MERITER HEALTH SERVICES, INC.
CORPORATE MANAGEMENT POLICY

Policy No: A-10

Subject: Confidentiality (of Company Information and Privacy of Protected Health Information)

Signature: Sue Erickson, President & CEO

Effective Date: April 30, 2018

POLICY STATEMENT

UnityPoint Health - Meriter places a high value on patient, client and customer (collectively "Patient") privacy, and the confidentiality of Company Information. It is the expectation that Company Information as well as information about the Patient, including care received, remains confidential and is made available only to individuals who have a legitimate right to know. UnityPoint Health - Meriter recognizes that all employees ("Employees"), as well as volunteers, students, community clergy and pastoral caregivers, medical staff members, medical residents, housestaff, outside contractors/agencies and independent contractors ("Meriter Affiliates") have an ethical and/or legal obligation to keep Company Information and certain information about Patients confidential and to protect and safeguard such information against tampering and unauthorized use or disclosure.

Employees found to be in violation of this policy and the associated Corporate Procedures may be subject to disciplinary action, up to and including termination and/or legal action. UnityPoint Health - Meriter Affiliates who have access to Protected Health Information (PHI) and Company Information at or through UnityPoint Health - Meriter are expected to comply with this policy and the associated Corporate Procedures to the same extent as Employees, and if found to be in violation of this policy may be subject to termination of privileges and/or legal action. PHI is protected by federal and state laws and regulations that define civil and criminal penalties for violations of confidentiality.

DEFINITIONS

This Privacy Policy concerns two different types of information, Protected Health Information ("PHI") and other "Company Information."

PHI, as defined by federal law, means any individually identifiable Patient information, including but not limited to: Patient name, medical record number, account number, address, birth date, telephone number, subscriber number, e-mail address, and fax number, and medical records.

Company Information includes, but is not limited to: UnityPoint Health - Meriter payroll and personnel records, strategic plans, business and supporting financial plans, marketing plans, financial information, materials related to clinical quality and patient safety, and all documents specifically designated "confidential," whether verbally or physically labeled as such.

REVIEWED						

PHI and Company Information are not confined to written materials, facsimiles, or hard copy, but also include information derived from any source, including, but not limited to: electronic mail, computer data, data stored on electronic media, disks, or personal digital assistants, verbal communications or recordings, and visual observation.

PROCEDURE

1. Disclosure and/or Discussion of Information

   1.1 An Employee or UnityPoint Health - Meriter Affiliate may access, discuss, use and disclose PHI and Company Information only for UnityPoint Health - Meriter business as it relates to that person's specific job functions and/or responsibilities.

   1.2 PHI and Company Information must never be the subject of casual conversation either inside or outside of the work place. PHI and Company Information must not be discussed in lobbies, stairwells/elevators, restrooms, hallways, smoking areas or any other public area where conversation might be easily overheard by visitors, Employees or Meriter Affiliates who do not have a need to know.

   1.3 Employees and Meriter Affiliates may disclose Company Information only to third parties that have a legitimate need to know or who have prior written authorization.

   1.4 PHI may only be released to or accessed by authorized individuals or individuals with a legitimate right to know as defined in the following policies: UnityPoint Health - Meriter Hospital policy, "Release of/Access to Patient Information," Health Information Management, No. 3.

   1.5 Only the "Minimum Necessary" PHI may be disclosed. "Minimum Necessary" means only that amount of PHI necessary to accomplish the intended purpose of the use or disclosure.

   1.6 PHI may only be disclosed to the news media in accordance with UPH Corporate Management System Policy 1.MR.12, "Use of Protected Health Information for Marketing."

2. Business Associates

   2.1 A "Business Associate" is a person or entity that provides functions, activities, or services for UnityPoint Health - Meriter or on Meriter's behalf involving the use and/or disclosure of PHI. A business associate is also an organization that provides data transmission of protected health information such as a Health Information Exchange Organization, Regional Health Information Organization, E-Prescribing Gateway or a vendor that offers personal health records to patients.

   2.2 UnityPoint Health - Meriter will require all Business Associates to sign a contract that assures UnityPoint Health - Meriter that Business Associates will follow the same level of confidentiality and privacy practices for PHI as expected at UnityPoint Health - Meriter. It is the responsibility of each Department Director or Vice President to obtain, track and retain Business Associate (BA) contracts for contracted services within their departments. Such contracts will conform to the requirements in federal law. The template for contracts to be used by UnityPoint Health - Meriter is available from Corporate Compliance and can also be downloaded from the HIPAA resource page on MyMeriter.

2.3 No Protected Health Information shall be shared with the Business Associate until the contract is signed.

2.4 Business Associates may use PHI only for the purpose of providing services to UnityPoint Health - Meriter, and Business Associates shall safeguard the information from misuse and/or unauthorized disclosure.

2.5 All Business Associates are required to report all breaches of confidentiality to UnityPoint Health - Meriter in accordance with their contracts with UnityPoint Health - Meriter.

