# HIPAA - Health Insurance Portability and Accountabilty Act

**by Sudheer Sharma - Wednesday, April 01, 2009**

http://dwhnotes.com/data-warehousing/hipaa

What do you think of this post?

Awesome (0) Interesting (0) Useful (0)

**Health Care Access, Portability, and Renew ability**

**HIPAA** regulates the availability and breadth of group and individual health insurance plans. It amends both the Employee Retirement Income Security Act and the Public Health Service Act.

Title I prohibits any group health plan from creating eligibility rules or assessing premiums for individuals in the plan based on health status, medical history, genetic information, or disability. This does not apply to private individual insurance.

Title I 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. However, individuals may reduce this exclusion period if they had health insurance prior to enrolling in the plan. 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.

To illustrate, suppose someone enrolls in a group health plan on January 1, 2006. This person had previously been insured from January 1, 2004 until February 1, 2005 and from August 1, 2005 until December 31, 2005. To determine how much coverage can be credited against the exclusion period in the new plan, start at the enrollment date and count backwards until you reach a significant break in coverage. So, the five months of coverage between August 1, 2005 and December 31, 2005 clearly counts against the exclusion period. But the period without insurance between February 1, 2005 and August 1, 2005 is greater than 63 days. Thus, this is a significant break in coverage, and any coverage prior to it cannot be deducted from the exclusion period. So, this person could deduct five months from his or her exclusion period, reducing the exclusion period to seven months. Hence, Title I requires that any preexisting condition begin to be covered on August 1, 2006.

Title I also forbids individual health plans from denying coverage or imposing preexisting condition exclusions on individuals who have at least 18 months of creditable group coverage without significant breaks and who are not eligible to be covered under any group, state, or federal health plans at the time they seek individual insurance.

**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. However, the most significant provisions of Title II are its Administrative Simplification rules. Title II requires theDepartment 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.

**The Privacy Rule**

The Privacy Rule took effect 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. 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. 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 authorization 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. 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. 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

**The Transactions and Code Sets Rule**

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 announced that the Medicare contingency period ended 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 used for HIPAA compliance are:

**EDI Health Care Claim Transaction set (837)** is used to submit health care claim billing information, encounter information, or both. It can be sent from providers of health care services to payers, either directly or via intermediary billers and claims clearinghouses. It can also be used to transmit health care claims and billing payment information between payers with different payment responsibilities where coordination of benefits is required or between payers and regulatory agencies to monitor the rendering, billing, and/or payment of health care services within a specific health care/insurance industry segment.

For example, a state mental health agency may mandate all healthcare claims, Providers and health plans who trade professional (medical) health care claims electronically must use the 837 Health Care Claim: Professional standard to send in claims. As there are many different business applications for the Health Care claim, there can be slight derivations to cover off claims involving unique claims such as for Institutions, Professionals, Chiropractors, and Dentists etc.

**EDI Health Care Claim Payment/Advice Transaction Set (835**) can be used to make a payment, send an Explanation of Benefits (EOB) remittance advice, or make a payment and send an EOB remittance advice only from a health insurer to a health care provider either directly or via a financial institution.

**EDI Benefit Enrolment and Maintenance Set (834)** can be used by employers, unions, government agencies, associations or insurance agencies to enroll members to a payer. The payer is a healthcare organization that pays claims, administers insurance or benefit or product. Examples of payers include an insurance company, health care professional (HMO), preferred provider organization (PPO), government

agency (Medicaid, Medicare etc.) on any organization that may be contracted by one of these former groups.

**EDI Application Advice (824)** this transaction set can be used to report the results of an application system's data content edits of transaction sets. The results of editing transaction sets can be reported at the functional group and transaction set level in either coded or free-form format. It is designed to accommodate the business need of reporting the acceptance/rejection or acceptance with change of any transaction set. The Application Advice should not be used in place of a transaction set designed as a specific response to another transaction set (e.g., purchase order acknowledgment sent in response to a purchase order.)

**EDI Payroll Deducted and other group Premium Payment for Insurance Products (820)** this transaction set can be used to make a premium payment for insurance products. It can be used to order a financial institution to make a payment to a payee.

**EDI Health Care Eligibility/Benefit Inquiry (270)** is used to inquire about the health care benefits and eligibility associated with a subscriber or dependent

**EDI Health Care Eligibility/Benefit Response (271)** is used to respond to a request inquire about the health care benefits and eligibility associated with a subscriber or dependent

**EDI Health Care Claim Status Request (276)** this transaction set can be used by a provider, recipient of health care products or services or their authorized agent to request the status of a health care claim.

**EDI Health Care Claim Status Notification (277)** This transaction set can be used by a health care payer or authorized agent to notify a provider, recipient or authorized agent regarding the status of a health care claim or encounter, or to request additional information from the provider regarding a health care claim or encounter. This transaction set is not intended to replace the Health Care Claim Payment/Advice Transaction Set (835) and therefore, is not used for account payment posting. The notification is at a summary or service line detail level. The notification may be solicited or unsolicited.

**EDI Health Care Service Review Information (278)** This transaction set can be used to transmit health care service information, such as subscriber, patient, demographic, diagnosis or treatment data for the purpose of request for review, certification, notification or reporting the outcome of a health care services review.

**EDI Functional Acknowledgement Transaction Set (997)** this transaction set can be used to define the control structures for a set of acknowledgments to indicate the results of the syntactical analysis of the electronically encoded documents. The encoded documents are the transaction sets, which are grouped in functional groups, used in defining transactions for business data interchange. This standard does not cover the semantic meaning of the information encoded in the transaction sets.

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

**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 pertains to all (PHI) protected heath information, including paper and Electronic. The Security rule deals specifically with (EPHI) electronic protected health information. 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 Unique Identifiers Rule (National Provider Identifier)**

Effective May 2006 (May 2007 for small health plans), all covered entities using electronic communications (e.g., physicians, hospitals, health insurance companies, and so forth) must use a single new National Provider Identifier (NPI). The NPI replaces all other identifiers used by health plans, Medicare (i.e., the UPIN), Medicaid, and other government programs. The NPI does not replace a provider's DEA number however, or a provider's state license number or tax identification number. The NPI is 10 digits (may be alphanumeric), 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.

**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, however its deterrent effects seems to be negligible with few prosecutions for violations

**Effect 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. While respect for patient privacy was already informally considered a cornerstone of medicalprofessionalism, 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. An August 2006 article in the journal Annals of Internal Medicine detailed some such concerns over the implementation and effects of HIPAA.

**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. A study from theUniversity of Michigan demonstrated that implementation of the HIPAA Privacy rule resulted in a drop from 96% to 34% in the proportion of follow-up surveys completed by study patients being followed after a heart attack.[26] Another study, detailing the effects of HIPAA on recruitment for a study on cancer prevention, demonstrated that HIPAA-mandated changes led to a 73% decrease in patient accrual, a tripling of time spent recruiting patients, and a tripling of mean recruitment costs.

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 more user-unfriendly for patients who are asked to read and sign them.

These data suggest that the HIPAA privacy rule, as currently implemented, may be having negative impacts on the cost and quality of medical research. Dr. Kim Eagle, professor of internal medicine at the University of Michigan, was quoted in the Annals article as saying, "Privacy is important, but research is also important for improving care. We hope that we will figure this out and do it right."

**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 company and Medicare reimbursement is also declining.