

## Are Your Sign-In Sheets HIPAA Privacy Violations?

Rob Sherman, Esq.

1. Your sign-in sheets are in public view for everyone to see.
2. You have a discussion with a patient within earshot of other patients.
3. You treat in open areas, where patients are in one large room together.

Are these activities now in violation of federal privacy laws?

You've probably heard of HIPAA - the Health Insurance Portability and Accountability Act, passed in 1996. It was named for the insurance "portability" it brought employees who left one job for another.

But HIPAA also contained other provisions, most notably privacy requirements for business entities and providers. Remember the flood of privacy notices you received from financial institutions and other businesses a while back? These were required under HIPAA and the Graham-Leach-Bliley Act.

Now it's your turn. Although the final privacy rules are still under review, providers have until April 14, 2003 to implement them. For the chiropractic office, compliance is not overly difficult. The following are answers to frequently asked questions (FAQs) about the privacy rules.

FAQ #1: Why privacy rules?

In years past, you wrote patient records on paper, filed them in a folder and placed them in a cabinet. Maybe you even locked the cabinet, so access to these records was reasonably restricted.

Electronic data transfer has changed the way information is exchanged: Patient records are no longer secure. Many examples exist where patient records find their way into loan application recommendations and other areas where these records have no business influencing decisions. The electronic transfer of data has created an arena ripe for abuse. Congress passed the HIPAA to deal with this problem.

FAQ #2: Do the rules apply to my practice?

HIPAA privacy rules apply to any health care entity that transfers records electronically. If you deal with insurance in any manner, you probably transfer some records electronically. If so, HIPAA applies to all of your patient records. It also applies to those business entities, such as billing or consulting services, that may have access to patient records.

FAQ #3: What does HIPAA require me to do?

1. Adopt written privacy procedures. Perhaps the most onerous requirement of HIPAA is that providers must develop written privacy policies. These policies will cover patient record disclosure

procedures and the manner in which patient records are maintained.

It is anticipated that chiropractic associations and other third parties will draft these documents for use by their members. You should customize these "templates" to suit the procedures applicable to your individual practice.

Attorney Ross Lanzafame, New York Chiropractic Association general counsel, distributed a "privacy notice" to all members of the National Association of Chiropractic Attorneys (NACA). If your association attorney is a member of this group, he or she received an electronic copy of the notice you can easily access at your association's web site.

The privacy notice written by Attorney Lanzafame contains a "consent" that the patient "must" sign. However (and this is an important "however"), it is not clear if the final rule will require a signed patient consent. The Bush administration is listening to provider complaints about the currently proposed rule, and wants to drop the requirement for a signed patient consent. Instead, the new rule would require a "good-faith" effort by the provider to inform patients of their privacy rights.

Is this a big deal for a chiropractic office? Probably not. Signing a patient consent form is easy, but the change in the rule would seemingly allow the posting of the notice in the reception area or at other highly visible areas around the office. A signed form would not be required. For offices that do not want to add six additional pages within the patient file, the dropping of this requirement is a welcome change!

Can you still use patient sign-in sheets? Yes. HIPAA issued a guidance statement indicating that sign-in sheets are still permissible. Your privacy notice should explain to the patient the use of patient sign-in sheets. For instance, it may contain a provision that states:

"The practice maintains patient sign-in sheets that are visible and accessible to patients, staff and others who may enter this office."

The privacy notice should also contain a list of patients' rights, which includes an explanation of how others may gain access to patient records. All states allow for patient access to records, but doctors who continue to violate those rights now face federal law violations. You can still charge for copying records under applicable state law, but it is ill advised for you to refuse to relinquish copies of patient records because of an unpaid bill.

2. Keep records secure. Most offices will have to make some modifications in the manner in which records are maintained. Attorney John Peick, a Bellevue, Washington NACA member, explains that you should protect your computer records through the use of passwords; log-on/log-off sequences; antivirus programs and updates; audit trails to access patient records; firewalls against hackers; and backups. You should also shred paper records before disposal and assure that computer hard drives do not contain patient information when discarding old computers.