If UnityPoint Health - Meriter becomes aware of a pattern or practice of a Business Associate that constitutes a breach or violation of the Business Associate's obligations under its contract with UnityPoint Health - Meriter, UnityPoint Health - Meriter will take reasonable steps to cure the breach or end the violation.

2.6 The Corporate Compliance Department shall provide guidance to departments with regard to any questions or concerns about Business Associate contracts and services. Departments are required to send the following information to the Corporate Compliance Department for tracking purposes: name of BA, name of UnityPoint Health - Meriter point person, type of services provided by BA, form of PHI shared (paper, electronic, etc.).

2.7 Periodic audits shall be conducted by Corporate Compliance to assure compliance with the BA requirements.

2.8 Refer to UPH Corporate Management System Policy 1.CE.13, "Business Associates" for further guidance.

3. Electronic Data

UnityPoint Health - Meriter's Information Security Officer is responsible for systems and policies that are established to ensure the protection of electronic data.

4. Access to Information

4.1 Company Information and PHI may only be accessed as related to specific job functions and/or responsibilities.

4.2 Employees may not access their own or their minor child's medical record on Epic or any other electronic or paper system.

4.3 Casual reading of PHI by any individual is not permitted under any circumstance.

4.4 Maintaining confidentiality is not meant to imply that unnecessary obstacles should be placed before Employees or Meriter Affiliates who need information to perform their job duties.

4.5 Employees or Meriter Affiliates with legitimate access to PHI and Company Information are responsible for protecting this information from casual or unauthorized access. A courteous, yet assertive, response should be used to deny unauthorized or casual access.

5. Privacy of Patients

5.1 UnityPoint Health - Meriter's Notice of Privacy Practices will be posted and provided to all patients at all points of admission at all UnityPoint Health - Meriter entities.

5.2 At the time of admission, or as soon as reasonably practical after emergency care is rendered and patient is able to comply with the request, all patients will sign a form acknowledging that they have received or declined UnityPoint Health - Meriter's Notice of Privacy Practices.

5.3 Any requests for release of PHI outside of payment, treatment or healthcare operations will require authorization from the patient.

5.4 Absent a clinical reason to the contrary, Patient names will not be displayed outside Patient rooms. Other displays of Patient names in public or easily visible locations shall be avoided whenever possible.

5.5 Inpatients may request an increased level of privacy by designation of privacy status. See UnityPoint Health - Meriter Patient Care policy #155, "Privacy Status Designation".

5.6 Employees who become Patients will have the same rights of privacy and confidentiality of information as other Patients.

5.7 Employees providing care for Patients are responsible for ensuring that, whenever possible, Patient-provider conversations occur in private surroundings.

5.8 Employees providing care for Patients are responsible for ensuring that, whenever possible, Patients are protected and shielded from casual observation by other Employees and third parties not involved in direct care of the Patient.

6. Security of PHI and Company Information

6.1 Original Medical Records may not be removed from the premises except by authorized persons acting in accordance with a lawful court order, or properly executed subpoena duces tecum. Please refer to Hospital policy, "Release of/Access to Patient Information," Health Information Management, No. 3.

Employees and Meriter Associates may remove documents or notes containing PHI or Company Information from the facility only as it relates to specific job functions and/or responsibilities. It is the expectation that only the minimum amount of information necessary is removed from the facility. Documents, lists or reports that contain large amounts of PHI or Company Information or that reference multiple patients or employees may only be removed from the facility with the approval of the requestor's director or vice president. It is the responsibility of each Employee and Meriter Associate to protect and safeguard from loss, damage and unauthorized use all documents or notes that are removed.

6.2 Use of the original PHI rather than reproductions (copies) is encouraged. Copying of PHI should be kept to a minimum and made for legitimate purposes only. Copies of PHI are to be destroyed after use by shredding or by placing them in a covered recycling bin for destruction by Environmental Services.

6.3 Case studies or other PHI used in legitimate training activities shall be controlled and protected. Patient's identity will be removed whenever possible. Extra copies of study materials will be collected and destroyed and not left in meeting or conference rooms. The Patient's demographics, placement in the facility and other identifying data must be vigorously shielded wherever and whenever it is used for legitimate education and training activities. Any Patient information used in research is strictly controlled by Meriter's Institutional Review Board. Please refer to policy, "Human Subject Research Conducted at Meriter" (B-10).

6.4 Employees and Meriter Affiliates are encouraged to review PHI in the Health Information Management Department and are responsible for records that are checked out to them. It is the responsibility of the Employee to protect and safeguard from damage and unauthorized use all records that are removed from the Health Information Management Department.

6.5 Active records are maintained, stored and secured at the treatment site (e.g., nursing unit, outpatient clinic). These sites must provide for the security of these records and protect them from damage and unauthorized access. All inactive records are maintained, stored and secured in the Health Information Management Department. Departments, entities, clinics and Employees that

maintain copies of records or professional notes must provide for the security of these records/documents.

