



THE QUANTUM GROUP

What is HIPAA?

What is the Health Insurance Portability and Accountability Act of 1996?

The Health Insurance Portability and Accountability Act ("HIPAA") in the words of Secretary of Department of Health and Human Services (HHS) Governor Tommy Thompson, is:

"The largest and most aggressive regulatory action in healthcare since Medicare. These new federal health privacy regulations set a national floor of privacy protections that will reassure patients that their medical records are kept confidential. The rules will help to ensure appropriate privacy safeguards are in place as we harness information technologies to improve the quality of care provided to patients. Consumers will benefit from these new limits in the way their personal medical records may be used or disclosed by those entrusted with this sensitive information."

"The new protections give patients greater access to their own medical records and more control over how their personal information is used by their health plans and healthcare providers. Consumers will get a notice explaining how their health plans, doctors, pharmacies and other healthcare providers use, disclose and protect their personal information. In addition, consumers will have the ability to see and copy their health records and to request corrections of any errors included in their records. Consumers may file complaints about privacy issues with their health plans or providers or with the Office for Civil Rights."

"The new rules also reflect a common-sense balance between protecting patients' privacy and ensuring the best quality care for patients. They do not interfere with the ability of doctors to treat their patients, and they allow important public health activities, such as tracking infectious disease outbreaks and reporting adverse drug events, to continue."

What are some historical details about HIPAA and how it was created?

HIPAA went through a speedy passage in Congress starting in the Ways and Means Committee of the House in March 18, 1996. HIPAA was signed into law five months later. It passed the House by a vote of 421 to 2 and the Senate by 98 to 0. Following the stipulations of the law, Donna Shalala, then Secretary of the Department of Health and Human Services ("DHHS"), published the Final Privacy Rules in the Federal Register in December 28, 2000.

Within an hour after being sworn in as the 43rd President, Bush suspended implementing new regulations including HIPAA. The current Secretary of DHHS, Governor Tommy Thompson, opened for comments the HIPAA regulations, and his Department went through a detailed analysis of all the implications behind the law. On April 12, 2001, President Bush signed an order ratifying HIPAA's Privacy Rule (with only slight changes from the Clinton version).

The HIPAA regulations were allowed a final revision and additional comments period prior to being published. HIPAA regulations were published in the Federal Register on August 14, 2002, thus, making the HIPAA regulations final.

The Privacy Section of HIPAA became effective April 14, 2003.

How does HIPAA affect a medical practice or business?

HIPAA radically deals with three components of the healthcare sector:

- Transactions of health information
- Privacy of Protected Health Information (PHI)
- Security of all health information

The Privacy component is probably the one that will cause the greatest impact in the healthcare industry. It is a consumer oriented set of regulations designed to give a very strong support to the privacy rights of patients' PHI. Consumers get more control over the use and disclosure of their PHI, and they are given powerful rights to access and change this information. The regulations impose a tremendous change in the routine activities and procedures physicians follow in their offices. It requires setting up protocols, identifying a privacy officer, training the workforce, restricting access to PHI, using the "minimum necessary" amount of information in their communications, rewriting all the contracts with their business associates (diagnostic centers, answering services, billing companies, accountants, attorneys, and so on) and to deploy a multitude of new, specific forms to deal with all aspects of clinical treatment.

What kind of medical businesses are affected?

All healthcare businesses that come into contact with PHI, as defined by HIPAA, are impacted, as well as associated businesses, such as pharmacies, diagnostics, billing and payroll companies, storage of medical records organizations, HMO, third party administrators, and all businesses having self-funded insurance with access to their employees' medical records. We estimate that there are over 1.1 million businesses that will have to comply in the United States.

Who will enforce the HIPAA law?

The Office of Civil Rights of the Department of Health and Human Services will be responsible for enforcing HIPAA.

Is there a whistle-blower provision in the regulation?

Yes, it is very likely at the earliest stages; this will be one of the most common ways to initiate a federal investigation in a provider's office. On the OCR's website - <http://privacyruleandresearch.nih.gov>, a whistle-blower can get instructions on how to file a HIPAA Privacy violation complaint, online or in paper form.

What are the fines associated with violating HIPAA law?

Even if the physician unintentionally violates HIPAA, he/she could face a fine of up to \$25,000 per year for repeatedly violating only one rule, requirement or prohibition out of hundreds in the Final Rule. If this violation extends to several patients, it applies to each one, potentially becoming a huge financial loss for the provider. If the physician knowingly violates HIPAA, he/she could face criminal charges carrying a fine of up to \$250,000 and 10 years in prison.

What was the deadline for HIPAA compliance?

The deadline for the Privacy Component of HIPAA was April 14, 2003. The deadline for the Transaction Component, dealing with the IT process, was October 16, 2003.

What has happened since April 14, 2003?

Since the effectiveness of HIPAA Privacy, the medical community had begun to move forward in earnest. A recent survey conducted by the Atlantic Information Service on the compliance of HIPAA was titled "The Good, The Bad, and The Ugly of HIPAA Compliance." It noted the progress made by the HMOs as "good," the hospitals as the "bad" and the physicians as the "ugly." The survey further noted, "with the exception of a handful of large multi-specialty medical groups, the vast majority of group practices and physicians have done "nothing whatsoever" to comply with the privacy rules and show little or no tendency to do so."

What is the projected cost for the healthcare industry to become compliant?

The cost to the healthcare industry to become HIPAA compliant has been estimated to be anywhere between \$20 and \$42 billion in the next five years.

The Department of Health and Human Services estimates that the HIPAA regulations will cost the healthcare industry \$3.2 billion for the first year and \$17.6 billion over the next 10 years. The regulations qualify those estimates as conservative.

Analysis done by healthcare industry groups paint a much different picture. In December 2001, the American Hospital Association released a report concluding that for hospitals alone, HIPAA compliance could cost up to \$22.5 billion over the next five years--not with all the regulations but with three key provisions it asserts DHHS omitted from its cost estimates. The left-out provisions are the "minimum necessary" requirement, directing organizations to release only

the minimum amount of patient information necessary to accomplish an intended purpose; the "business partner" provision, requiring healthcare entities to make sure all of their business partners comply with HIPAA; and the "state law preemption," requiring compliance with all state laws that provide greater privacy protections than HIPAA.

The analysis further asserts that HHS "may have seriously underestimated" the impact of other HIPAA provisions. "These costs are just the tip of the iceberg--the proposal's total impact on hospitals hasn't been fully considered," said AHA president Dick Davidson in a statement.

The Blue Cross Blue Shield Association commissioned its own analysis of the medical privacy rules in February 2002. Their resulting report, by the management consulting firm Robert E. Nolan Company, concluded that the costs of compliance for the entire healthcare industry would reach \$42.9 billion over five years. "There are a lot of things they [DHHS] didn't account for," says Alissa Fox, the Association's Executive Director of policy. "They underestimated how detailed and prescriptive these rules are. They underestimated how much things cost." Because of the nature of the Act, yearly reviews of the provider's protocols and procedures are certain. New regulations and new interpretations are going to be the rule.