


Methodist Health Services Corporation  General Administration	Page # 1 of 2	Section: C	Policy # C-1.14
	Approved by: <i>E. Nicole Robinson</i>	Date 03/16	
	Date Revised: 03/16 Supersedes 12/15, 09/09; 09/07; 02/05		
	Primary Responsible Party: Nicole Robinson		
	Secondary Responsible Party: Angie Moore		
The Joint Commission Standard: RI.01.01.01, IM.02.01.01			
SUBJECT: Confidentiality			

I. Policy

It is the policy of UnityPoint Health Methodist | Proctor to provide guidelines for the release of confidential/privileged information that meet applicable legal requirements.

II. Purpose & Standard

The purpose of this Policy is to ensure confidential/privileged information is released and/or communicated only when proper and authorized.

III. Policy Scope

This policy applies to all UnityPoint Health Methodist | Proctor entities.

IV. General Information.

A. General Exposure to Confidential/Privileged Information.

1. During the normal course of business, employees, volunteers and students have access to or are privileged to various types of information. This may include patient or personnel information and information about the day to day operations of UnityPoint Health Methodist | Proctor entities. This can be in written, verbal or electronic (computer) format.
2. Through direct communication with a patient, review of documents or data entries or third party communications among others, staff may become aware of medical, personal, financial and/or insurance information. On a need-to-know basis, employees, volunteers or students may need to access and/or share this information to care for the patient. However, the sharing of this information must be conducted in appropriate locations such as the nursing units and departments and in such a manner as to insure confidentiality and disclosure should follow the minimum necessary rule. See UPH policy 1.MR.07 Protected Health Information – Minimum Necessary Requirement. Unauthorized release or sharing of this information other than on a need-to-know basis is strictly prohibited. Locations where unauthorized third parties are in position to overhear communications, such as hallways, elevators, cafeteria, the lobby and other common areas are not appropriate areas to discuss patient information. See UPH policy 1.MR.11 Safeguards for Protecting PHI.

B. Confidentiality of Personnel Records and Information. Personnel information such as phone numbers, address and information regarding the day-to-day operations is considered Protected Health Information (PHI) and treated in the same manner. The release or sharing of PHI is on a need-to-know basis. Personnel records will only be released per applicable

law and, in specific circumstances, a written authorization is necessary. Contact Human Resources for further details. See UPH policy 1.AD.04 Protections of Information Guidelines.

- C. **Information Security Agreements.** Employees, volunteers and students who have access to information electronically must sign the Information Security Agreement and will be issued a unique username and password. Passwords are not to be shared with co-workers, family or friends and the sharing of a computer password will be treated the same as if breaching confidential information. See UPH policy 1.IT.06 Information Systems Access. screen and should never leave their computer unattended while logged on. All computers should be locked or logged off when not in use by the employee.

- D. **Confidentiality Statements.** As part of the employment process, employees are required to sign a Confidentiality Statement. This statement outlines the employees' responsibilities and the consequences for breaching confidential information. Failure to sign the statement may impact the employment relationship.

- E. **Non-retaliation.** Employees who report any breach or suspected breach of confidential information afforded protections in accordance with UnityPoint Health policies 1.CE.05 Compliance Helpline and 1.CE.06 Reporting and Investigating Dishonest, Illegal, or Fraudulent Activities.

- F. **Compliance with this Policy.** Failure to follow these guidelines concerning patient/personnel confidentiality can have serious legal implications and result in disciplinary action up to and including termination. See UPH policy 1.HR.04 Discipline/Corrective Action for Breaches of PHI. An unauthorized disclosure may in some instances be unlawful and nothing herein shall be construed as indicating that disciplinary action would be the only result. Unauthorized release may also subject the person making the release to legal action for monetary damages and/or other relief sought by the person aggrieved by the disclosure.

- G. **Use of Locked Confidential Bins.** No confidential material is to be placed in the general trash. Confidential material in all areas of UnityPoint Health Methodist | Proctor will be placed into designated locked receptacles labeled "confidential material". See UPH policy 1.MR.11 Safeguards for Protecting PHI. Confidential material may be placed in a container at an employee's workstation and then transported to a centrally located confidential material receptacle in a department or area as long as it remains attended by the employee. Confidential material consists of:
 - 1. Items that would contain PHI
 - 2. Items that would be confidential for UnityPoint Health Methodist | Proctor
 - 3. Confidential material that may be exposed to potentially infectious bodily fluids will be placed in a red bag lined trash can

References:

1.AD.04 Protection of Information Guidelines

1.CE.05 Compliance Helpline

1.CE.06 Reporting and Investigating Dishonest, Illegal, or Fraudulent Activities

1.HR.04 Discipline/Corrective Action for Breaches of PHI

1.MR.07 Protected Health Information – Minimum Necessary Requirements

1.MR.11 Safeguards for Protecting PHI

For a list of all HIPAA policies, visit the HIPAA Information Center on ConnectMe.