Dynamic Chiropractic

NEWS / PROFESSION

HIPAA Q&A With Howard Ross

Dynamic Chiropractic Staff

Following the publication of "Everything You Ever Wanted to Know About HIPAA: An Interview With HIPAA Authority Howard Ross," many doctors and assistants contacted us with questions for Mr. Ross. In this article, we present some of those questions, along with responses from Mr. Ross. Some questions are presented verbatim; others have been combined or modified to include more than one question/scenario. Identification has been removed for privacy reasons. (*Editor's note*: The original article appeared in the Nov. 30, 2002 issue, available online at www.chiroweb.com/archives/20/25/09.html.)

Open Floor Plan

Q: My office is small (355 sq. ft.) and has an open floor plan. Everything anyone says can be heard by everyone else in the office (and anyone passing by the open windows). What is the best way to deal with privacy issues concerning overheard conversations?

A: The Privacy Rule requires that you make "reasonable" attempts to secure confidentiality and privacy in your health-care environment. In your case, the office setting is such that it is likely that others will overhear some conversations in the office. If you establish procedures that address how you and your personnel will make "reasonable" attempts to protect this privacy, HIPAA calls these overheard conversations "incidental disclosures." The OCR (Office of Civil Rights) addresses this issue in one of their FAQ documents:

"*The HIPAA Privacy Rule is not intended to prohibit providers from talking to each other and to their patients. Provisions of this Rule requiring you to implement reasonable safeguards that reflect their particular circumstances and exempting treatment disclosures from certain requirements are intended to ensure that the provider's primary consideration is the appropriate treatment of their patients. The Privacy Rule recognizes that oral communications often must occur freely and quickly in treatment settings. Thus, you are free to engage in communications as required for quick, effective, and high quality health care. The Rule also recognizes that overheard communications in these settings may be unavoidable and allows for these incidental disclosures.*"

I suggest that you include in your NOTICE OF PRIVACY PRACTICES (given to each patient starting April 14, 2002) an explanation of your use of an "open treatment" environment, and that it is possible that an "incidental disclosure" may occur. Doing this places patients on notice of your privacy practices, and allows them to object if they are uncomfortable. Reasonable precautions you might decide on in your procedures manual include using lowered voices or talking apart from others when sharing protected health information, or erecting a privacy screen or other type of sound, secure area if and when necessary.

Files and Sign-In Sheets

Q: I attended a management seminar recently, and was told that I can no longer use a sign-in sheet; have to keep all files locked in a filing cabinet; must remove patient names from folders and only use numbers; can't keep travel cards in trays on the reception desk anymore; and can never

call out a patient's name in the reception room again. Is all this correct? (By the way, the management company was willing to sell us everything that we needed to fix all these problems for $4,800.)

A: This is probably the most-asked set of questions of all the committee members in the organizations with which I am affiliated! There are many different scenarios I will address with this answer, including:

- open filing systems built into the walls, without the ability to lock;
- rolling filing tables that are not lockable;
- leaving "files-in-progress" on the insurance department desk;
- leaving files on the doctor's desk, pending reports;
- using plastic file boxes on the outside of treatment room doors; and
- stacking patient files on a desk of all patients coming in that day.

The above scenarios are all part of a functioning small practice with limited space, equipment capabilities and resources. The Privacy Rule is clear on the idea that privacy and security are meant to be scalable. This means you do not have to tear your office down and rebuild Fort Knox! You have to do what is necessary to implement "reasonable" safeguards to protect PHI (protected health information). You are going to have to make some changes in order to achieve HIPAA compliance. The changes you will have to make are related to what you are going to do procedurally, rather than to what you are going to have to buy, fix, build, rip out or add.

Walk through your office with paper and clipboard, and make a list of each publicly accessible area where PHI is stored. Decide how you can make that area secure for the storage of PHI documents, then turn this into a documented procedure for your office. For example, you might make the insurance department off-limits to the public, and make sure the door is kept closed during working hours when unattended. Additionally, you can ensure that the area of an open filing system is off limits to unescorted public access, and that all files are kept out of the view of unauthorized individuals. The same rationale applies to all of the above scenarios. Document procedures to ensure your office and your staff know how to make this PHI safe from public disclosure.

