

HIPAA

Health Insurance Portability and Accountability Act of
1996

David Gleason, Esq.
Office of General Counsel

HIPAA Overview

- HIPAA mandates:
 - Extensive documentation and implementation of policies, procedures & mechanisms employed to **protect privacy and security of personal health information**
 - New rights for persons to review/seek amendment to their own medical records
 - Standardized forms in health e-commerce
 - Mandatory compliance with EDI transactions for certain health care providers

HIPAA APPLICATION

- ⦿ An entity having to abide by HIPAA is a “Covered Entity”
- ⦿ Application of HIPAA to an organization means adherence to rules concerning:
 - **privacy of protected health information**
 - **security of records, facilities and computer systems**
 - EDI transactions
 - health care codes and identifiers
- ⦿ HIPAA applies to any health care plan, insurer or entity who acts as a payer under the regs (“payers”), clearinghouse, or **provider who has submitted even one covered electronic transaction**, (e.g. health care claim, eligibility request/determination, claim payment or any one of 8 other related transactions)

HIPAA Privacy

- Once HIPAA applies, privacy requirements cover **all records, including electronic and paper formats, and verbal communication**
- Privacy regulations cover all personally identifiable health information in designated records maintained by the Covered Entity (**Protected Health Information or PHI**)

HIPAA DEADLINES

- ⦿ Privacy compliance was required to be in place prior to April 14, 2003
- ⦿ Security regulations were subsequently implemented and compliance was mandated by February 2005

Covered Entities

- Covered Entities must put into place all HIPAA requirements in EVERY operation of the covered unit or supporting affiliate unit (Covered Components).
- Any information flow outside of the Covered Components must be conducted pursuant to a specific Authorization or under a Business Associate Contract (BAC)

Does HIPAA Apply to Us?

- ⦿ How does HIPAA apply to a university?
 - Hybrid Entity- when an organization's primary purpose is not health care, but portions of the organization handle PHI (e.g., the Clinic), the relevant sub-unit can be designated as a Covered Entity
- ⦿ **Hybrid Entities must adopt full HIPAA requirements in only those dept's that are designated as Covered Entities**

HYBRID ENTITIES

- PHI may not be released outside the Covered Entity except under certain specific exemptions (e.g., Public health, HIPAA enforcement authorities)
- In order to support the health care component in its **treatment, payment and health care operations**, supporting component units can be designated as part of the Covered Entity workforce

HYBRID ENTITIES

- ⦿ Supporting units must adhere to most of the privacy and security requirements applicable to the Covered Entity
- ⦿ These privacy and security requirements fundamentally include:
 - Assignment of responsibility
 - Information flow analysis for each office
 - Established policies and procedures
 - Training

EXCLUSIONS from HIPAA

Types of records excluded from HIPAA:

- Student Health records
- Employment records, even if related to health care of employees
- Any records covered by FERPA

Health Care and Supporting Units

- The UMBC Student Health Services clinic treats non-students (faculty, staff, visitors), and is therefore covered a entity.
- Certain other campus units may receive PHI in the normal course of operations and are therefore designated as part of the health care component.

Health Care and Supporting Units

- Supporting component units include:
 - Offices of the President and Provost
 - Office of the General Counsel
 - Office of Information Technology
 - Bursar

Effects of Non-Compliance

- ⦿ There are civil and criminal penalties for non-compliance with HIPAA requirements.
 - Civil fines include \$100 per occurrence up to \$25,000 annually.
 - Criminal penalties for willfull violation vary between \$50K and 1 year in prison to \$250K and 10 years in prison