

A Short Description of the Health Insurance Portability and Accountability Act

From Wikipedia, the free encyclopedia

If you want a full and complete actual copy of the bill then go here:

- [Full text of the Health Insurance Portability and Accountability Act](#)
- [Centers for Medicare and Medicaid Services - HIPAA Page](#)

There are many more sources if you do a web search under HIPAA. This following description is mostly adequate for our web site as a short reference.

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 (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.

Contents

[\[hide\]](#)

- [1 Title I: Health Care Access, Portability, and Renewability](#)
- [2 Title II: Preventing Health Care Fraud and Abuse; Administrative Simplification; Medical Liability Reform](#)
 - [2.1 The Privacy Rule](#)
 - [2.2 The Transactions and Code Sets Rule](#)
 - [2.3 The Security Rule](#)
 - [2.4 The Enforcement Rule](#)
- [3 Effect on research and clinical care](#)
 - [3.1 Effects on research](#)
 - [3.2 Effects on clinical care](#)
 - [3.3 Costs of implementation](#)
- [4 Legislative information](#)
- [5 See also](#)
- [6 References](#)
- [7 External links](#)

[\[edit\]](#)

Title I: Health Care Access, Portability, and Renewability

Title I of 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^[1].

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^[2]. 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^[3]. “Creditable coverage” is defined quite broadly and includes nearly all group and individual health plans, [Medicare](#), and [Medicaid](#)^[4]. A “significant break” in coverage is defined as any 63 day period without any creditable coverage^[5].

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^[6].

[\[edit\]](#)

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. 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 way that is regulated by HIPAA ^[10] ^[11].

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.

[\[edit\]](#)

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^[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 instance, 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) ^[23]^[24].

[\[edit\]](#)

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 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 from the [Washington Publishing Company](#) for a fee, now that CMS is not subsidizing the publications.

The National Council for Prescription Drug Programs' Telecommunication Standard version 5.1 is also used for the transmission of third-party pharmacy claims. The NCPDP Telecommunication Standard version 5.1 is available to NCPDP members at [NCPDP's website](#).

[\[edit\]](#)

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. 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 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
 - 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.)

[\[edit\]](#)

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.

[\[edit\]](#)

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 medical [professionalism](#), 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. ^[25]

[\[edit\]](#)

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 the [University 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. ^[27]

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."^[25]

[\[edit\]](#)

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."^[25]

[\[edit\]](#)

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.

[\[edit\]](#)

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](#) Standards for Privacy of Individually Identifiable Health Information; Final Rule: 45 CFR Parts 160 and 164
- [HHS](#) Security Standards; Final Rule: 45 CFR Parts 160, 162, and 164

[\[edit\]](#)

See also

- [Information technology audit](#)
- [Eric Drew](#)
- [Identity theft](#)

[\[edit\]](#)

References

1. [^ 29 U.S.C. § 1182\(a\)\(1\)](#)
2. [^ 29 U.S.C. § 1181\(a\)\(2\)](#)
3. [^ 29 U.S.C. § 1181\(a\)\(3\)](#)
4. [^ 29 U.S.C. § 1181\(c\)\(1\)](#)
5. [^ 29 U.S.C. § 1181\(c\)\(2\)\(A\)](#)
6. [^ 42 U.S.C. § 300gg-41](#)
7. [^ 42 U.S.C. § 1320a-7c](#)
8. [^ 42 U.S.C. § 1395ddd](#)
9. [^ 42 U.S.C. § 1395b-5](#)
10. [^ 45 C.F.R. 160.103](#)
11. [^ Definitions of a Covered Entity](#)
12. [^ 45 C.F.R. 164.501](#)
13. [^ 45 C.F.R. 164.524\(b\)](#)
14. [^ 45 C.F.R. 164.512](#)
15. [^ 45 C.F.R. 164.524\(a\)\(1\)\(ii\)](#)
16. [^ 45 C.F.R. 164.502\(a\)\(1\)\(iv\)](#)
17. [^ 45 C.F.R. 164.502\(b\)](#)
18. [^ 45 C.F.R. 164.526](#)
19. [^ 45 C.F.R. 164.522\(b\)](#)
20. [^ 45 C.F.R. 164.528](#)
21. [^ 45 C.F.R. 164.530\(a\)](#)
22. [^ 45 C.F.R. 164.530\(b\)](#)
23. [^ How to File A Health Information Privacy Complaint with the Office for Civil Rights](#)
24. [^ 45 C.F.R. 160.306](#)
25. [^ a b c](#) Fisher Wilson, J. Health Insurance Portability and Accountability Act Privacy Rule Causes Ongoing Concerns among Clinicians and Researchers. Ann Int Med 2006:145(4), pp. 313-316.
26. [^](#) Armstrong D, Kline-Rogers E, Jani SM, Goldman EB, Fang J, Mukherjee D, et al. Potential impact of the HIPAA privacy rule on data collection in a registry of patients with acute coronary syndrome. Arch Int Med 2005:165, pp. 1125-1129. [PMID: 15911725]
27. [^](#) Wolf MS, Bennett CL. Local perspective of the impact of the HIPAA privacy rule on research. Cancer 2006:106, pp. 474-479. [PMID: 1632254]