Here is a statement from the OCR (Office of Civil Rights) in one of their Public Clarification documents:

"*...the Privacy Rule does not require structural changes be made to facilities. ... Entities must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information. This standard requires the entities make reasonable efforts to prevent uses and disclosures not permitted by the Rule. The Department does not consider facility restructuring to be a requirement under this standard... the Privacy Rule does not require that all risk of PHI disclosure be eliminated. Entities must review their own practices and determine what steps are reasonable to safeguard their patient information.*"

"*...The Privacy Rule permits the practice of placing patient charts in plastic boxes outside an exam room as long as the clinic takes reasonable and appropriate measures to protect the patient's privacy ... Examples of measures that could be reasonable and appropriate to safeguard the patient chart in such a situation would be limiting access to certain areas, ensuring that the area is supervised, escorting non-employees in the area, or placing the patient chart in the box with the front cover facing the wall rather than having PHI about the patient visible to anyone who walks by. Each entity must evaluate what measures are reasonable and appropriate in its environment. Entities may tailor measures to their particular circumstances.*"

Medical Records Release

Q: If an attorney or an insurance company sends the office an "Authorization to Release Medical Records" signed by the patient, does the office need to A) have the patient sign an in-house authorization; B) include a line in its "Statement of Privacy Practices" stating that it will, if necessary, release information to these organizations; or C) do none of the above?

A: One of the requirements of the Privacy Regulation of HIPAA is that a "valid" authorization form be used anytime you release protected health information except for treatment, payment or business operations. The regulations are quite clear about what has to be in an authorization. The one that you are using now probably does not meet the requirements set forth in the regulation. What worries me most is that an attorney is probably going to send an authorization that is "defective." When that happens, you will have to have the patient sign a "valid" authorization, or return the one from the attorney, explaining that their form is "defective" and that you need a corrected one. (I'll bet that will make some of the attorneys crazy!) Below are the authorization requirements as written in the Privacy Regulation:

VALID AUTHORIZATION:

This section must be written in plain language and must contain at least the following elements:

1. A description of the information to be used or disclosed that identifies the information in a specific and meaningful fashion.

2. The name or other specific identification of the person(s), or class of persons, authorized to make the requested use or disclosure.

3. The name or other specific identification of the person(s), or class of persons, to whom the covered entity may make the requested use or disclosure.

4. A description of each purpose of the requested use or disclosure. The statement "at the request of the individual" is a sufficient description of the purpose when an individual initiates the authorization and does not, or elects not to, provide a statement of the purpose.

5. An expiration date or an expiration event that relates to the individual or the purpose of the use or disclosure. The statement, "end of the research study," "none," or similar language is sufficient if the authorization is for a use or disclosure of protected health information for research, including for the creation and maintenance of a research database or research repository.

6. Signature of the individual and date. If a personal representative of the individual signs the authorization, a description of such representative's authority to act for the individual must also be provided.

A statement of the individual's right to revoke the authorization in writing and a description of how the individual may revoke the authorization are also required elements.

The disclosure of protected health information must be the minimum necessary to accomplish the intended purpose. (Do not send the entire medical record unless specifically asked to do so by the patient.)

DEFECTIVE AUTHORIZATION:

A covered entity may not use or disclose protected health information to a requesting party if the authorization is defective. A defective authorization is one that has expired, is incomplete, has been revoked, or is known to be false.

1. Return all authorizations known to be defective to the party requesting the information with an explanation of why the requested information is not being disclosed; or,

2. Have the patient review the defective authorization, and have the patient read and sign a new authorization form before releasing the health information.

New Patient Rights

Q: Mr. Ross refers to "new patient rights" in his HIPAA article. What exactly are the "new patient rights?"

A: Beginning April 14, 2003, HIPAA Privacy Regulations have granted the following rights to all patients with regard to their Protected Health Information:

1. the right to receive a Notice of how their Protected Health Information will be used by any health care entity that provides health care;
2. the right to object to certain disclosures by the covered entity;
3. the right to receive information from the health care entity by an alternative means. (They may not want you to mail or contact them at their home or office address, and you have to abide by the request);
4. the right to access and or copy their Protected Health Information Records;
5. the right to amend their Protected Health Care Information;
6. the right to complain to the Privacy Officer of the entity concerning any breach of privacy or security; and
7. the right to file a formal complaint with the Secretary of the Department of Health and Human Services concerning a breach of any of these rights.

You are required to be aware of and understand all these rights! A good office procedure manual will keep you out of trouble and compliant with the regulations.

Business Associate Agreements

Q: Will each insurance company dictate what is within the Business Associate Contract given to providers?

A: Yes and no. A Business Associate Contract protects the originating entity (an insurance company or a doctor's office) from any misconduct of the Business Associate. The Business Associate contract extends the "long arm of HIPAA" to those who have signed the Contract. The Privacy Regulations have established "core elements" and "required statements" that must be in every Business Associate Contract. DHHS will consider any contract that is missing these elements "defective" and make the originating entity responsible for any and all actions of the Business Associate. Here are a few of the requirements of a Business Associate Contract.

