PHARMACIST'S LETTER

**PHARMACIST'S LETTER**
**SPECIAL REPORT**

# HIPAA Made Simple: Pharmacist's Survival Guide

Continuing Education Self-Study Course #02014 ~ Volume 2002 ~ Course No. 14

Pharmacists wishing to be awarded CE credit for studying this special report, should read the accreditation information at the end of this report.

The Health Insurance Portability and Accountability Act (HIPAA) will have a major effect on most every aspect of the health care industry. This Act has lots of different tentacles. There are security issues, transaction issues, privacy issues, training issues, and others. Various parts of this Act will affect different players within the health care industry. The Act is huge. A whole industry has been established to interpret, train, and analyze various portions.

HIPAA actually was born in 1996. Technology was advancing at a breakneck pace. "Electronic medical records" became a catchphrase. At the same time, the government wanted to offset the costs of health insurance portability for employers by standardizing health information. This meant that comprehensive federal laws were needed to protect this health information for the electronic age. The Department of Health and Human Services (HHS) has been leading the rulemaking process.

After a few years and several drafts, the final privacy rules were issued on August 9, 2002. The bottom line of HIPAA is that health care providers and health plans must protect patient information, and may not use or disclose an individual patient's health information except for treatment, payment, or regular health care operations. Additional uses of a patient's health information would require an advanced authorization signed by the patient.

Health care providers and health plans must be in compliance with the privacy sections of the Act by April 14, 2003.

The original intent of the Act makes sense. The ultimate goal is to make it easier for consumers to get seamless care no matter which provider they go to. Providers and patients should all be able to access the important patient medical information. And, while making the information available, the Act is designed to protect patient privacy and confidentiality as much as possible…without hindering the access to, and quality of, health care.

The final rules simplify some significant issues compared to the draft that had been circulated and discussed since November 1999. Over 63,000 comments were received by HHS on the various drafts. HHS had the difficult task of protecting patient privacy without interfering with patient care. This means that many of the scary requirements you may have heard about will not be quite as hard to implement.

The privacy protection gives patients federal rights that guarantee they can inspect their medical records, correct mistakes, inquire who has seen their records, and seek penalties if their health information is used inappropriately. It also virtually eliminates the unauthorized use of medical information for marketing.

But the privacy rules still allow personal medical information to be shared for basic health care operations, such as treating patients and transmitting claims for payment. HIPAA requires health care providers to make their best efforts to protect patient medical records and share the smallest amount of information needed. This isn't a giant shift in the general practice of many health care professionals. Pharmacists and physicians are already aware of the importance of protecting medical records. Hospitals and physician offices already use consent forms on the use of medical records. The American Pharmaceutical Association Code of Ethics already says:

> With a caring attitude and a compassionate spirit, a pharmacist focuses on serving the patient in a private and confidential manner.

*More. . .*


*Pharmacist's Letter / Prescriber's Letter* ~ P.O. Box 8190, Stockton, CA 95208 ~ Phone: 209-472-2240 ~ Fax: 209-472-2249
www.pharmacistsletter.com ~ www.prescribersletter.com

This Special Report will help you gain an understanding of the basic concepts and terminology and will help you incorporate HIPAA concepts into your daily practice.

This Special Report is NOT designed to address the issues that will be faced by corporate management, hospital management, attorneys, or HIPAA privacy officers. This document is not intended to represent legal advice. For detailed information and advice necessary for these individuals, we recommend a more specific resource. A list of resources and manuals that delve deeper into the new privacy rules are listed at the end of this report.

**We have selected some of the main concepts and terms contained in HIPAA. Read about each term below…and you will have an understanding of what you need to know about HIPAA.**

## Who has to be concerned with the HIPAA requirements?

"Covered entities" must abide by the new HIPAA requirements. This pretty much means any person, business, or institution that provides health care or keeps records on patients. All practicing pharmacists with direct relationships with patients are covered entities and must comply.

## Hybrid Entity

This applies to an entity in which part of the entity is covered by this Act, and other parts are not. For example, a huge discount department store might have quite a few employees working in the "front end" and fewer employees working in the pharmacy. The "hybrid entities" concept means a large department store could remain legal by providing all the required training to all the pharmacy-related employees…but not providing the HIPAA training to clerks and others who work in the "front end" of the store as long as the necessary "firewalls" are in place to keep patient health information in the pharmacy area.