7. Breach of Confidentiality

7.1 Any Employee or Meriter Affiliate who believes he/she has observed a breach of confidentiality is encouraged to address the person who committed the breach directly. If this is not an option, the supervisor of the person believed to have breached confidentiality should be notified. If the person who breaches

confidentiality is not an Employee or Meriter Affiliate, or if the first two options are not acceptable to the observer, then the UnityPoint Health – Meriter Privacy Officer should be notified.

The Privacy Officer may refer calls, as appropriate, to the supervisor, administrator or executive of the entity, or to the Chief Medical Officer, or other appropriate individual(s).

7.2 Employees found to be in violation of this policy may be subject to disciplinary action, up to and including termination and/or legal action. PHI is protected by federal and state laws and regulations that define civil and criminal penalties for violations of confidentiality. Company Information is protected by this policy.

7.3 Meriter Affiliates who violate this policy will be subject to disciplinary action as determined by UnityPoint Health - Meriter and the respective contract, medical staff committee or affiliating organization.

8. Safeguarding Confidential Information

8.1 Disposal of PHI and Company Information
In order to maintain confidentiality from receipt until destruction, any item containing PHI or Company Information must be discarded according to the standards identified below:

Item	Description/Examples	Where discarded	Ultimate Disposal
Paper	Medical Records, labels, x-ray sleeves, or any paper containing PHI or Company Information	Covered Paper Recycling Collection Containers (Small desktop recycling containers may be used in non-public areas but should be emptied into covered recycling containers on a regular basis.)	Madison Recycling Center (MRC) where it is shredded, destroyed and recycled.
Blue Chips And Patient Wrist Bands	Patient information cards used for charging purposes and patient identification	Small collection bins (specifically for blue chips and wrist bands) located at nurses stations	Madison Recycling Center (MRC) where it is pelletized, destroyed and recycled
Hazardous Materials	Chemotherapy waste or medication with Patient labels	Yellow biohazard container located where medications are utilized	MERI transports to V.A. Hospital for incineration
Electronic	Computer discs	1. Reformat or 2. Destroy (open and cut up) and discard in general waste.	1. reused 2. landfill

8.2 Employees and Meriter Affiliates must follow the Corporate Faxing Policy and may not leave any PHI or Company Information on fax machines or copiers. Transmission of patient information/medical record documents via fax will be limited to transmittals needed for emergent/urgent patient care, for placement of patients for continuing care and other authorized situations. Please refer to Corporate Policy "Faxing Confidential Information", (A-24).

8.3 Employees and Meriter Affiliates are to use caution and discretion when leaving voicemail messages containing PHI or Company Information, in compliance with UPH Corporate Management System Policy 1.IT.01, "Voicemail Usage."

8.4 Employees and Meriter Affiliates may leave messages for patients on their answering machine or with a family member or other person who answers the phone when the patient is not home. However, to reasonably safeguard the individual's privacy, staff should take care to limit the amount of information disclosed and leave only a name and number and other information necessary to confirm an appointment, or ask the individual to call back.

8.5 Employees and Meriter Affiliates are to lock their computer or use auto time-out features in order to secure their workstation when not in work area, in compliance with UPH Corporate Management System Policy 1.AD.04, "Protection of Information Guidelines."

8.6 Employees and Meriter Affiliates are to use caution and discretion when e-mailing PHI and Company Information within UnityPoint Health - Meriter. E-mailing PHI and Company Information outside of UnityPoint Health - Meriter is permitted only

with encryption software. Please refer to UPH Corporate Management System Policy 1.IT.03, "Electronic Messaging."

8.7 Employees and Meriter Affiliates are to use access controls and encryption for storage of PHI and Company Information on portable computing devices, in compliance with UPH Corporate Management System Policy 1.AD.04, "Protection of Information Guidelines."

8.8 Employees and Meriter Affiliates are to properly secure all interdepartmental mail and external mail containing PHI and Company Information. Please refer to Corporate Policy "Mailing Confidential Information (Interdepartmental Mail and Other", (A-25).

8.9 Employees and Meriter Affiliates are to properly secure all medical equipment containing PHI. Employees are to log out of each patient encounter when use of medical equipment is complete.

9. Training-Employees

9.1 All new Employees are required to attend New Employee Orientation, which provides a confidentiality compliance overview. Additional orientation is completed at the department level as warranted by specific job duties.

9.2 All new Employees must complete the HIPAA/Confidentiality training modules assigned in Netlearning. Current Employees should have already completed these required modules.

9.3 All new Employees must sign a Confidentiality Agreement. (As of 10/1/05)

9.4 All Employees are required to complete an annual "HIPAA 101" Confidentiality Review Module on Netlearning.

9.5 All Employees are required to sign an "Information Systems Acceptable Use Acknowledgement" form as a prerequisite to gaining access privileges to any UnityPoint Health information system, in accordance with UPH Corporate Management System Policy 1.AD.04, "Protection of Information Guidelines."

10. Training-Other

10.1 Volunteers, Work-study students, other students, interns and medical residents will be educated about UnityPoint Health - Meriter's confidentiality and privacy policies and procedures at the time of assignment and will receive a copy of this Confidentiality policy.

10.2 Volunteers and Work-study students will complete the Confidentiality training module.