HIPAA

HIPAA – Health Insurance Portability and Accountability Act of 1996

What is HIPAA?

President Clinton signed the Health Insurance Portability and Accountability Act (HIPAA) into law in August of 1996. HIPAA has its roots in Clinton's proposed universal health care plan of 1993. When that proposal failed, Congress eventually passed the Kennedy-Kassebaum Act which was most known for allowing an individual to move their health insurance from one job to another. The rest of the Act dealt with reducing healthcare fraud and abuse, enforce standards of health information and guaranteeing the security and privacy of health information.

HIPAA eventually will include seven sets of regulations but it is actually divided into four sections.

- security and privacy of health information
- standardized health information transactions
- standardized code sets and
- national identifiers for providers, health plans and employees*

Privacy Regulations

- Became effective in April, 2001 and health plans and providers had to comply by April 14, 2003. Small health plans have until April 14, 2004.

A federal regulation defining administrative steps, policies and procedures to safeguard individuals' personal and private health information (PHI), establishes a federal floor of safeguards to protect the confidentiality of health information. State laws, especially those states with more stringent privacy protections, will continue to apply over and above the new federal privacy standards.

The health care industry will have to protect the privacy of patients' medical information, will have to inform patients in writing about how the information will be used, and will have to track and manage the information the way they told the patients they would.

*not to be completed until 2005.

The regulations cover any individually identifiable information, whether it was disclosed during oral conversations, electronic transmission, or written documentation. It sets an industry standard for disclosing only the minimum amount of information necessary to satisfy an authorized request for patient information.

All covered entities will have to produce three sets of forms; a notice to patients of the privacy procedures of that organization to include patient rights, a consent form authorizing the sharing of information, and an authorization form that enables usage of information that may fall outside treatment.

Covered entities include health plans, health care providers and health information clearinghouses. The privacy rule also holds covered entities liable for rule violations of their business associates, or those with whom they exchange information or contract for administrative or other services.

Security Standards

Will outline the minimum administrative, technical, and physical safeguards required to prevent unauthorized access to health information. Businesses that transmit or maintain electronic health information must develop a security plan. The final security standards have not been developed and the deadline is April 21, 2005.

Most of these regulations involve software issues, staff training and the physical security of health information.

Transaction Standards

The "Transaction and Code Sets" final rule provides standards for electronic transactions and code sets that health care providers and payers use to identify diagnoses, drugs, and procedures.

In summary, all providers will use – and all health plans must accept – the same transaction standards. The standard diagnostic and procedural code sets to be used for dentistry are the CDT codes administered by the American Dental Association.

These set out standardized ways that patient health, administrative, and financial data can be transmitted. Most of these regulations went into effect in October of 2002. The regulations specify a standard format for verification of coverage, authorization for procedures, and referrals.

It also required covered entities to adopt a set of nationally recognized codes – used to identify medical procedures, diagnostic criteria, patient demographics and other health-related services and supplies.

FAQs

Who is responsible for this within my dental office?

Ultimately, the dentist.

HIPAA compliance for healthcare providers has been difficult and expensive. Your dentist should educate and train the dental office staff on compliance procedures. The protection of individually identifiable patient information is a major challenge.

In large offices this job may require a full-time position. More likely, the office manager should be responsible but each employee should review the policies.

HIPAA workload is largely driven by two things; the volume of health information maintained and the number of transactions with those within and outside of the health care system.

Will dental offices have to become soundproofed?

No. Once the initial regulations were released over two years ago, many feared the language would force all medical offices to become soundproofed to protect patient privacy. Over 10,000 letters of comment were sent to the Secretary of Health and Human Services relaying concerns such as this. Modifications were made and soundproofing of offices is not required under HIPAA.

What information is protected?

Protected information is health information that identifies an individual and is maintained or exchanged electronically or in hard copy. If the information has any components that could be used to identify a person, it would be protected. Examples would be a social security number or address.