Health Insurance Portability and Accountability Act of 1996

The Health Insurance Portability and Accountability Act, commonly referred to as HIPAA, became a federal law in 1996. The act contains insurance reform provisions and introduces the establishment of a fraud and abuse control program when rendering medical care to Medicare patients. In 2000, regulations were established to protect the privacy of personal health information maintained by health care providers, health plans, hospitals, health care clearinghouses, and health insurers. These regulations became effective in 2003 (2004 for small health plans). Violators of HIPAA may be subjected to fines, prison, or both.

HIPAA is organized into three parts:

- Privacy regulations. HIPAA regulations guide health care providers with overall privacy measures, such as turning the charts toward the wall and making sure the computer screen is not visible. Five forms are required (privacy notice, acknowledgment, authorization, business associate agreement, and trading partner agreement).
- Transaction standards. Requirements must be followed when putting the office software into HIPAA compliance.
- Security regulations. HIPAA requires health care providers to keep computers safe.

The first two parts had 2003 deadlines for compliance and the third part has a 2005 deadline.

To adhere to the HIPAA regulations, a medical practice must have an appointed privacy official draft privacy policies and procedures, and implement a program to educate and train all physicians and employees to the mandates of HIPAA. These policies become part of the office policies and procedures manual.

Confidentiality (privacy) policies must be followed. Refrain from talking about patients and their problems where outsiders may overhear. A medical record contains privileged information; therefore it must not be mislaid within viewing of other individuals. State laws may require the release of information for the good of society. Examples include the following:

- Births, stillbirths, and deaths
- Certain communicable, infectious, or contagious diseases
- Child or elder abuse or neglect
- Incest
- Spousal rape
- Suspicious wounds
- Injuries inflicted by oneself or by the acts of another by means of a knife, gun, pistol, or other deadly weapons
- Assault or abusive conduct
- Injuries inflicted in violation of any penal law
- Known or suspected drug abuse
- Epileptic seizures and related disorders

Every precaution must be used when transmitting information by voice mail, e-mail, or fax.

Release of Information

Consent

Both federal and state laws exist concerning the release of medical information. With HIPAA regulations, patients have the right to know how their health information is used and may exercise control over the content of the information disclosed. Patient consent is not an option; providers must obtain a consent form. Patients can be denied treatment if they refuse to give consent. A one-time signed consent form (see sample) is required before physicians use or disclose personally identifiable health information for treatment, payment, or routine health care operations, such as performance reviews, audits, training programs and certain types of fundraising.

There are three exceptions when consent is unnecessary:

1. When there is an emergency situation; however, written consent must be obtained as soon as reasonably possible after treatment.
2. When a language barrier occurs, the consent is implied.
3. When treating prison inmates.

Authorization

A signed authorization form (see sample) must be obtained for use and disclosure of protected health information not included in the consent. Disclosure is allowed only after written consent by the patient, guardian in the case of a minor, or if subpoenaed by a court. A minimum set of elements must be included disclosing the purpose for which the health care information is to be used and disclosed. Authorization forms should be retained in the patient chart. These documents become part of the permanent medical record. Only the information indicated in the authorization may be disclosed to physicians, insurance companies, and attorneys. For cases of continuity of patient care, in which requests are received to move records from hospital to hospital, physician to physician, or hospital to nursing home, it is not necessary to have the authorization form signed by the patient. The wording on the release of information form must meet Medicare's requirements for confidentiality.

Patients have the right to ask for an accounting of all health information disclosures (using the authorization form) made by the provider in the past six years. This request must be answered within 60 days. The majority of requests are provided at no charge, but in certain instances a fee may be charged.

A patient's request for his or her medical record should be honored; however, caution should be taken because a patient may become emotionally upset due to an inability to interpret technical or medical terms. Photocopies of the records should be sealed in an envelope or faxed using a special authorization form. Patients should sign a receipt for any radiographic films removed from the office. Consultation reports from other physicians (even if stamped "confidential") and accounting records may be released to a patient. Patients waive their right to confidentiality when filing a suit against the physician.

In the event of litigation (a lawsuit), the physician's lawyer has access to the patient's medical record, but must not release medical information to any other party unless subpoenaed or unless the patient has signed an authorization.

If asked to make photocopies or if a photocopying service visits the office, the pages should be numbered to ensure pages are not missing after the photocopying is completed. A fee may be charged for the copies.

