HIPAA - General Information

The Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II) require the Department of Health and Human Services (HHS) to adopt national standards for electronic health care transactions and national identifiers for providers, health plans, and employers. To date, the implementation of HIPAA standards has increased the use of electronic data interchange. Provisions under the Affordable Care Act of 2010 will further these increases and include requirements to adopt:

- operating rules for each of the HIPAA covered transactions
- a unique, standard Health Plan Identifier (HPID)
- a standard and operating rules for electronic funds transfer (EFT) and electronic remittance advice (RA) and claims attachments.

In addition, health plans will be required to certify their compliance. The Act provides for substantial penalties for failures to certify or comply with the new standards and operating rules.

For more information regarding HIPAA including additional provisions under the Patient Protections and Affordable Care Act (Affordable Care Act or ACA) of 2010

Title I: Health Care Access, Portability, and Renewability

Title I of HIPAA regulates the availability and breadth of group health plans and certain individual health insurance policies. It amended the Employee Retirement Income Security Act, the Public Health Service Act, and the Internal Revenue Code.

Title I requires the coverage of and also limits restrictions that a group health plan can place on benefits for preexisting conditions. Group health plans may refuse to provide benefits relating to preexisting conditions for a period of 12 months after enrollment in the plan or 18 months in the case of late enrollment. Title I allows individuals to reduce the exclusion period by the amount of time that they had "creditable coverage" prior to enrolling in the plan and after any "significant breaks" in coverage. "Creditable coverage" is defined quite broadly and includes nearly all group and individual health plans, Medicare, and Medicaid. A "significant break" in coverage is defined as any 63 day period without any creditable coverage.

Title I also requires insurers to issue policies without exclusion to those leaving group health plans with creditable coverage (see above) exceeding 18 months, and renew individual policies for as long as they are offered or provide alternatives to discontinued plans for as long as the insurer stays in the market without exclusion regardless of health condition.

Some health care plans are exempted from Title I requirements, such as long-term health plans and limited-scope plans such as dental or vision plans that are offered separately from the general health plan. However, if such benefits are part of the general health plan, then HIPAA still applies to such
benefits. For example, if the new plan offers dental benefits, then it must count creditable continuous coverage under the old health plan towards any of its exclusion periods for dental benefits.

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

Title II of HIPAA defines policies, procedures and guidelines for maintaining the privacy and security of individually identifiable health information as well as outlining numerous offenses relating to health care and sets civil and criminal penalties for violations. It also creates several programs to control fraud and abuse within the health care system. 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.

These rules apply to "covered entities" as defined by HIPAA and the HHS. Covered entities include health plans, health care clearinghouses, such as billing services and community health information systems, and health care providers that transmit health care data in a way that is regulated by HIPAA.

Per the requirements of Title II, the HHS has promulgated five rules regarding Administrative Simplification: the Privacy Rule, the Transactions and Code Sets Rule, the Security Rule, the Unique Identifiers Rule, and the Enforcement Rule.

Privacy Rule

The effective compliance date of the Privacy Rule was April 14, 2003, with a one-year extension for certain "small plans". The HIPAA Privacy Rule regulates the use and disclosure of Protected Health Information (PHI) held by "covered entities" (generally, health care clearinghouses, employer sponsored health plans, health insurers, and medical service providers that engage in certain transactions.) By regulation, the Department of Health and Human Services extended the HIPAA privacy rule to independent contractors of covered entities who fit within the definition of "business associates". PHI is any information held by a covered entity which concerns health status, provision of health care, or payment for health care that can be linked to an individual. This is interpreted rather broadly and includes any part of an individual's medical record or payment history. Covered entities must disclose PHI to the individual within 30 days upon request. They also must disclose PHI when required to do so by law such as reporting suspected child abuse to state child welfare agencies.

Covered entities may disclose protected health information to law enforcement officials for law enforcement purposes as required by law (including court orders, court-ordered warrants, subpoenas) and administrative requests; or to identify or locate a suspect, fugitive, material witness, or missing person.
A covered entity may disclose PHI (Protected Health Information) to facilitate treatment, payment, or health care operations without a patient's express written authorization. Any other disclosures of PHI (Protected Health Information) require the covered entity to obtain written authorization from the individual for the disclosure. 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.

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

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. They must appoint a Privacy Official and a contact person responsible for receiving complaints and train all members of their workforce in procedures regarding PHI.

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). However, according to the Wall Street Journal, the OCR has a long backlog and ignores most complaints. "Complaints of privacy violations have been piling up at the Department of Health and Human Services. Between April of 2003 and November 2006, the agency fielded 23,886 complaints related to medical-privacy rules, but it has not yet taken any enforcement actions against hospitals, doctors, insurers or anyone else for rule violations. A spokesman for the agency says it has closed three-quarters of the complaints, typically because it found no violation or after it provided informal guidance to the parties involved. However, in July 2011, UCLA agreed to pay $865,500 in a settlement regarding potential HIPAA violations. An HHS Office for Civil Rights investigation showed that from 2005 to 2008 unauthorized employees repeatedly and without legitimate cause looked at the electronic protected health information of numerous UCLAHS patients."

**2013 Final Omnibus Rule Update**

In January 2013, HIPAA was updated via the Final Omnibus Rule. Included in changes were updates to the Security Rule and Breach Notification portions of the HITECH Act. The greatest changes relate to the expansion of requirements to include business associates, where only covered entities had originally been held to uphold these sections of the law.

Additionally, the definition of 'significant harm’ to an individual in the analysis of a breach was updated to provide more scrutiny to covered entities with the intent of disclosing more breaches which had been previously gone unreported. Previously an organization needed proof that harm had occurred whereas now they must prove the counter, that harm had not occurred.
Protection of PHI was changed from indefinite to 50 years after death. More severe penalties for violation of PHI privacy requirements were also approved.

**Transactions and Code Sets Rule**

HIPAA was intended to make the health care system in the United States more efficient by standardizing health care transactions. HIPAA added a new Part C titled "Administrative Simplification" to Title XI of the Social Security Act. This is supposed to simplify health care transactions by requiring all health plans to engage in health care transactions in a standardized way.

After July 1, 2005 most medical providers that file electronically did have to file their electronic claims using the HIPAA standards in order to be paid.

Under HIPAA, HIPAA-covered health plans are now required to use standardized HIPAA electronic transactions. Information about this can be found in the final rule for HIPAA electronic transaction standards (74 Fed. Reg. 3296, published in the Federal Register on January 16, 2009), and on the CMS website here: CMS information on HIPAA standardized electronic transactions

**Security Rule**

The Final Rule on Security Standards was issued on February 20, 2003. 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. Some privacy advocates have argued that this “flexibility” may provide too much latitude to covered entities. 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 with which they communicate. 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.)