Another example would apply to a hospital. A hospital would not have to apply the HIPAA training to employees who work in parts of the hospital or parts of the pharmacy that don't have anything to do with patient privacy. The person selling gifts in the gift shop doesn't have to be trained on HIPAA. But the law does require that the pharmacy needs to protect patient medical information from being accessed by non-pharmacy employees.

The final version of the rules is very generous in its definition of hybrid entity. The original draft rules did not recognize hybrid entities, and said that all employees would have to get the HIPAA training. But, the final rules took care of this snafu, so that only appropriate employees would need to receive the HIPAA training.

Chances are good that your practice is in a "hybrid entity" and therefore allows for some employees to be trained, while others are not. If you practice in a small pharmacy that does nothing but provide medical/pharmaceutical care, then you may not be in a hybrid entity, and all employees would need HIPAA training.

## Direct Treatment Relationship

Certain parts of the law apply to health care providers who have a direct treatment relationship with a patient. Pharmacists obviously do…if they are providing products or services to the patient. For comparison, other parts of the health care industry do not. For example, the laboratory might be working on a patient's blood sample, but does not have a direct treatment relationship with the patient, and therefore follows somewhat different rules.

If you are practicing in a pharmacy and providing services to patients, then you have a "direct treatment relationship" and need to follow the appropriate parts of the law.

## Privacy Officer

HIPAA requires that each covered entity must appoint a Chief Privacy Officer, who is responsible for developing and implementing policies to comply with the privacy rules. There also must be a contact person or means in place for customers to submit complaints and ask questions about privacy issues. The contact person and the privacy officer can be the same person. Chain pharmacies or affiliated hospitals that are under common ownership only need one privacy officer and/or contact person for the whole group. Make sure you know who your privacy officer is...and how to get in touch with him or her.

*More. . .*


*Pharmacist's Letter / Prescriber's Letter* ~ P.O. Box 8190, Stockton, CA 95208 ~ Phone: 209-472-2240 ~ Fax: 209-472-2249
www.pharmacistsletter.com ~ www.prescribersletter.com
**Reprinted with Permission for Montana State Board of Pharmacy**

**Protected Health Information (PHI)**

You'll hear a lot of people adding "PHI" to their health care alphabet soup. Protected Health Information refers to any patient information in any form that:

1. is created or received by a covered entity;
2. relates to a patient's health condition in the past, present, or future;
3. and identifies the patient.

PHI is any information transmitted or maintained in any form, such as prescription records, billing records, patient profiles, and oral communications on the phone or during patient counseling. Keep the HIPAA requirements in mind any time you are handling any health information that pertains to a patient.

**De-identified Health Information**

This refers to patient information that cannot be used to identify an individual. HIPAA does not apply to de-identified health information. The privacy rules DO allow giving out health information without patient authorization under certain situations and if certain things are removed, such as names, street addresses, social security numbers, e-mail addresses, telephone and fax numbers, license numbers, full face photographs, med ID numbers, finger prints, etc.

De-identified information can include city, state, zip code, date of birth, and date of death. These "limited data sets" can be used for research, public health purposes, quality improvement activities, or health care operations within the hospital or pharmacy. If your hospital or pharmacy plans to release limited data sets for research, make sure that the information is "de-identified" and that the researchers have signed a Data Use Agreement which meets HIPAA requirements.

**Minimum Necessary**

One concept prevalent in the Act is the concept that patient privacy should be protected by minimizing the amount of private information that is given out about a patient, and minimizing where the information is sent. This concept is often referred to as "minimum necessary." The privacy rule requires you to make a reasonable effort to limit PHI to the minimum required to accomplish what needs to be done. Keep this concept in mind and apply it wherever you can. For example, if you are submitting a claim for a prescription for a patient, and the payer does not need to know the diagnosis, do not provide the diagnosis.

The rules say that whatever information the payer asks for will be considered to be the minimum necessary information unless the pharmacist disagrees. If in your judgment the information that the payer asks for is not the minimum necessary, you are supposed to negotiate with the payer to agree upon the minimum necessary information. This depends on your judgment and you do not have to provide information that you do not think meets the requirement of being the minimum necessary. Keep in mind that the payer does not have to pay you. This means that you might win the battle…meaning you do not have to divulge information you don't want to…but the payer might win the war…because they don't have to pay you if they don't get the information they want from you.

