Dynamic Chiropractic

Everything You Ever Wanted to Know about HIPAA - But May Still Be Afraid to Ask

INTERVIEW WITH HIPAA AUTHORITY HOWARD ROSS

Editorial Staff

DC: Many doctors are hearing and talking about HIPAA, the Health Insurance Portability and Accountability Act of 1996, but are uncertain about their obligations. Can you give us your background on HIPAA, and your level of authority?

Ross: I have been a health insurance and health management consultant to chiropractors since 1972. For the last three months, I have been specifically working on the issues of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) from the standpoint of what's going to be required to teach in my seminars, and the management of the doctor's office relative to HIPAA. My office has been assembling and coordinating all the HIPAA documents available from the public and private sectors, so that we have a decent database of information and briefs.

I'm working with a number of groups, including the Maryland Health Care Commission, which was sanctioned in 1999 as a consortium under a state grant, and also has a contract grant through the Department of Health and Human Services (DHHS) for the assistance and implementation of HIPAA. I'm on the commission's structure committee, which consists of about 30 people. I'm also on the North Carolina Health Information and Communications Alliance. In both of these relationships, I worked on and assisted in the preparation of the *Guide to Privacy Readiness*, which was produced by the Maryland Health Care Commission, and a program developed by the North Carolina Health Information and Communications Alliance called *Early View*, which was sold to its member doctors to determine if they were in compliance with policies and procedures.

I'm also on a committee of the Workgroup for Electronic Data Interchange (WEDI) out of Virginia, a large consortium of different types of organizations, including insurance companies and electronic data facilities, and they are the ones that have created the majority of the work. They are also under a DHHS contract and created the ASCX Electronic Data Interchange standards for claims submission process, and the other eight claims standards that were created by HIPAA. They've also created the Strategic National Implementation Process (SNIP). In a subcommittee of the SNIP, we created a small practice implementation discussion draft (SPIDD), which we have now disseminated over the last month or two to members of SNIP.

I'm also on a subcommittee for Georgetown and Columbia Universities, which have DHHS grants for implementing HIPAA.

DC: Can you give us a brief overview of HIPAA and its general objective?

Ross: HIPAA was passed by Congress in 1996, and was meant to make insurance portable for employees that are changing jobs. People were losing their health care benefits when going from one

employer to another. There needed to be a law to prevent loss of benefits, since each state had a different set of laws on how pre-existing conditions affected new policies. They changed pre-existing conditions clauses and created an accountability section. There are four things that a doctor needs to be concerned about:

1. the national standards that have been established by HIPAA;
2. the unique health identifiers that HIPAA will create;
3. changing standards to protect electronic security and information; and
4. privacy and confidentiality provisions.

DC: What are the really big issues for the doctor of chiropractic to worry about?

Ross: The first two of these provisions (national standards and identifiers) are just going to happen to the doctor; they [DHHS] have created eight different kinds of national standards for submitting insurance information electronically. These are electronic:

1. claims submission;
2. enrollment checking;
3. eligibility verification;
4. health care explanation of benefits;
5. health plan premium payment;
6. health claims status;
7. referral certification and authorization; and
8. coordination of benefits.

If you do any of these eight things electronically, you qualify as a covered entity under HIPAA.

DC: At what level is the doctor liable when privy to patient information under HIPAA?

Ross: Faxing, for example, falls under the security and privacy provision of the act. The cost of administering health care is currently 25 cents on every dollar. When Congress worked on this, it asked, "What are some of the ways we can simplify administration and cut costs?" One solution was a design such that each insurance company doesn't have different claim forms or other qualifications, and no company can request a different claim form, or request to verify eligibility one way as opposed to another. With this plan, they basically standardize the submission process.

DC: For doctors to take advantage of this, they will have to be under HIPAA jurisdiction?

Ross: You are a covered entity if you utilize any one of the eight standards mentioned earlier. I don't usually worry about things like national HIPAA standards, because once doctors submit something that is wrong, they will get the claim back unpaid, saying that it doesn't fit in with the correct standards - either that, or you're running a free clinic! Whether it's in paper or electronic form, it won't make a bit of difference to the insurance company.

The national HIPAA standards also include some coding issues. Everybody will use the CPT codebook, and the ICD-9 diagnosis codebook, and the federal medical devices codebook. Since October 16, doctors are no longer able to use what's called a "local code." If they fail to comply with these standards, they will find out real quickly!

On national identifiers, every doctor will be given:

1. an identifier number that will be issued by the IRS as a federal tax ID number;
2. a unique identifier number;
3. a health care identifier number (there won't, for example, be a "Blue Shield" number, only a health care ID number); and
4. individual identifier numbers (although there was much opposition against using social security numbers from the Office of Civil Rights).

