAL INFORMATION:**

As pre-professionals students must adhere to the professional behaviors as directed by the program’s professional code of ethics (ex. American Nurses Association Code of Ethics for Nurses with Interpretive Statements) which include maintenance of confidentiality and requirements documented in the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

MC students may not disclose any information regarding clients, their families or information pertaining to clinical agencies outside of that specific care giving experience.

Every MC student will be required to sign the “Student Confidentiality Form” at the beginning of the first clinical course. The confidentiality policy will be re-emphasized in each subsequent clinical course.

The signed “Student Confidentiality Form” will be kept in the student’s health record file in the Enrollment Management Office.



**METHODIST COLLEGE  
STUDENT CONFIDENTIALITY FORM**

As a Methodist College student and pre-professional, I must not disclose or release any Health Insurance Portability and Accountability Act of 1996 (HIPAA) Protected Health Information (PHI) to unauthorized individuals during or after the time I attend Methodist College.

I understand that PHI includes personal, financial, and medical information and can be in the form of verbal, written, electronic or video communication and include external storage such as CDs, Jump Drives, or Cloud storage.

I understand that I cannot share my secure login information with others. I also understand that I must only use my student login for all student-related activities.

I understand that I am not allowed to access my personal medical information or that of friends/ family using my student access.

I understand that I am not allowed to access PHI for any persons for whom I am not directly providing care.

I understand I am not allowed to copy, paste, print, or photograph PHI from electronic medical records including EPIC. During my clinical experience on the unit, the nursing staff may provide me with written PHI. I will ensure that the nurse will retain possession of these materials for proper care and disposal.

I understand that I am not allowed to post PHI or clinical experiences on social media. I will not post information regarding clinical experiences, including general statements about the experience and/or photographs on social media

I understand that an unauthorized disclosure, whether intentional or unintentional, is unlawful. If I disclose confidential or privileged information to unauthorized individuals or businesses without proper authorization, I may be subject to legal action for monetary damages and/or relief sought by the person aggrieved by the disclosure. I further understand that, if I am found in violation of this policy, I will be subject to disciplinary action up to and including dismissal from the College.

My signature below indicates that I have read and understood the following policies:

- S-82 Client Confidentiality
- E-09 Health Insurance Portability and Accountability Act

\_\_\_\_\_  
Student Signature

\_\_\_\_\_  
Date

## Student HIPAA and Confidentiality

### **What is HIPAA?**

The Health Insurance Portability and Accountability Act (HIPAA) is an important federal law that covers the privacy and security of protected health information (PHI). Compliance with this federal law is important. Intentional and non-intentional violations can result in fines and criminal penalties to the organization and the INDIVIDUAL (You).

### **Am I required to follow the HIPAA law?**

Yes. All persons within a healthcare organization are required to follow the law. This includes doctors, nurses, students, volunteers, social workers, clinicians, non-clinical staff (EVS, Registration, Billing) and unlicensed assistive personnel (C.N.A, M.A, PCT).

### **What is covered under Protected Health Information?**

The following are covered items and formats:

- Personal Information (Name, address, email address, phone number, photographs)
- Financial Information (Social Security Number, Insurance Account Information)
- Medical Information (Medical Record Number, Account Number, Admission Date, Discharge Date).
- Spoken/Verbal
- Written
- Electronic
- Video
- CD
- Jump Drive

### **As a student, when can I use patient information?**

You may only use the information in the process of doing your job, in this case your student work. This includes during the clinical experience, post conference debriefing, and completion of assignments for the purpose of education. You may only share with the faculty member and clinical group. It is your responsibility to de-identify the patient and to protect all information from unauthorized access.

### **What can I do to protect from a breach of information?**

Follow safe computing and workstation security – this includes locking your computer or logging out prior to leaving the workstation for ANY reason. This also includes storing laptops, tablets, and removable media securely.

Never share your password

Follow the rules for allowable use and disclosure of PHI

Follow proper disposal of PHI in confidential bins

Follow proper storage of PHI

Report any suspected privacy and security breaches, even your own

### **When is it okay to share patient information on social media?**

This is never okay to share any type of patient information including pictures on social media. Even if you think you have clouded the details to the situation it cannot be shared. Patients and families can figure out who you are talking about.

As a rule, you may not share any specific clinical experience on social media per Student Policy S-82 “Client Confidentiality.”

Note: Sharing of protected health information will be reported to the affected organization and any/all repercussions may ensue.

Methodist College will in turn follow the policy S-02, “Student Code of Conduct” violation process to determine the outcome for the student.

### **Is it okay if I look up my own health information or that of my family?**

It is never okay to look up your own health information or that of your family. Remember it only okay to access PHI when it is needed to do your job as a student. This type of violation will follow the S-82, Client Confidentiality and Student Code of Conduct process as stated in the previous question.

The Patient Portal is available for use or you can access copies of your records by contacting Health Information Management.

### **Phishing**

Policy S82 / Client Confidentiality

These trick emails convince the receiver to open an attachment that is infected with a virus or malware. This can include copying your login and password thus leading to PHI access.

The screenshot shows a web browser window displaying a page titled "What does a phishing email message look like?". On the left, there is a list of characteristics of a phishing email. On the right, an email interface is shown with several red boxes and arrows pointing to specific parts of the email, illustrating these characteristics. A large red "Phishing" stamp is overlaid on the email content.

### What does a phishing email message look like?

Here is an example of what a phishing scam in an email message might look like.

- Unknown sender
- Threatens user that their account will be deleted if they do not respond
- No real person's name included and no phone number to call
- No company logo

**From:** Webmail Helpdesk Support Centre - ch...@nevus.it. Sent: Fri 11/11/2011 4:26 PM  
**To:** undisclosed-recipients  
**Subject:** \*\*Warning: Potential Phishing CoFC40\*\* Update Your Account !!!

This is to inform you that you have exceeded your email quota limit of [redacted] and you need to increase your email quota limit because in less than 48 hours your email will be disable. Increase your email quota limit and continue to use your email account.

To increase your email quota limit to 2.2GB, you must reply to ( [account-demo@gmx.com](mailto:account-demo@gmx.com) ) this email immediately and enter your account details below.

Username: (\*\*\*\*\*)  
Password: (\*\*\*\*\*)  
Date Of Birth(\*\*\*\*\*)

Failure to do this will immediately render your account deactivated from our database.

Thank you for your understanding.

**Phishing**

< PREV    NEXT >