

of sonment	Offense
	Single violation of a provision violations with penalty of \$100 as each violation is for a different
	Multiple violations of an identical or prohibition during a calendar

HIPAA Privacy Laws: Violators Face Jail Time, Fines up to \$250,000 and No Payments by Insurance Companies

The HIPAA patient privacy and security laws are real - as are the penalties for their violation. To assure the accountability of those who had access to personal health information (PHI), the U.S. Congress required the imposition of civil and criminal penalties for any entity or person that uses PHI improperly. The penalties for improper uses are described below:

Some insurance companies have already indicated they will no longer pay providers who are not compliant. Sooner or later, you are going to have to work with your lawyer, a consultant who has HIPAA expertise (whose HIPAA experience is more than the last six months) or utilize a computer program to create administrative and compliance manuals that are customized to your specific practice. Essentially, these are the only ways to become HIPAA-compliant. Boilerplate manuals will not qualify.

Also, some organizations have mistakenly suggested that you need only be concerned if you are processing your insurance claims electronically. This is simply not the case. Let me give you just two reasons why compliance is not an option.

Civil Penalties

Monetary penalty	Term of imprisonment	Offense
\$100	N/A	Single violation of a provision (can be multiple violations with penalty of \$100 each, as long as each violation is for a different provision).
\$25,000	N/A	Multiple violations of an identical requirement or prohibition during a calendar year.

Criminal Penalties

Monetary penalty	Term of imprisonment	Offense
Up to \$50,000	Up to one year imprisonment.	Wrongful disclosure of individually identifiable health information.
Up to \$100,000	Up to five years	Wrongful disclosure of individually identifiable health information committed under false pretenses.
Up to \$250,000	Up to 10 years	Wrongful disclosure of individually identifiable health information committed under false pretenses, with intent to sell, transfer, or use for commercial advantage, personal gain, or malicious harm.

Business Associate Agreements

Unless you have no plans of ever getting paid by a third-party payer, you will be asked to sign various forms of Business Associate Agreements. Some of these will include very stiff provisions holding you accountable for complying with various aspects of the HIPAA regulations.

If you haven't seen them already, you soon will. A quick look at the "Obligations and Activities" section of any of these agreements will show you very clearly that you must abide by most, if not all, HIPAA privacy and security provisions. You will be required contractually and legally to abide by the majority of the provisions in the HIPAA regulations the minute you sign your first Business Associate contract. Violation of this agreement will have severe and immediate penalties as the payers are under just as much scrutiny as providers are. And as we are already seeing, if you don't sign the contract, you won't get paid.

So even if your practice doesn't file claims electronically, you will still be expected to sign Business Associate Agreements with most, if not all, third-party payers you work with. These Business Associate Agreements will obligate you to be compliant with the HIPAA privacy laws regardless of how you file your claims. This is where the "long arm of HIPAA" ensures that every provider in the system is abiding by the patient privacy and security regulations.

But this is not the only reason you are going to want to be HIPAA privacy-compliant by the April 14, 2002, deadline.

Patient Confidence and Expectation

The HIPAA regulations empower your patients with new rights regarding the privacy of their personal health information. As the months go by, they will become more and more aware of these rights. They will come to expect every health care provider they see to be in accordance with new patient privacy laws. They may even feel obliged to change providers if the doctor they are seeing is not willing to become HIPAA-compliant. The proverbial question will be, "Why doesn't my doctor want to protect my privacy?"

Your patients may not understand the difference between a "covered entity" and a non-covered entity. What they will understand is if you are complying with the federal standards created to protect the privacy of their health information. They will want to hear you say: "Our office is HIPAA-compliant."

Becoming HIPAA privacy-compliant tells them that you acknowledge all of the rights they now have and have the forms and documents needed to accommodate their requests. At the very least, you must have written policies, procedures and forms to:

- provide your patients access to their records;
- allow them to amend their records;
- allow them to specify how access to their health information is restricted and from whom;
- enforce the "minimum necessary use" of their health information;
- demonstrate how you safeguard your patients' information both in receipt and storage;
- establish a published policy for employee sanctions for breach of policy; and
- ensure that all of your sub-contractors and service providers are in like compliance.

This should come in the form of two manuals: a compliance manual and an administrative manual. The compliance manual will provide all of the information and procedures your office needs to comply with when handling confidential patient information. It will state specifically what your office does and doesn't do to protect your patients' confidentiality. These procedures will be the rule by which your office will be measured should you ever be audited or have a complaint filed against you. This is why they must be specific to your office and not "boiler plated."

The administrative manual is your in-house recording of specific actions taken by your office to ensure the confidentiality of your patients' information. This will also be where you record any challenges by your patients to the information contained in their records and other events regarding confidentiality and security.

Should you violate these new regulations because you chose not to be HIPAA privacy-compliant, you will be violating numerous Business Associate Agreements and will risk various forms of censure and penalties based on the manner of the complaint against you and how it is viewed by the Office of Civil Rights, which has been empowered to enforce HIPAA compliance.

Worse yet, you risk violating patient trust. You will put yourself and your staff in the uncomfortable position of explaining just why it is that you chose not to adopt procedures that would protect the privacy of your patients' personal health information. This will be especially painful should a complaint be filed before you make your office HIPAA-compliant.

Doctors of chiropractic have always been known for their proactivity when it comes to patients' rights. The new HIPAA laws are no different.

As a longtime advocate and defender of chiropractic practice rights, I have defended numerous doctors against a wide variety of accusations and lawsuits. I can tell you firsthand that accusations by patients are the toughest. This will be especially true for those who are accused of violating their patient's privacy when becoming compliant is not that much additional work and you have the next four months to do it.

The cost of becoming HIPAA-compliant is relatively small compared to the penalties for noncompliance. If you are a small, one-to-three-doctor office, it is unlikely that you will need to spend more than \$500 for a consultant or a computer program that will produce customized manuals specific to your practice. (Be wary of spending under \$200, as I have yet to see anything priced that low that wasn't boilerplate.)

Just be certain that what you are getting requires you or your staff to enter information specific to your practice that creates custom manuals; that it includes both the Federal and the state regulations where applicable; and that you end up with separate compliance and administrative manuals.

Protect your office now by becoming HIPAA-compliant. Do it to ensure you will get paid by third-party payers, and do it so that your patients will know that you care enough about the privacy of their health care information to become complaint with the new laws designed to protect them.

Michael J. Schroeder, Esq
Santa Ana, California

Mr. Schroeder is a longtime member of the National Association of Chiropractic Attorneys (NACA), and the vice president for the last 17 years. He was selected as NACA's Chiropractic Attorney of the Year in 1995.

JANUARY 2003