



Health Insurance Portability And Accountability Act Guide

Title II: Preventing Health Care Fraud and Abuse; Administrative Simplification; Medical Liability Reform

Title II of HIPAA defines numerous offenses relating to health care and sets civil and criminal penalties for them. It also creates several programs to control fraud and abuse within the health care system.^{[7][8][9]} However, the most significant provisions of Title II are its Administrative Simplification rules. Title II requires the [Department of Health and Human Services](#) (HHS) to draft rules aimed at increasing the efficiency of the health care system by creating standards for the use and dissemination of health care information.

Title II of HIPAA, the Administrative Simplification (AS) 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 the US health care system.

The Privacy Rule

The Privacy Rule took effect on [April 14, 2003](#), with a one-year extension for certain "small plans." It establishes regulations for the use and disclosure of Protected Health Information (PHI). PHI is any information about health status, provision of health care, or payment for health care that can be linked to an individual.^[12] This is interpreted rather broadly and includes any part of a patient's [medical record](#) or payment history.

Covered entities must disclose PHI to the individual within 30 days upon request.^[13] They also must disclose PHI when required to do so by law, such as reporting suspected [child abuse](#) to state child welfare agencies.^[14]

A covered entity may disclose PHI to facilitate treatment, payment, or health care operations^[15] or if the covered entity has obtained authorization from the individual.^[16] However, when a covered entity discloses any PHI, it must make a reasonable effort to disclose only the minimum necessary information required to achieve its purpose.^[17]

The Privacy Rule gives individuals the right to request that a covered entity correct any inaccurate PHI.^[18] It also requires covered entities to take reasonable steps to ensure the confidentiality of communications with individuals.^[19] For example, an individual can ask to be called at his or her work number, instead of home or cell phone number.

The Privacy Rule requires covered entities to notify individuals of uses of their PHI. Covered entities must also keep track of disclosures of PHI and document privacy policies and procedures.^[20] They must appoint a Privacy Official and a contact person^[21] responsible for receiving complaints and train all members of their workforce in procedures regarding PHI.^[22]

An individual who believes that the Privacy Rule is not being upheld can file a complaint with the [Department of Health and Human Services](#) Office for Civil Rights (OCR).

The Security Rule

The Final Rule on Security Standards was issued on [February 20, 2003](#). It took effect on [April 21, 2003](#) with a compliance date of [April 21, 2005](#) for most covered entities and [April 21, 2006](#) for small plans. The Security Rule complements the Privacy Rule. While the Privacy Rule pertains to all Protected Health Information (PHI) including paper and electronic, the Security Rule deals specifically with Electronic Protected Health Information (EPHI). It lays out three types of security safeguards required for compliance: administrative, physical, and technical. For each of these types, the Rule identifies various security standards, and for each standard, it names both required and addressable implementation specifications. Required specifications must be adopted and administered as dictated by the Rule. Addressable specifications are more flexible. Individual covered entities can evaluate their own situation and determine the best way to implement addressable specifications. The standards and specifications are as follows:

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 electronic protected health information (EPHI). Access to EPHI 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 of 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

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.)

The Enforcement Rule

On [February 16, 2006](#), HHS issued the Final Rule regarding HIPAA enforcement. It became effective on [March 16, 2006](#). The Enforcement Rule sets civil money penalties for violating HIPAA rules and establishes procedures for investigations and hearings for HIPAA violations.