A contract between the covered entity and a business associate must:

1. establish the permitted and required uses and disclosures of such information by the business associate. The contract may not authorize the business associate to use or further disclose the information in a manner that would violate the requirements of this subpart.
2. provide that the business associate will:

1. not use or further disclose the information other than as permitted or required by the contract or as required by law;
2. use appropriate safeguards to prevent use or disclosure of the information other than as provided for by its contract;
3. report to the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware;
4. ensure that any agents, including a subcontractor, to whom it provides protected health information received from, or created or received by the business associate on behalf of, the covered entity agrees to the same restrictions and conditions that apply to the business associate with respect to such information;
5. make available protected health information in accordance with 164.524;
6. make available protected health information for amendment and incorporate any amendments to protected health information in accordance with 164.526;
7. make available the information required to provide an accounting of disclosures in accordance with 164.528;
8. make its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of, the covered entity available to the Secretary for purposes of determining the covered entity's compliance with this subpart; and
   (li)at termination of the contract, if feasible, return or destroy all protected health information received from, or created or received by the business associate on behalf of, the covered entity that the business associate still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

3. authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.

   After the contract meets all the required elements, an insurance company may add any additional language that does not contradict or interfere with the above language. I expect we will see many insurance companies add language to support some of their business practices.

Editor's note: For information on "Business Associate Agreements," please refer to "Business Associate Agreements Are Coming! What to Expect, What to Watch Out For" by attorney Michael J. Schroeder, in the January 14, 2003 issue. (www.chiroweb.com/archives/21/03/20.html).

Can Insurance Companies Include Only HIPAA-Covered Entities?

Q: Will insurance companies be allowed to include a provision in patient health care contracts stating services must be provided by HIPAA-covered entities?

A: There is no actual reference in the law pertaining to this question. I can say that any insurance company or entity can refuse to share Protected Health Information with any entity (doctor) that does not sign a Business Associate Contract. Remember, this contract protects the originator from the misdeeds of the signing entity.

Cash Practices

Q: What changes will need to be made by doctors who have 100 percent cash practices?

A: Having a cash practice does not relieve you of the responsibilities of securing Protected Health

Information. The HIPAA privacy law is a consumer protection law, similar to the recently passed "credit" laws. At minimum, you should conduct a walk-through of your practice and determine the best way to protect this information. Remember, patient files, computer management systems, travel cards and records are susceptible to security breaches.

Also, don't forget that patients now have new rights with regard to their Protected Health Information. They have a right to view or copy their records; amend their records; restrict disclosures; demand alternative communications; receive an accounting of all disclosures by your office; and complain to the secretary of Health and Human Services.

Essentially, a cash practice will have to meet the same requirements under the Privacy Regulations as a practice or hospital that does insurance and electronic transmissions.

Available Programs

Q: Thank you for the informative article on HIPPA. The only thing I did not get from the article was: What do we do about this? Is there some form of software that walks us through this, and where do we buy it?

A: Scare tactics abound! It seems that everyone is trying to make a buck out of this new law! Some are even going to the extent of embellishing and misquoting the law or deliberately not disclosing the rest of the story. Remember, this "new" law is not new. You already do 90 percent of all this stuff. The only difference is that you now have to have "formal documented procedures" to protect patient health information. That simply means, turn the law into office procedures and put it into your privacy and administration manuals.

There are a number of reputable consultants and companies offering HIPAA privacy compliance assistance. Some offer computer programs that walk you through creating your own HIPAA manuals. Here are the things you really need to look out for:

- No boilerplate! Make certain that what you are getting incorporates your present office procedures into your HIPAA manual. The last thing you need is to find out during a HIPAA audit that your boilerplate HIPAA manual requires you to do office procedures you've never even heard of.

- Two HIPAA Manuals. Your office needs both a policy manual and an administrative manual to effectively implement the HIPAA privacy laws.

- State Laws Included. Be sure your HIPAA program includes your state laws as well as the federal. In many cases, your state law is stricter, and therefore supercedes the federal HIPAA laws.

- Generate a Compliance Verification Report. You will want the program/consultant to ultimately provide you with a compliance verification report once you've finished the process.

- Eight Hours or Less. You are a doctor of chiropractic. There is no reason for you to become a HIPAA expert any more than you have to. The program/consultant you use should be able to create a complete policy and procedure manual specifically for your practice in less than eight hours of staff time. Any more than that is unnecessary.

- $700 or Less. Unless you have a very unique practice, there is no reason to spend more than $700 to make your office HIPAA-compliant.

Editor's note: Mr. Ross has developed a demo of his own HIPAA program, and has made it available on his Web site (www.hjrosscompany.com). Readers may want to compare this information with other programs/consultants they are considering.

FEBRUARY 2003