

Health Insurance Portability and Accountability Act (HIPAA) of 1996

What is HIPAA?

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 was signed into law by former President Bill Clinton on August 21, 1996. Conclusive regulations were issued on August 17, 2000, to be instated by October 16, 2002. HIPAA requires that the transactions of all patient healthcare information be formatted in a standardized electronic style. In addition to protecting the privacy and security of patient information, HIPAA includes legislation on the formation of medical savings accounts, the authorization of a fraud and abuse control program, the easy transport of health insurance coverage, and the simplification of administrative terms and conditions.

What does HIPAA cover?

HIPAA encompasses three primary areas, and its privacy requirements can be broken down into three types: privacy standards, patients' rights, and administrative requirements.

1. Privacy Standards. A central concern of HIPAA is the careful use and disclosure of protected health information (PHI), which generally is electronically controlled health information that is able to be distinguished individually. PHI also refers to verbal communication, although the HIPAA Privacy Rule is not intended to hinder necessary verbal communication. The U.S. Department of Health and Human Services (USDHHS) does not require restructuring, such as soundproofing, architectural changes, and so forth, but some caution is necessary when exchanging health information by conversation.

An Acknowledgment of Receipt Notice of Privacy Practices, which allows patient information to be used or divulged for treatment, payment, or healthcare operations (TPO), should be procured from each patient. A detailed and time-sensitive authorization can also be issued, which allows the dentist to release information in special circumstances other than TPOs. A *written consent* is also an option. Dentists can disclose PHI *without* acknowledgment, consent, or authorization in very special situations, for example, perceived child abuse, public health supervision, fraud investigation, or law enforcement with valid permission (i.e., a warrant). When divulging PHI, a dentist must try to disclose only the *minimum necessary* information, to help safeguard the patient's information as much as possible.

It is important that dental professionals adhere to HIPAA standards because healthcare providers (as well as healthcare clearinghouses and healthcare plans) who convey *electronically* formatted health information via an outside billing service or merchant are considered *covered entities*. Covered entities may be dealt serious civil and criminal penalties for violation of HIPAA legislation. Failure to comply with HIPAA privacy requirements may result in civil penalties of up to \$100 per offense with an annual maximum of \$25,000 for repeated failure to comply with the same requirement. Criminal penalties resulting from the illegal mishandling of private health information can range from \$50,000 and/or 1 year in prison to \$250,000 and/or 10 years in prison.

2. Patients' Rights. HIPAA allows patients, authorized representatives, and parents of minors, as well as minors, to become more aware of the health information privacy to which they are entitled. These rights include, but are not limited to, the right to view and copy their health information, the right to dispute alleged breaches of policies and regulations, and the right to request alternative forms of communicating with their dentist. If any health information is released for any reason other than TPO, the patient is entitled to an account of the transaction. Therefore, it is important for dentists to keep accurate records of such information and to provide them when necessary.

The HIPAA Privacy Rule determines that the parents of a minor have access to their child's health information. This privilege may be overruled, for example, in cases where there is suspected child abuse or the parent consents to a term of confidentiality between the dentist and the minor. The parents' rights to access their child's PHI also may be restricted in situations when a legal entity, such as a court, intervenes and when a law does not require a parent's consent. For a full list of patient rights provided by HIPAA, be sure to acquire a copy of the law and to understand it well.

3. Administrative Requirements. Complying with HIPAA legislation may seem like a chore, but it does not need to be so. It is recommended that you become appropriately familiar with the law, organize the requirements into simpler tasks, begin compliance early, and document your progress in compliance. An important first step is to evaluate the current information and practices of your office.

Dentists will need to write a *privacy policy* for their office, a document for their patients detailing the office's practices concerning PHI. The ADA's *HIPAA Privacy Kit* includes forms that you (the dentist) can use to customize your privacy policy. It is useful to try to understand the role of healthcare information for your patients and the ways in which they deal with the information while they are visiting your office. Train your staff; make sure they are familiar with the terms of HIPAA and your office's privacy policy and related forms. HIPAA requires that you designate a *privacy officer*, a person in your office who will be responsible for applying the new policies in your office, fielding complaints, and making choices involving the minimum necessary requirements. Another person with the role of *contact person* will process complaints.

A *Notice of Privacy Practices*—a document detailing the patient's rights and the dental office's obligations concerning PHI—also must be drawn up. Further, any role of a third party with access to PHI must be clearly documented. This third party is known as a *business associate* (BA) and is defined as any entity who, on behalf of the dentist, takes part in any activity that involves exposure of PHI. The *HIPAA Privacy Kit* provides a copy of the USDHHS "Business Associate Contract Terms," which provides a concrete format for detailing BA interactions.

The main HIPAA privacy compliance date, including all staff training, was April 14, 2003, although many covered entities who submitted a request and a compliance plan by October 15, 2002, were granted one-year extensions. It is recommended that dentists prepare their offices ahead of time for all deadlines, which include preparing privacy policies and forms, business associate contracts, and employee training sessions.

For More Information on HIPAA

For a comprehensive discussion of all of these terms and requirements, a complete list of HIPAA policies and procedures, and a full collection of HIPAA privacy forms, contact the American Dental Association for a *HIPAA Privacy Kit*. The relevant ADA Web site is www.ada.org/goto/hipaa. Other Web sites that may contain useful information about HIPAA are:

- USDHHS Office of Civil Rights: www.hhs.gov/ocr/hipaa
- Work Group on Electronic Data Interchange: www.wedi.org/SNIP
- Phoenix Health: www.hipaadvisory.com
- USDHHS Office of the Assistant Secretary for Planning and Evaluation: <http://aspe.os.dhhs.gov/admnsimp/>

Bibliography

1. *HIPAA Privacy Kit*
2. <http://www.ada.org/prof/prac/issues/topics/hipaa/index.html>