ACUPUNCTURE Today

# Confidentiality -- What Is HIPAA? Part Two

## COMPLYING WITH HIPAA

Fred Lerner, DC, PhD, FACO

Here are some simple steps to take regarding HIPAA compliance:

1. Take patient privacy and confidentiality very seriously. The penalties for violation are very steep, and there are felony charges that could potentially cause the loss of your license.
2. Designate someone in your office who can create a procedure to handle protected health information; if not, you will need to employ an outside party.

    a. Such a person will need to develop a written HIPAA policy that all must follow in the office.
    b. They will also need to train office staff on how to handle protected health information, including under what circumstances protected health information may be disclosed.

3. Use consent/authorization documents that the patient signs.
4. Don't discuss ANY medical information with any third parties unless WRITTEN consent/authorization has been obtained.
5. Be careful when discussing a patient's protected health information with office staff.

    a. Disseminate it on a need-to-know basis.
    b. Assign user IDs and passwords to anyone with access to electronic information (computer billing software, voice dictation programs, etc.).

        i. You may want to make sure that different employees are limited to only the access they need. For example, the billing person only has access to the billing, not medical record information.

    c. Contact your practice management software company and make sure the version you are using is HIPAA compliant.

6. Use passwords and security programs to protect and maintain computer files. a. Electronic transmission of protected health information must be secure.

    i. For e-mail, obtain written consent from the patient and use encryption software.
    ii. Use electronic signatures to authenticate who sent the e-mail.
    iii. Use auditing software to monitor who sent what and when.

7. Create a policy for the destruction and/or retention of medical records that includes e-mail communications.

There are four parts to HIPAA's "administrative simplification":

I. Electronic Health Transactions Standards

1. Use of ANSI formats (except for claims and first injury reports).
2. Use of standard code sets

    a. Description of diseases, injuries and other health problems, and their causes, symptoms and actions, must be uniform.

II. Unique Identifiers for Providers, Employers, Health Plans and Patients

III. Security of Health Information & Electronic Signature Standards

1. There will be a uniform level of protection of all health information that is:

    a. housed or transmitted electronically and that
    b. pertains to an individual

2. The physical storage and maintenance, transmission, and access to records will be safeguarded.
3. This will apply to all individual health information that is maintained or transmitted.

IV. Privacy and Confidentiality

1. Limit the non-consensual use and release of private health information.
2. Give patients new rights to access their medical records and to know who else has accessed them.
3. Restrict most disclosure of health information to the minimum needed for the intended purpose.
4. Establish new criminal and civil sanctions for improper use or disclosure.
5. Establish new requirements for access to records by researchers and others.

Conclusion

Like it or not, you will have to comply with HIPAA. If all your information is kept on paper, you do not have to comply on the surface; however, if you plan to fax, e-mail or in any other way electronically send information, you will be responsible. As the deadline approaches, managed care entities will require you to practice the HIPAA way. Several consultants will no doubt offer their services to guide you through the HIPAA "jungle" to make sure you are compliant. As always, check them out and make sure they are knowledgeable and responsible for their work.

OCTOBER 2002