HARVARD
Information Security

Health Insurance Portability and Accountability Act (HIPAA)

This is a federal law that protects the privacy and security of individually, identifiable, health information and was created in response to the growing anxiety among Americans about the use and dissemination of health information in an age when computers allow easy sharing of data.

HIPAA defines individually, identifiable, health information as medical records, including medical history, diagnosis and treatment; payment information, including bills, receipts and explanation of benefits; and ancillary services, including x-rays and labs. HIPAA also protects demographic information, such as date of birth and social security number when it is maintained with health information. The protection applies to all forms of information, including electronic, paper and oral and pertains to the past, present and future health of a person.

HIPAA applies to health care providers, who electronically transmit protected health information in connection with a standard transaction; health plans, including individual and group health plans that provide or pay for medical care; and health care clearinghouses that process nonstandard information received from another entity into a standard format. These three groups are referred to as covered entities*.

HIPAA requires covered entities to ensure individual privacy rights. Under HIPAA individuals have the right to have their questions answered, have access to their information, obtain copies of their records, request to amend their records, request an accounting of certain uses and disclosures, and under certain circumstances, restrict uses and disclosures of information. In addition, covered entities must implement administrative requirements, including appointing a privacy officer, drafting and publishing a privacy notice, amending plan documents, obtaining business associate agreements with vendors and service providers, training their entire work force, instituting administrative, technical and physical safeguards, and providing a forum for filing privacy complaints.

In higher education settings, covered entities may include but not be limited to the following areas: university health services, including hospitals, clinics, and faculty practice plans and health plans, including self and fully insured health and dental plans and medical flexible spending accounts. In addition, HIPAA may affect other parts of the university that are not covered entities. Specifically, HIPAA may affect research involving human subjects, including non-clinical research and development activities involving patient solicitation and fundraising activities.

Recognizing variations in organizational structures, affiliations, and business purposes, HIPAA provides several models organizations can elect. Many universities have chosen the hybrid model, since their primary function is education and research. HIPAA requires that institutions electing the hybrid model designate in writing those parts of the organization that are covered by the regulation.

* Note on Medical Records and HIPAA: Harvard units or programs that are so-called "covered entities" under the Health Insurance Portability and Accountability Act (HIPAA) must comply with HIPAA’s data

security rules. As of the effective date of this policy, the covered entities are University Health Services, Harvard Dental Services, and certain University benefits plans. Other units or programs may be required to comply with HIPAA data security rules for limited purposes under the terms of specific contracts, such as a business associate agreement.