Always keep in mind the idea of "minimum necessary" when you are giving...or requesting patient health information. Only request what you need to know...and only disclose what is required. But don't feel too constrained by this rule...HIPAA does allow for certain exceptions for the minimum necessary rule. For example, the minimum necessary requirement does not apply when talking directly with the patient or any disclosures that fall under a written authorization from the patient. Other exceptions are discussed in the next section.

Minimum necessary is also designed to encourage your pharmacy to evaluate who should be accessing patient records. If support staff don't need patient medical records to do their jobs, don't give them access to the records.

**Disclosure**

The law stipulates who you can give information to…and who you cannot. One concept is that you CAN disclose information to another health care provider as long as the other health care provider has a treatment relationship with the patient and has informed the patient of their own privacy policy. For example, this

*More. . .*

means you can always call a physician who is caring for a patient to discuss the patient and freely trade information back and forth. It is important to note that the concept of "minimum necessary" information does NOT apply to these sorts of communications. The law does not want to inhibit your communication with a physician or other health professional that would make it harder for you to act in the best interest of your patient.

HIPAA does permit friends or family members to pick up prescriptions for a patient. But the pharmacist is required to use professional judgment and look out for the patient's best interest when allowing someone else to pick up the prescription. Keep the necessary information to a minimum and invite the patient to call you by phone if they have any questions or need counseling. HIPAA also allows health professionals, at their discretion and with certain limitations, to speak to relatives, friends, or caregivers...unless the patient specifically requests them not to. Keep the patient's best interest in mind when discussing their health information with relatives, etc, and only discuss items pertinent to the current health condition.

Don't be afraid to announce a patient name over the store or waiting room PA system. This would be considered a part of your health care operations, so HIPAA allows it. Just keep it to the minimum: "Mrs. Lamberjack, please return to the pharmacy." Don't announce any health-specific information, such as a condition or drug name.

Disclosure of patient health information is allowed under certain circumstances, such as public health activities, victims of abuse, law enforcement purposes, to comply with workers compensation, and to report adverse events or other drug- or device-related problems to the FDA. Keep in mind that in the case of civil matters, such as divorce proceedings, patient-related health information should only be turned over pursuant to a subpoena or appropriate legal document.

Many health professionals have heard about the HIPAA regulations through the legislative process and are very concerned that they will be in violation if some information slips out while they are speaking or a piece of paper is seen by somebody who should not see it. Many of these rules were softened during the final rule writing. HIPAA does allow for incidental disclosures as long as policies are in place to protect patient information. For example, you wouldn't be in violation of the law if you were talking with a patient in a semi-private counseling area, or discussing the patient's condition at a nurses station, and someone accidentally overhears you. Keep in mind that this type of accidental disclosure is only okay if it couldn't be reasonably prevented…is limited in nature…and is an unintended result of a permitted disclosure.

It is important to use good judgment, and try to protect patient health information, but the final rules take into account that it is unreasonable to control every possible situation in which the information could leak out.

HIPAA does allow the transfer of patient medical records in the event of a change of ownership. So if you work in a pharmacy that is being bought, the patient information automatically goes to the new owner. Patient authorizations to transfer their records are not required by HIPAA under this circumstance.

**Accounting and Disclosures**

Patients can ask you to give them a list of any instance, going back six years or less, in which their information was disclosed to anybody outside the realm of treatment, payment, or regular operations. This means that you have to keep records of who you sent information to for at least six years. Once requested by a patient, you will have 60 days to provide them an accounting of these disclosures, including the date, name and address of who you gave the information to, brief description of the disclosure, and the reason for it. But, remember this is only for non-routine uses.

You do not have to account for disclosures that have to do with treatment, billing, accounting, or conversations you had directly with the patient. Unintended disclosures of patient health information, for example, if someone accidentally overhears a conversation, also do NOT need to be documented and included in the list of disclosures. And you don't have to track or account for those you are legally required to make, such as to a court under a subpoena or other law or governmental authorities. Accounting is also not required if the disclosure is made pursuant to a patient

*More. . .*


*Pharmacist's Letter / Prescriber's Letter* ~ P.O. Box 8190, Stockton, CA 95208 ~ Phone: 209-472-2240 ~ Fax: 209-472-2249
www.pharmacistsletter.com ~ www.prescribersletter.com
**Reprinted with Permission for Montana State Board of Pharmacy**

authorization. Therefore, keep a record of any time you give out information on any patient, for a non-routine use, and be prepared to give this information to a patient if it is requested.