3. Designate a privacy officer. HIPAA law requires health care entities to designate specific individuals to serve as privacy officers. For a small chiropractic office, you could name an employee or designate yourself as the officer. This individual is responsible for employee training on privacy procedures.

You should keep minutes of these training meetings in a "privacy training" notebook and have employees acknowledge their participation in these training events.

4. Obtain patient authorization before using patient records for marketing. If you plan to use

patient records for marketing through third parties, you must have a signed patient authorization. This requirement will not change, even if the final rules do relax the patient consent requirement discussed earlier.

Attorney Peick explains that it is not necessary for you to obtain authorization when the marketing communication is face-to-face; concerns products or services of nominal value; or concerns health-related products or services you provide. For instance, it would not be necessary to obtain authorization to sell nutritional supplements to patients as part of their health care regime if the provider sells these products. Authorization would be required, however, if another vendor were selling the products to the patient.

Further, if you market a patient newsletter, you should explain in your privacy notice to patients that you distribute such a publication and they may "opt-out" by sending notice to you that they want to be removed from the distribution list. The doctor should place a similar notice within each issue of the newsletter.

5. Maintain contracts with business associates. HIPAA requires you to enter into agreements with "business associates" who have access to patient records, to assure that these records are not disclosed improperly. Attorney Peick suggests that such business associates include: independent contractors treating your patients; computer consultants; management consultants; billing services; record transcription services; radiological labs; clinical labs; and vendors. Personal injury attorneys are not included, but an attorney defending a malpractice case or discipline case would be.

Again, thanks to Attorney Lanzafame, a template for these business associate agreements was provided to all NACA attorneys for distribution to association members. You can easily adapt this agreement to the specific circumstances of each agreement.

FAQ #4: Can I discuss patient health care issues with other doctors or my staff?

Opponents argued that the original rules had an unintended result of punishing providers who spoke to other physicians and staff members about patient health issues. The Bush administration is making sure that the final rules do not extend to this activity or to information that is inadvertently overheard by others.

FAQ #5: Do I have to build walls in my open treatment rooms?

The rules were also not intended to require a provider to change the configuration of the practice. You don't need to build new walls or tear apart your office to comply with the HIPAA, but you should take added precautions to avoid disclosing patient information in these open areas.

FAQ #6: What are the penalties for not complying?

The new law imposes civil and criminal penalties for noncompliance. Fines range from \$100 to \$25,000 per violation of a civil nature. Criminal violators may incur fines up to \$250,000 and 10 years in jail.

Online Filing

Besides the privacy provisions contained in this story, HIPAA also requires providers to establish new Final Electronic Transactions and Code Sets by October 16, 2002. Congress has permitted providers a one-year extension of these electronic transfer requirements if the doctor has established an Electronic Health Care Transactions and Code Sets Standards Model Compliance

Plan. You can file your compliance plan on line at <http://cms.hhs.gov/hipaa/hipaa2/ascaform.asp>. For more information about HIPAA, go to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) page at [www.hcfa.gov/hipaa/hipaahm.htm](http://www.hcfa.gov/hipaa/hipaahm.htm).

### Begin Today

As we wait for the final rules to become law, you can begin implementation today by becoming aware of the obvious areas within your practice that demand immediate attention. Are your patients' computerized records secure? When was the last time you updated your virus protection? Do you even own a paper shredder?

Take the first step by designating a staff member to serve as privacy officer. This designee can begin recommending ways to better protect patient privacy.

Yes, it is true that the federal government has created an added burden to your practice. But your association will ease implementation by providing you with the necessary tools to comply with these privacy requirements. Besides, wouldn't you expect this same protection of your health care records if you were the patient?

*Rob Sherman, Esq.*

*Columbus, Ohio*

[shermanrps@aol.com](mailto:shermanrps@aol.com)

[www.ExcellenceInChiropractic.com](http://www.ExcellenceInChiropractic.com)

JULY 2002