Perry4Law
An Exclusive Techno-Legal Corporate, IP & ICT Law Firm

New Delhi, India

Health Insurance Portability And Accountability Act Of 1996

Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a comprehensive Federal legislation of United States (US) that ensures health care coverage, privacy protection, electronic information security, and fraud prevention regarding health care related issues.

Before the enactment of HIPAA there was no centralised legislation that covered the entire US. Even regarding privacy issues, there were numerous uncoordinated Federal legislations which addressed privacy in some form. Prior to HIPAA, there was no standard authority for enforcement of fraud and abuse that applied to State and Federal health care programs.

HIPAA "consolidated" all these issues at a single place and made it much easier and effective to implement health insurance related matters in US. Further, HIPAA also ensured cyber security and data security for electronic patient and health related information.

The Preamble to HIPAA says that it is an Act to amend the Internal Revenue Code of 1986 to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes.

Title II of HIPAA, deals with prevention of health care frauds and abuse, administrative simplification and medical liability reform. It 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.

The Department of Health and Human Services (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.

(1) Privacy Rule: 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.

A covered entity may disclose PHI to facilitate treatment, payment, or health care operations, or if the covered entity has obtained authorisation from the individual. 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. 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).

(2) Transactions and Code Sets Rule: HIPAA was intended to make the health care system in the United States more efficient by standardising health care transactions. Under HIPAA, HIPAA-covered health plans are now required to use standardised HIPAA electronic transactions.

(3) Security Rule: 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:

(a) Administrative Safeguards – policies and procedures designed to clearly show how the entity will comply with the act

(i) 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.

(ii) The policies and procedures must reference management oversight and organisational buy-in to compliance with the documented security controls.

(iii) 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.

(iv) The procedures must address access authorization, establishment, modification, and termination.

(v) Entities must show that an appropriate ongoing training program regarding the handling of PHI is provided to employees performing health plan administrative functions.

(vi) 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.

(vii) 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.

(viii) 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.

(ix) Procedures should document instructions for addressing and responding to security breaches that are identified either during the audit or the normal course of operations.

(b) Physical Safeguards – controlling physical access to protect against inappropriate access to protected data

(i) 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.)

(ii) Access to equipment containing health information should be carefully controlled and monitored.

(iii) Access to hardware and software must be limited to properly authorized individuals.

(iv) Required access controls consist of facility security plans, maintenance records, and visitor sign-in and escorts.

(v) 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.

(vi) If the covered entities utilise contractors or agents, they too must be fully trained on their physical access responsibilities.

(c) 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.

(i) Information systems housing PHI must be protected from intrusion. When information flows over open networks, some form of encryption must be utilised. If closed systems/networks are utilized, existing access controls are considered sufficient and encryption is optional.

(ii) Each covered entity is responsible for ensuring that the data within its systems has not been changed or erased in an unauthorized manner.

(iii) Data corroboration, including the use of check sum, double-keying, message authentication, and digital signature may be used to ensure data integrity.

(iv) 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.

(v) Covered entities must make documentation of their HIPAA practices available to the government to determine compliance.

(vi) 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.

(vii) 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.)

(4) Unique Identifiers Rule (National Provider Identifier): HIPAA covered entities such as providers completing electronic transactions, healthcare clearinghouses, and large health plans, must use only the National Provider Identifier (NPI) to identify covered healthcare providers in standard transactions.

All covered entities using electronic communications (e.g., physicians, hospitals, health insurance companies, and so forth) must use a single new NPI. The NPI replaces all other identifiers used by health plans, Medicare, Medicaid, and other government programs. However, the NPI does not replace a provider's DEA number, state license number, or tax identification number. The NPI is 10 digits (may be alphanumeric), with the last digit being a checksum. The NPI cannot contain any embedded intelligence; in other words, the NPI is simply a number that does not itself have any additional meaning. The NPI is unique and national, never re-used, and except for institutions, a provider usually can have only one. An institution may obtain multiple NPIs for different "subparts" such as a free-standing cancer center or rehab facility.

(5) Enforcement Rule: The Enforcement Rule sets civil money penalties for violating HIPAA rules and establishes procedures for investigations and hearings for HIPAA violations.

American Recovery and Reinvestment Act of 2009/Division A/Title XIII/Subtitle D: HITECH Act: Privacy Requirements

Subtitle D of the Health Information Technology for Economic and Clinical Health Act (HITECH Act), enacted as part of the American Recovery and Reinvestment Act of 2009, addresses the privacy and security concerns associated with the electronic transmission of health information.

This subtitle extends the complete Privacy and Security Provisions of HIPAA to business associates of covered entities. This includes the extension of newly updated civil and criminal penalties to business associates. These changes are also required to be included

in any business associate agreements with covered entities. On November 30, 2009, the regulations associated with the new enhancements to HIPAA enforcement took effect.

Another significant change brought about in Subtitle D of the HITECH Act, is the new breach notification requirements. This imposes new notification requirements on covered entities, business associates, vendors of personal health records (PHR) and related entities if a breach of unsecured protected health information (PHI) occurs. On April 27, 2009, the Department of Health and Human Services (HHS) issued guidance on how to secure protected health information appropriately. Both HHS and the Federal Trade Commission (FTC) were required under the HITECH Act to issue regulations associated with the new breach notification requirements. The HHS rule was published in the Federal Register on August 24, 2009 and the FTC rule was published on August 25, 2009.

The final significant change made in Subtitle D of the HITECH Act, implements new rules for the accounting of disclosures of a patient's health information. It extends the current accounting for disclosure requirements to information that is used to carry out treatment, payment and health care operations when an organisation is using an electronic health record (EHR). This new requirement also limits the timeframe for the accounting to three years instead of six as it currently stands. These changes won't take effect until January 1, 2011, for organizations implementing EHRs between January 1, 2009 and January 1, 2011, and January 1, 2013, for organisations who had implemented an EHR prior to January 1, 2009.

Effects On Research And Clinical Care

The enactment of the Privacy and Security Rules has caused major changes in the way physicians and medical centers operate. The complex legalities and potentially stiff penalties associated with HIPAA, as well as the increase in paperwork and the cost of its implementation, were causes for concern among physicians and medical centers.

(a) Effects on Research: HIPAA restrictions on researchers have affected their ability to perform retrospective, chart-based research as well as their ability to prospectively evaluate patients by contacting them for follow-up. In addition, informed consent forms for research studies now are required to include extensive detail on how the participant's protected health information will be kept private. While such information is important, the addition of a lengthy, legalistic section on privacy may make these already complex documents even less user-friendly for patients who are asked to read and sign them.

(b) Effects on Clinical Care: The complexity of HIPAA, combined with potentially stiff penalties for violators, can lead physicians and medical centers to withhold information from those who may have a right to it. A review of the implementation of the HIPAA Privacy Rule by the U.S. Government Accountability Office found that health care providers were "uncertain about their legal privacy responsibilities and often responded

with an overly guarded approach to disclosing information than necessary to ensure compliance with the Privacy rule".

Costs Of Implementation

In the period immediately prior to the enactment of the HIPAA Privacy and Security Acts, medical centers and medical practices were charged with getting "into compliance". With an early emphasis on the potentially severe penalties associated with violation, many practices and centers turned to private, for-profit "HIPAA consultants" who were intimately familiar with the details of the legislation and offered their services to ensure that physicians and medical centers were fully "in compliance". In addition to the costs of developing and revamping systems and practices, the increase in paperwork and staff time necessary to meet the legal requirements of HIPAA may impact the finances of medical centers and practices at a time when insurance companies and Medicare reimbursement is also declining.