Patients also have the right to obtain a copy of their pharmacy records. If you receive a request, you have 30 days to provide the patient with a copy. Patients can also request a change to their records. It's best to ask the patient to put the request in writing and include the reason for the change. You must act within 60 days to determine whether the change is appropriate and then correct the records if necessary. For example, say a patient denies receiving a prescription for haloperidol. Under the privacy rules, you might be required to check your records, contact the physician, etc to see if this is a real error before updating the patient's medical record. Before you delete any health information from a patient's record, make sure the removal of the information is consistent with other laws or your organization's general practices.

**Consent**

There was a lot of talk that you would be required to get the patient's signed consent before doing anything with any patient information. This potential requirement has been eliminated. You do not need to get the patient's consent before you process information about a patient. One reason this concept was eliminated was to accommodate prescriptions that were faxed or called in to the pharmacy. Under the previous version of HIPAA, you would not be able to use any of the information on new prescriptions if you did not have a signed consent form on file. Basically, you couldn't talk to the physician's office to take the prescription, let alone enter it into the computer.

The final privacy rules did away with mandatory consent. Consent is now only an OPTION. If your hospital or pharmacy already uses consent forms for various purposes, it is okay to continue using them. The privacy rules don't have specific requirements for what should be included in a consent form, so no changes to your current versions are needed.

**Notice of Privacy Practices**

The final version of the rules relies on giving a "notice of privacy practices" in place of obtaining the patient's signed "consent." This is a major change from what many pharmacists are anticipating. You do not have to have patients give their signature and authorize you to use their private information. You just have to give them the written Notice of Privacy Practices. If your pharmacy or hospital continues using consent forms, they are still required to also provide a Notice of Privacy Practices.

The privacy notice is intended to create an initial moment and spur discussion between you and your patients concerning how you will use their PHI. This provides an opportunity for patients to make requests for additional restrictions on the use of their medical information. A patient could request that no one other than themselves can pick up his or her prescriptions...or hospital staff are not to discuss his or her condition with family or friends. Document any additional requests on the privacy notice and make a note in the computer or their chart to remind you of their requests.

The federal government wants the privacy notice to be specific for your pharmacy or hospital. They don't want to see everybody using the same model policy. In other words, you must have a policy stating how you protect patient information, and who you will or will not give the information to. A single privacy notice covers all the pharmacies in a single chain or all the departments of a hospital. For the privacy notice to be valid, it must meet the following requirements:

1. Be written in plain language (for example, a 6th grade reading level);
2. Describe, with examples, the types of disclosures to be made with or without patient consent or authorization;
3. State that other disclosures require a patient's written authorization which may be revoked at any time;
4. State that your pharmacy, hospital, or covered entity is required by law to maintain the privacy of protected health information;
5. Explain to patients their rights, including their right to inspect and amend their records and to ask for accounting of disclosures containing their protected health information;
6. Alert patients that they can complain to the Secretary of the HHS;

*More. . .*

7. Identify the contact person at the pharmacy, hospital, or covered entity regarding privacy issues;
8. And contain the wording: "This notice describes how medical information about you may be used and disclosed and how you can get access to this information. Please review it carefully."

You must give or mail this notice to your patients on the same day you first provide treatment or service, and you must have your patients indicate that they have received the information. This is quite different from having your patients indicate that they actually consent to giving the information out. Hand the privacy notice to the patient with your first face-to-face meeting. If you are providing products or services without face-to-face contact, such as offering advice or counseling them on the phone, you must mail the notice to the patient on the same day. In emergency situations, the notice needs to be delivered as soon as reasonably practicable after the emergency. If you have an Internet site that patients can go to, you need to make sure the privacy notice is available as a link. You are also required to post a copy of your privacy notice in an easy-to-view area of your pharmacy or hospital, such as a waiting area or check-in desk.

