Health Insurance Portability and Accountability Act

From Wikipedia, the free encyclopedia.

(Redirected from HIPAA)
Jump to: navigation, search

The **Health Insurance Portability and Accountability Act** (**HIPAA**) was enacted by the U.S. Congress in 1996.

According to the Centers for Medicare and Medicaid Services' (CMS) website, Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs.

Title II of HIPAA, the Administrative Simplification provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers.

The AS provisions also address the security and privacy of health data. The standards are meant to improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of electronic data interchange in health care.

As a matter of linguistic-political criticism, many have noted that the Act did little to actually make health insurance more "portable" in the sense of preserving access to health care when an individual changes employers. Also, despite its many new rules on the sharing of medical information, the Act did not significantly increase health insurers' "accountability" for wrongdoing.

Contents

[hide]

[edit]

Administrative simplification provisions

The Administrative Simplification provisions are only applicable to "covered entities", which include health care providers (e.g. doctors offices and hospitals) which engage in electronic transactions subject to the HIPAA/EDI rules below, health plans (which includes health insurance companies and employer-sponsored "group health plans"), and health care clearinghouses.

[edit]

Privacy provision

The HIPAA Privacy provision took effect on April 14, 2003, with a one-year extension for certain "small plans".

Key privacy provisions include:

- Individuals must be able to access their record and request correction of errors
- Individuals must be informed of how their personal information will be used.
- Individuals "protected health information" (or "PHI") cannot be used for marketing purposes without the explicit consent of the involved individuals.
- Individuals can ask covered entities which maintain PHI about them to take reasonable steps to ensure that their communications with the individual are confidential. For instance, an individual can ask to be called at his or her work number, instead of home or cell phone number.
- Individuals can file formal privacy-related complaints to the Department of Health and Human Services (HHS) Office for Civil Rights.
- Covered entities must document their privacy procedures, but they have discretion on what to include in their privacy procedure.
- Covered entities must designate a privacy officer and train their employees.
- Covered entities may use an individual's information without the individual's consent for the purposes of providing treatment, obtaining payment for services and performing the non-treatment operational tasks of the provider's business.

[edit]

HIPAA Electronic Data Interchange (HIPAA/EDI)

The HIPAA/EDI provision was scheduled to take effect October 16, 2003 with a one-year extension for certain "small plans"; however, due to widespread confusion and difficulty in implementing the rule, CMS granted a one-year extension to all parties. As of October 16, 2004, full implementation was not achieved and CMS began an open-ended "contingency period." Penalties for non-compliance were not levied; however, all parties are expected to make a "good-faith effort" to come into compliance.

CMS has announced that the Medicare contingency period will end July 1, 2005. After July 1, most medical providers that file electronically will have to file their electronic claims using the HIPAA standards in order to be paid. There are exceptions for doctors that meet certain criteria.

Key EDI transactions are:

- **837**: Medical claims with subtypes for Professional, Institutional, and Dental varieties.
- **820**: Payroll Deducted and Other Group Premium Payment for Insurance Products
- **834**: Benefits enrollment and maintenance
- **835**: Electronic remittances
- **270/271**: Eligibility inquiry and response
- **276/277**: Claim status inquiry and response
- **278**: Health Services Review request and reply

These standards are X12 compliant, and are grouped under the label X12N.

Implementation Guides are available for free from the Washington Publishing Company.

[edit]

Security provision

The HIPAA Security provisions took effect April 20, 2005 with a one-year extension for certain "small plans". The Security provision complements the Privacy provision. HIPAA defines three segments of security safeguards for compliance: administrative, physical, and technical. Key provisions are:

- ***Administrative Safeguards*** - policies and procedures designed to clearly show how the entity will comply with the act
    - Covered entities (entities that must comply with HIPAA requirements) must adopt a written set of privacy procedures and designate a privacy officer to be responsible for developing and implementing all required policies and procedures.
    - The policies and procedures must reference management oversight and organizational buy-in to compliance with the documented security controls.
    - Procedures should clearly identify employees or classes of employees who will have access to protected health information (PHI). Access to PHI in all forms must be restricted to only those employees who have a need for it to complete their job function.
    - The procedures must address access authorization, establishment, modification, and termination.
    - Entities must show that an appropriate ongoing training program regarding the handling PHI is provided to employees performing health plan administrative functions.