[\[edit\]](#)

External links

- [Centers for Medicare and Medicaid Services - HIPAA Page](#)
- [Office for Civil Rights page on HIPAA](#)
- [Full text of the Health Insurance Portability and Accountability Act](#)
- [California Office of HIPAA Implementation](#) CalOHI Burt R. Cohen, Director.
- [HIPAA 101](#) Provides basic introduction to HIPAA.
- [Final Rule on HIPAA Enforcement](#) Effective March 16, 2006.
- [Congressional Research Service \(CRS\) Reports regarding HIPAA](#) from University of North Texas Libraries
- [HIPAA Lawsuits and Violations](#)

Retrieved from

"http://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act"
Categories: [1996 in law](#) | [Healthcare policy in the United States](#) | [Privacy](#) | [United States federal healthcare legislation](#) | [Medicare and Medicaid \(United States\)](#)

WIKIPEDIA MAKES NO GUARANTEE OF VALIDITY

Wikipedia is an online open-content collaborative encyclopedia, that is, a voluntary association of individuals and groups who are developing a common resource of human knowledge. The structure of the project allows anyone with an Internet connection and World Wide Web browser to alter its content. Please be advised that nothing found here has necessarily been reviewed by professionals with the expertise required to provide you with complete, accurate or reliable information.

That is not to say that you will not find valuable and accurate information in Wikipedia; much of the time you will. However, **Wikipedia cannot guarantee the validity of the information found here.** The content of any given article may recently have been changed, vandalized or altered by someone whose opinion does not correspond with the state of knowledge in the relevant fields.

No formal peer review

We are working on ways to select and highlight reliable versions of articles. Our active community of editors uses tools such as the [Special:Recentchanges](#) and [Special:Newpages](#) feeds to monitor new and changing content. However, Wikipedia is not uniformly peer reviewed; while readers may correct errors or engage in casual [peer review](#), they have no legal duty to do so and thus all information read here is without any implied warranty of fitness for any purpose or use whatsoever. Even articles that have been vetted by informal peer review or [featured article](#) processes may later have been edited inappropriately, just before you view them.

None of the authors, contributors, sponsors, administrators, sysops, or anyone else connected with Wikipedia in any way whatsoever can be responsible for the appearance of any inaccurate or libelous information or for your use of the information contained in or linked from these web pages.

No contract; limited license

Please make sure that you understand that the information provided here is being provided freely, and that no kind of agreement or contract is created between you and the owners or users of this site, the owners of the servers upon which it is housed, the individual Wikipedia contributors, any project administrators, sysops or anyone else who is in *any way connected* with this project or sister projects subject to your claims against them directly. You are being granted a limited license to copy anything from this site; it does not create or imply any contractual or extracontractual liability on the part of Wikipedia or any of its agents, members, organizers or other users.

There is **no agreement or understanding between you and Wikipedia** regarding your use or modification of this information beyond the [GNU Free Documentation License](#) (GFDL); neither is anyone at Wikipedia responsible should someone change, edit, modify or remove any information that you may post on Wikipedia or any of its associated projects.

Trademarks

Any of the trademarks, service marks, collective marks, design rights, personality rights or similar rights that are mentioned, used or cited in the articles of the Wikipedia encyclopedia are the property of their respective owners. Their use here does not imply that you may use them for any other purpose other than for the same or a similar informational use as contemplated by the original authors of these Wikipedia articles under the GFDL licensing scheme. Unless otherwise stated Wikipedia and Wikimedia sites are neither endorsed nor affiliated with any of the holders of any such rights and as such Wikipedia can not grant any rights to use any otherwise protected materials. Your use of any such or similar incorporeal property is at your own risk.

Jurisdiction and legality of content

Publication of information found in Wikipedia may be in violation of the laws of the country or jurisdiction from where you are viewing this information. The Wikipedia database is stored on a server in the State of [Florida](#) in the [United States of America](#), and is maintained in reference to the protections afforded under local and federal law. Laws in your country or jurisdiction may not protect or allow the same kinds of speech or distribution. Wikipedia does not encourage the violation of any laws; and cannot be responsible for any violations of such laws, should you link to this domain or use, reproduce, or republish the information contained herein.

Not professional advice

If you need specific advice (for example, medical, legal, financial, or risk management) please seek a professional who is licensed or knowledgeable in that area.

Retrieved from "http://en.wikipedia.org/wiki/Wikipedia:General_disclaimer"

Category: [Wikipedia disclaimers](#)