



Methodist College
UnityPoint Health

Page # 1 of 1

Section: E

Policy #: E-09

Approval:

Dr. K. P. A. [Signature]

Date: 8/2015

Review by: 8/2015

Date Revised: NEW

Policy/Revision Submitted by: L. Moore

SUBJECT: Health Insurance Portability and Accountability Act (HIPAA)

I. POLICY:

The purpose of this policy is to comply with HIPAA.

II. GENERAL INFORMATION:

Authority for Use or Disclosure. A covered Entity may only use and/or disclose the Protected Health Information (“PHI”) of an individual as follows: (i) when the use/disclosure is expressly allowed by HIPAA without the authorization of the individual, and is consistent with other state or federal laws, or (ii) with the written authorization of the individual.

No Authorization Required. In certain situations, HIPAA allows Covered Entities to use and disclose PHI without the authorization of the individual if such use/disclosure is not otherwise prohibited by state or federal law. However, specific rules apply to how and when these uses and disclosures can be made. The following is a list a few examples where an authorization is not required for certain uses and/or disclosures of PHI if (i) the Covered Entity otherwise complies with the specific rules regarding how and when the use or disclosure of PHI may be made, and (ii) the use/disclosure is not prohibited by state or federal law.

1. To the individual.
2. For the treatment of the individual.
3. To conduct the Health Care Operations of the Covered Entity.
4. Certain unintended, incidental disclosures.
5. Certain PHI in the following examples after giving the individual the opportunity to agree or object to the disclosure, as applicable.
 - a. To family members, relatives, or personal friends involved in the individual care.
 - b. To aid in disaster relief efforts.
6. When required by law.
7. When needed for certain public health activities.
8. About victims of abuse, neglect, or domestic violence.
9. For judicial and administrative proceedings.
10. For law enforcement purposes.
11. To advert a serious threat to health or safety.
12. A Limited Data Set for Research, public health or Health Care Operations if the covered Entity enters into a data use agreement with the recipient of the PHI.

Authorization Required. If the contemplated use or disclosure is not expressly authorized by HIPAA, the Covered Entity must obtain a written authorization from the individual, which meets the requirements of HIPAA or other applicable state or federal law, in order to use or disclose the PHI. The following is a non-exclusive list of uses or disclosures that require an express authorization from the individual:

1. For marketing (with certain exceptions).
2. In certain situations for Research (with some exceptions).
3. Treatment records relating to substance abuse (with certain exceptions).
4. Treatment records relating to mental health conditions (with certain exceptions).
5. Psychotherapy Notes (with certain exceptions).
6. Records relating to a patient’s HIV/AIDS status or treatment for HIV/AIDS (with certain exceptions).

Patient Rights. HIPAA also gives patients certain rights with regard to their PHI. Specifically, individuals have the right to:

1. Receive a written copy of the Covered Entity's Notice of Privacy Practices.
2. Inspect and copy their medical records (except Psychotherapy Notes and certain other documents).
3. Request an amendment to their medical record if information contained in the medical record is incorrect.
4. Make a complaint to the Covered Entity if the individual believes his/her privacy rights have been violated.

A Covered Entity may not require an individual to waive any of these rights as a condition of treatment.

1. De-Identification of PHI. In lieu of complying with the restrictions on uses and disclosures of PHI imposed by HIPAA, a Covered Entity may de-identify PHI.
2. Minimum Necessary Requirement. With certain exceptions, a Covered Entity is required to take reasonable steps to only disclose the minimum amount of PHI necessary to accomplish the intended purpose.
3. Safeguards. A Covered Entity is required to put in place reasonable safeguards to prevent improper use or disclosure of PHI.
4. Privacy Officer. A Covered Entity is required to designate a Privacy Officer who is responsible for the privacy policies and procedures at the Covered Entity and a contact person or office that is responsible for receiving complaints on privacy issues.
5. Business Associates. A Covered Entity is required to have business Associate Agreements with persons or entities that perform a function on behalf of the Covered Entity involving the use or disclosure of PHI.

Training.

1. Methodist College must train all the employees of its Workforce on its privacy and security policies and procedures, as necessary and appropriate for the employees to carry out their respective job functions.
2. Such training must be completed within a reasonable period of time after starting employment.
3. The Covered Entity shall document all training in written or electronic form and retain such documentation.

No Intimidation or Retaliation. A Covered Entity may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against an individual for:

1. Filing a complaint with the Secretary of Health and Human Services, its designee, or with the Covered Entity.
2. Exercising any of his/her rights under HIPAA.
3. Testifying, assisting or participating in any investigation or compliance review relating to the Covered Entity's HIPAA compliance.
4. Opposing any act or practice which is prohibited by HIPAA, if the individual has a good faith belief that the practice is unlawful and the manner of the opposition is reasonable and does not involve a disclosure of PHI in violation of HIPAA.