You must make a good faith effort to obtain acknowledgement from the patient that they have received your privacy notice. The patient can initial the notice, sign a list, or complete a separate document. If you have an Internet site, you can have the patient click a box on an electronic form, use a digital signature, or anything that requires some affirmative action on the part of the patient. You can use a "layered" notice, which consists of two versions...a short summary of the patient's rights...and the full notice explaining all the required information. Patients can initial or sign the summary and hand it to you for acknowledgement...and keep the full notice for their records. You can also send the notice home with the relative or friend who is picking up the patient's prescription. Have the patient either mail in their acknowledgement or drop it off at their next visit.

When patients sign or initial a log book acknowledging that they have received a copy of your policies, make sure the individual is clearly informed of what they are acknowledging…but there is a very specific kicker that you must be aware of. You CANNOT combine this acknowledgement with a waiver for something else. For example, you CANNOT have a patient initial or sign that they have received your privacy policy AND waive the requirement for counseling under OBRA with one initial or signature. You have to get them to initial or sign each of those two concepts separately. So you may end up having one log book that requires two separate signatures...or two separate log books.

Keep in mind one very important point. Patients are NOT required to sign or acknowledge the privacy notice if they choose not to. So don't deny treatment or services if a patient won't sign the privacy notice. Just document your efforts and the reason why the patient did not sign the acknowledgement.

Once a patient has received your privacy notice, they will not have to acknowledge it again. When your privacy notice is updated, make sure that you make the revised notice available to patients and post it in your pharmacy, hospital admissions, website, etc. But you are NOT required to physically redistribute the notice every time it's revised.

Keep all the patient acknowledgements of your privacy notice on file for at least 6 years.

## Minor's Rights

This raises an interesting question. If you have a minor who is getting birth control pills, or treatment for a sexually transmitted disease, or mental health treatments, etc, can you divulge information about this to the parents, if the parents ask? Sometimes yes, and sometimes no.

HIPAA says you need to abide by whatever your state law requires. Therefore, you need to know if your state law, or other applicable law, allows you to divulge this information or not. Most state laws do not stipulate. HIPAA says that if your state does not specifically allow or disallow release of this information to parents of a minor, then it is up to the pharmacist's professional judgment.

## Information for Marketing

Most of the concepts discussed thus far in this

*More. . .*

Special Report apply to using a patient's private health information in a manner related to the care of the patient. A whole set of new rules comes into play if the information is going to be used for marketing purposes.

If you are going to release any patient information to be used for marketing purposes, you need authorization from the patient. This is completely different than just having your patients acknowledge that they have received a copy of your privacy policy. You cannot put in your privacy policy that you will release information for marketing purposes and expect this to cover you. If you're going to release information for marketing, you need specific authorization from the patient before you release any information. This is in addition to the patient's acknowledgement of receiving a copy of your privacy policy.

This whole section depends on specific definitions of what constitutes marketing. The law says that marketing means to make a communication about a product or service that encourages the person to purchase or use the product or service.

But, the most important part of this rule are all the EXCEPTIONS.

You CAN provide all sorts of information to the patient that is NOT considered marketing. Any face-to-face encounter is generally appropriate. For example, you can inform patients about formulary restrictions or other features and benefits of their health plan. You can give them information about other treatments that are specific for them. You can give them any sort of general health communication, for example, how to care for diabetes, how to lower their blood pressure, etc. Any communication that relates to the treatment of the individual is not considered marketing. For example, you can send patients refill reminders. This could seem confusing because the refill reminders might seem like they are designed to promote purchase or use of the product or service, but the fact that they pertain to the treatment of the patient makes refill reminders exempt and perfectly okay to do. You also CAN recommend things such as generics, or different health care providers, or different alternatives, because they are considered part of your treatment for the patient, and therefore, are not considered marketing.

Be careful not to violate the anti-kickback statute. If you recommend a product or service, and you stand to make financial gain from it, and that service is paid for in part or in whole by the federal government, you would be committing a criminal act. For example, don't ever allow yourself to recommend a particular treatment and get paid by the drug manufacturer, because some of those patients might be getting coverage or reimbursement through some federal government program. You then could be guilty of violating the anti-kickback law and be subject to jail time for a criminal act. If you are going to use information for marketing purposes, and you are going to get any remuneration as a result of the marketing activities, you must mention this in the patient authorization form to release their information. Remember that refill reminders are NOT considered marketing, regardless of whether a third party pays for the reminders.