Federal and state agencies may have photocopies of the medical record. Medicare, Medicaid, and Tricare may request copies of the medical record to verify medical necessity. A signed authorization form is preferable. The information may only be used for audit and may not be released. Special attention is required when releasing information to employers even with the patient's signature. Any publication release in which the patients medical record or photograph will be used must be worded to indicate the manner in which the information is to be used.

Psychiatric records should always have the permission of the physician prior to release of medical records, even with a signed authorization. The Privacy Act of 1974 allows a physician to prevent patients (Medical and Tricare) from gaining access to privileged information, such as psychiatric information, by noting in the chart that they believe knowledge of its conteI1ts would be detrimental to the patient's best interests. Legal counsel should be sought prior to releasing any medical information on a patient who has a positive human immunodeficiency virus (HIV) test for acquired immune deficiency syndrome (AIDS).

Some states have restricted access. The authorization form must have specific sensitive information listed and the inclusive dates of treatment. The individual requesting the information should be instructed to destroy the information after use. Sensitive information should be maintained in a separate medical record from the general patient health record and locked in a private file.

Verbal and Nonverbal Communication

The patient sign-in log should be kept confidential by using layered, perforated, prenumbered tickets. When the patient arrives in the office, the patient signs the sheet. The adhesive label is removed and attached to the patient visit log, which is kept out of sight. This may be kept in a three-ring binder for future reference. Prenumbering will remain revealing the patient number and time of arrival. In a small office setting, the patient may check in verbally when they arrive and the medical assistant will note the arrival time on the encounter form.

A notice should be posted in the reception area in the health care setting explaining Health Insurance Portability and Accountability (HIPAA) policy on confidentiality. A copy of the privacy practice should be handed to all new patients. Acknowledgement of receiving a copy must be signed by the patient and the date must be recorded within the office computer software on the registration screen or in the patient chart on the registration form.

Regulations with regard to telephone confidentiality is also included in HIPAA. The caller can be identified by his or her home, work, or cell number. Questions from people who cannot be identified with certainty should not be answered. A cellular telephone is a wireless telephone and cellular signals are not secure. Other people may be able to listen to the conversations with a scanning radio. If using a speaker phone, permission must first be recurred from the caller and privacy for the conversation must be ensured. Voice mail is an excellent way to leave a message for the patient, but caution must be used by leaving only minimal information that contains the name of the person to contact and the phone number.

Patients should sign an authorization to release information to a spouse or adult children. Such a release allows health care providers to speak with the authorized individuals even if there is a possibility of being overhead by another authorized individual. Such a release also makes it permissible to discuss a patient's condition or lab test results in a joint treatment area or over the telephone. Voices should be kept lowered when possible. Follow-up appointment reminders should be mailed in a sealed envelope. Postcards should be avoided to ensure confidentiality.

HIPAA compliance mandates confidentiality with regard to medical records and medical software, including appointment schedulers, electronic progress or chart notes, and accounts receivable information. Passwords or IDs should be assigned to staff to access the specific sites they are allowed to access. Not all employees will be required to access all areas of software. For optimum security of medical records, file storage cabinets must have locks. Optimum office design would include a secured file and records room. Any documents that require disposal should be shredded to ensure confidentiality.

Written correspondence must remain confidential. Confidential information should never be circulated in a memo. HIPAA does not prohibit the use of tapes for dictation or outsourcing or transcription; however, specific language addressing confidentiality must be inserted in contracts with outside vendors or business associates. Open network transmission of patient information requires the use of password protection, encryption, and authentication. Patients should acknowledge that they understand the risk of e-mailing or faxing information.

Transaction standards

HIPAA legislated that the federal government adopt national electronic standards for automated transfer of certain health care data between health care payers, plans and providers, thus eliminating all nonstandard formats. The standard code set is ANSI ASC X12N v4010 837, and was implemented in 2001 with compliance by October 2002. This electronic claim may be referred to as the Health Care Claim: Professional. The field data is almost identical to data required on the CMA-1500 claim form.

AMERICAN ASSOCIATION
OF MEDICAL ASSISTANTS
20 N. WACKER DR., STE. 1575
CHICAGO, ILLINOIS 60606
website: www.aama-ntl.org 800/228-2262