As far as the provision of privacy, this is related to the HIPAA concern over patient rights. You are in control of confidential patient information, and starting April 14, 2003, this privacy law goes into effect. Here is a brief introduction to those rights:

1. Patients are entitled to see a copy of their records.
2. Patients are entitled to receive a copy of their records.
3. Patients are entitled to make an amendment in the file to their patient health information.
4. The doctor has a right to deny inclusion of amendments in the patient's file.
5. The patient has a right to disagree with the doctor's refusal of inclusion.
6. The doctor has a right to a rebuttal to the patient's disagreement, but any time a file is sent out, a copy of that rebuttal must be included.
7. The patient has a right to a privacy practice notice from the doctor providing the care. (The patient can object to certain information given to him in the privacy of his office, and the doctor can comply with this or refuse to treat the patient. The fine for violation of the privacy standards is $25,000 per incident.)

Among the many forms the doctor must use is an authorization form that must be signed by the patient any time information is given out about the patient for purposes other than billing. This also applies to insurance companies, attorneys in P.I. cases, or anybody dealing with outgoing or incoming patient paperwork (for example, with specific timelines for using the information). There will be a "request to view patient records"form, and forms for patients to request and amend those records, as well as those for denial of requests and disagreement of denials.

DC: Can you address some of the things a doctor might be liable for in an office under HIPAA?

Ross: The doctor, whether considered a "covered entity" or not, must maintain privacy, because the privacy issue isn't going to go away. Doctors must make sure they have established a policy, a procedure, and are training their staff to protect patient privacy. Two examples are computer monitors with patient information on them, or the recent question answered by the DHHS and OCR, concerning public sign-in sheets that can state a patient's name, but not a condition. Also, charts and records left on the door of a doctor's office are permissible, but come with the responsibility of the staff making sure those records are not left in the hands of those unauthorized to see them.

There is also a "chain of trust," which applies to those contracted with a doctor to send and receive patient records. Such contractors are covered entities, business associates, and all must meet the same requirements for privacy and security as if they were covered entities.

DC: So you're saying that if doctors don't comply, they can be denied payment?

Ross: That could be one of the outcomes, but I'm not going to say that this is automatic. An insurance company is required under the gigantic federal law to make people business associates. You can rest assured they're not going to pay a doctor who's not a business associate.

DC: So, one way or another, the doctor must comply with the HIPAA privacy provisions?

Ross: Yes, the associated business is under the chain of trust contract; even a company such as a janitorial service may have to sign a statement of confidentiality or a chain of trust form.

Let's say you faxed something out, and it went to the wrong person; the patient files a complaint, and it goes to OCR. Representatives come to your office, and you show how your equipment proves that it went to the right phone number, and that you have authorization on a patient disclosure form to use a fax or email. You have only made a mistake, and you won't be fined or penalized. Without that manual that is specific to you or your office (and if it looks like a 'boiler-plated' manual, the OCR and DHHS won't consider it applicable to your office), this complaint could result in a fine or worse. We saw this in the past, when a number of offices copied manuals, and they found that no work was done to make the manual applicable.

DC: It looks as if the doctors are going to have to go after this proactively.

Ross: One important thing to remember about this is that if you read too much into it, it becomes extremely complicated. Once you put into writing what is necessary, you don't have a lot of work to do. If a step-by-step procedure is written, one doesn't have to worry. For the small practitioner, manuals can be less than 100 pages. Requirements for matters such as privacy will just boil down to a simple procedure, involving such things as firewalls to protect computer systems and passwords to protect information. Common sense says that one doesn't have to tear an office up and buy thousands of dollars' worth of equipment.

Many people have asked me about information transmitted through copy machines, fax machines and computers, and we have adopted all these in our practices. There are currently some viruses that are specifically designed to enter and find patient names and diagnoses. The chiropractic profession doesn't know much about this; it doesn't know about the pharmaceutical companies attempting to obtain names and addresses of patients, and the marketing that goes on in that area. Yet, that is a large issue, and one of the main reasons that HIPAA's privacy and security will go into effect. Your systems are vulnerable; the diagnoses of your patients are vulnerable. Once the diagnosis can be tied to your patient's name and address, you have a problem.

We have more laws protecting credit information than protecting patient diagnosis information. Now you're seeing the first law for patient protection. Instead of having patchwork state laws do it, we have a baseline federal law. This is going to be implemented locally, allowing states to individually implement it, with the states' rules generally being tougher than those of HIPAA. An example of this is the time deadline for giving a patient a copy of records, which is five days in California, but 30 days under HIPAA. Of course, the five-day deadline would apply in this case.

DC: What about security issues?

Ross: Inside the security provision, the act requires that four issues be addressed:

1. policies and procedures concerning security;
2. safeguarding the office and physical plant;

3. technical security mechanisms; and
4. technical security services.

The last issue is one that doctors get really bogged-down in, but as a individual practitioner, you have a very limited set of resources that need to be dealt with. There is no specific implementation of security in HIPAA, but I feel that by the end of this year we will see an implementation date for HIPAA security requirements. You really can't have the privacy without the security.

DC: Thank you, Mr. Ross, for the wealth of information. We anticipate a large number of responses and questions from your interview. Would you be willing to answer questions from our readers in another article?

Ross: I will be glad to answer any questions from your readers, and provide a consortium of others available to readers.

(*Editor's note*: Readers with HIPAA-related questions may submit them to editorial@mpamedia.com. We will compile your questions, and have Mr. Ross answer them in an article.)

NOVEMBER 2002