    - Covered entities that out-source some of their business processes to a third party must ensure that their vendors also have a framework in place to comply with HIPAA requirements. Companies typically gain this assurance through clauses in the contracts stating that the vendor will meet the same data protection requirements that apply to the covered entity. Care must be taken to determine if the vendor further out-sources any data handling functions to other vendors and monitor whether appropriate contracts and controls are in place.
    - A contingency plan should be in place for responding to emergencies. Covered entities are responsible for backing up their data and having disaster recovery procedures in place. The plan should document data priority and failure analysis, testing activities, and change control procedures.
    - Internal audits play a key role in HIPAA compliance by reviewing operations with the goal of identifying potential security violations. Policies and procedures should specifically document the scope, frequency, and procedures of audits. Audits should be both routine and event-based.
    - Procedures should document instructions for addressing and responding to security breaches that are identified either during the audit or the normal course of operations.

- ***Physical Safeguards*** - controlling physical access to protect against inappropriate access to protected data
    - Responsibility for security must be assigned to a specific person or department. This responsibility includes the management and oversight of data protection and personnel conduct with respect to data protection. Frequently, a Chief Security Officer position is established to fulfill this requirement. This position typically reports to executive level management.
    - Controls must govern the introduction and removal of hardware and software from the network. (When equipment is retired it must be disposed of properly to ensure that PHI is not compromised.)
    - Access to equipment containing health information should be carefully controlled and monitored.
    - Access to hardware and software must be limited to properly authorized individuals.
    - Required access controls consist of facility security plans, maintenance records, and visitor sign-in and escorts.
    - Policies are required to address proper workstation use. Workstations should be removed from high traffic areas and monitor screens should not be in direct view of the public.
    - If the covered entities utilize contractors or agents, they too must be fully trained on their physical access responsibilities.

- ***Technical Safeguards*** - controlling access to computer systems and enabling covered entities to protect communications containing PHI transmitted

electronically over open networks from being intercepted by anyone other than the intended recipient
    - Information systems housing PHI must be protected from intrusion. When information flows over open networks, some form of encryption must be utilized. If closed systems/networks are utilized, existing access controls are considered sufficient and encryption is optional.
    - Each covered entity is responsible for ensuring that the data within its systems has not been changed or erased in an unauthorized manner.
    - Data corroboration, including the use of check sum, double-keying, message authentication, and digital signature may be used to ensure data integrity.
    - Covered entities must also authenticate entities it communicates with. Authentication consists of corroborating that an entity is who it claims to be. Examples of corroboration include: password systems, two or three-way handshakes, telephone callback, and token systems.
    - Covered entities must make documentation of their HIPAA practices available to the government to determine compliance.
    - In addition to policies and procedures and access records, information technology documentation should also include a written record of all configuration settings on the components of the network because these components are complex, configurable, and always changing.
    - Documented risk analysis and risk management programs are required. Covered entities must carefully consider the risks of their operations as they implement systems to comply with the act. (The requirement of risk analysis and risk management implies that the act's security requirements are a minimum standard and places responsibility on covered entities to take all reasonable precautions necessary to prevent PHI from being used for non-health purposes.)

[edit]

Legislative information

- House: 104 H.R. 3103, H. Rept. 104-469, Pt. 1, H. Rept. 104-736
- Senate: 104 S. 1028, 104 S. 1698, S. Rept. 104-156
- Law: Pub. L. 104-191, 110 Stat. 1936
- HHS Privacy Rule: 45 CFR 160, 45 CFR 164