

What is HIPAA?

Answer: The Health Insurance Portability and Accountability Act of 1996 (HIPAA), which went into effect April 14, 2003, has four primary objectives:

- Assure health insurance portability by eliminating job-lock due to pre-existing medical conditions
- Reduce healthcare fraud and abuse
- Enforce standards for health information
- Guarantee security and privacy of health information

The University, in its role as a health care provider or hospital (e.g., University Health Services, UMASS Medical) is most impacted by the Standards for Privacy of Individually Identifiable Health Information (i.e., Privacy Rule) and the Security Rule.

The Privacy Rules are designed to protect patient's medical records and other health information provided by health plans, doctors, hospitals, and other health care providers. HIPAA focuses mainly on security and privacy but also involves data retention of patient records. The HIPAA regulation covers patient privacy within any health care setting, including pharmacies, hospitals, insurance companies, dental offices, podiatrists, and more. Note that not all researchers will have to comply with the Privacy Rule. It is important to understand that many research organizations that handle individually identifiable health information will not have to comply with the Privacy Rule because they will not be covered entities. The Privacy Rule will not directly regulate researchers who are engaged in research within organizations that are not covered entities even though they may gather, generate, access, and share personal health information. For instance, entities that sponsor health research or create and/or maintain health information databases may not themselves be covered entities, and thus may not directly be subject to the Privacy Rule. However, researchers may rely on covered entities for research support or as sources of individually identifiable health information to be included in research repositories or research databases. The Privacy Rule may affect such independent researchers, as it will affect their relationships with covered entities. In some instances, researchers may have to comply with the Privacy Rule because they may be or may work for a covered entity. For information on how the Privacy Rule may affect specific research areas, see http://privacypuleandresearch.nih.gov/pr_03.asp

The HIPAA Privacy Rule went into effect on April 14, 2003 and protects medical records and other individually identifiable health information, whether

it is on paper, in computers (i.e., electronic) or communicated orally.

The HIPPA Privacy Rules do not affect state laws that provide additional privacy protections for patients. The confidentiality protections are cumulative; any state law providing additional protections would continue to apply. When a state law requires a certain disclosure -- such as reporting an infectious disease outbreak to the public health authorities -- the federal privacy regulations would not preempt the state law.

The HIPPA Privacy Rule requires covered entities to establish policies and procedures to protect the confidentiality of protected health information about their patients. Covered entities must provide all the protections for patients cited above, such as providing a notice of their privacy practices and limiting the use and disclosure of information as required under the rule. In addition, covered entities must take some additional steps to protect patient privacy.

The HIPAA Security Rule adopts national standards for administrative, technical, and physical safeguards to protect the confidentiality, integrity, and availability of electronic protected health information collected, maintained, used or transmitted by covered entities (e.g., health care providers). The HIPAA Security Rule requires covered entities to implement basic safeguards to protect electronic protected health care information from unauthorized access, alteration, deletion and transmission. The Privacy Rule relates to the Security Rule in that it defines the scope of information (i.e., individually identifiable health information maintained by that entity) to which the safeguards must be applied. Note that the HIPAA Security Rule protects medical records and other individually identifiable health information in computers (i.e., electronic) only. It does not address records in any other format (e.g., paper). The compliance date for the HIPAA security regulation is April 21, 2005.

In regards to safeguard implementation, the Security Rule includes required and addressable security measure implementations. Required measures must be implemented. Addressable measures must either be implemented, replaced with alternate security measures that address the security issue, or shown to be already addressed in the current environment.

The Security Rule consists of the four areas of required and addressable standards that a covered entity would need to address to comply with HIPPA:

1. **Administrative Safeguards** □ includes assigning security responsibility, risk analysis and assessment, appropriate access to data, security awareness and training, security incident processes, contingency planning, and periodic review of HIPPA Security Rule compliance.

2. **Physical Safeguards** □ includes restricting access to applications that process/store protected health information and the facilities housing those applications, facilities contingency plans, facilities security plans, documentation of facilities maintenance, workstation security, control of hardware on which information is stored, disposal of data and hardware; procedures for hardware reuse; equipment monitoring, and development of a backup plan.
3. **Technical Safeguards** □ includes appropriate data security, appropriate access to data; unique operator ids, emergency access procedures, automatic logoff for inactivity; encryption of electronic protected health information, audit controls/trails, identity verification, and secure transmission of data.
4. **Organizational Safeguards** □ includes contracts with partners/business associates, and HIPPA compliance requirements for partners/business associates.

Lastly, the HIPPA Security Rule also contains policy and procedure documentation requirements (e.g., policies and procedures must be in writing; documentation must be available and retained for 6 years from the date of its creation or the date when it was in effect, whichever is later; and documentation must be periodically reviewed).

Failure to comply with HIPAA regulations result in possible penalties that include fines of \$100 per violation, up to \$25,000 per year for each requirement or prohibition violated. Criminal penalties range from a fine of \$50,000 and one year in prison up to a fine of \$250,000 and ten years in prison.