**Authorizations**

Before you use or disclose protected health information (PHI) that is not considered an exception under HIPAA, such as for marketing, you need to get a valid authorization from the patient. It is very important to remember you can no longer use "opt out" programs...that is to enroll a customer in a program with them having the ability to "opt out" if they desire. You must have the authorization signed and in hand before performing "marketing."

In general, an authorization form must contain specific elements, such as:

- Description of the information to be used or disclosed
- Names of the individuals or entities who are giving and are receiving the information
- Purpose of the disclosure
- An expiration date for the use of the information

Most pharmacists won't have to create the model of the authorization form the hospital or pharmacy will use. For managers, owners, or Privacy Officers who need to create a model authorization form, refer to the more detailed resources listed at the end of this Special Report.

When filling out an authorization form to

*More. . .*

disclose patient info, keep a couple of things in mind. If the patient is requesting you to release their records to someone, the patient is NOT required to state the exact purpose for the release. You can just write in that the patient is requesting it. And if you are completing an authorization form for marketing purposes, ALWAYS include any remuneration you will be receiving for releasing the protected health information.

**Transaction Standards**

If you are not concerned with the specific technical requirements that are involved with standardized electronic transmission of information, you might want to skip this section.

Part of the new law requires that certain electronic transmissions be standardized. Think of this as similar to the Universal Claim Form for submitting insurance claims. Years of work have gone into establishing what the universal standards will be. The new law requires using the National Council for Prescription Drug Programs (NCPDP) Telecommunication Standards Version 5.1. Most pharmacists won't have to deal with this directly. The Privacy Officer, techies, and upper management of the hospital or retail chain will make sure transaction standards are in place. If you are the Privacy Officer or owner of a small chain or individual pharmacy, contact your computer vendor to see if your system can support both 3.2 and 5.1 electronic transactions.

Every pharmacy must be using the new transaction standard by October 15, 2003. Actually, the requirement says October 15, 2002, but an amendment to the regulations allows you to get a one-year extension by filing an "Electronic Health Care Transactions and Code Sets Standards Model Compliance Plan." This Compliance Plan simply tells the government what you plan to do in order to comply with the transaction standards.

Even if you think you are going to be in compliance by October 15, 2002, send in the Compliance Plan to get the extension to buy yourself some time in case any problems pop up. In fact, the federal government is encouraging pharmacies to submit their Compliance Plan for the one-year extension.

The form should only take about 10 minutes to fill out. Simply answer a few questions about any compliance concerns you may have, and state where you are in the implementation process. You can go to www.cms.hhs.gov/hipaa/hipaa2/ascaform.asp to fill out and submit the form electronically. This is the fastest, easiest way to file your compliance plan. Just complete the compliance plan on-line, click "Submit" at the end, and it will be on its way. You will receive an on-line confirmation number, which will serve as acknowledgment of your extension. You will not receive a specific approval of your submitted compliance plan. You can also file it manually by downloading the Compliance Form as an Adobe Acrobat PDF form and mailing it in. If you mail in the Compliance Plan, make sure it is post-marked by Oct 15, 2002.

**Penalties under HIPAA**

HIPAA authorizes the Secretary of Health and Human Services to impose civil as well as criminal penalties to covered entities, such as pharmacies, if they have violated the new privacy rules. Fines can be as low as $100 for inappropriate disclosure of patients' PHI. If you knowingly disclose protected health information and use it for commercial gain, criminal penalties can be as high as $250,000 and possibly ten years in prison. This highlights the importance that is being placed on protecting medical information from inappropriate use. As long as you make a good faith effort to protect your patients' information and use it appropriately for their treatment and care, you shouldn't expect the government to come after you.

**Conclusion**

On all these HIPAA matters, use your common sense. HIPAA sets the bar, not the ceiling. Try to protect the privacy of your patients' information as best you can. Think about where you are sending patient information…unintentional disclosures…how to handle patient complaints on privacy…disposal of certain information such as old prescription labels and vials…how best to leave information on answering machines…how to dispose of the trash in the pharmacy...and similar situations. Even though the law does not address certain specific situations, and does not impose tight restrictions on you, it is appropriate for you to use your best judgment and minimize

*More. . .*

the potential for disclosing private health information. Also keep in mind that HIPAA doesn't override more stringent state privacy laws.

One easy tip to help you use patient information appropriately is to apply the "Mom Rule." How would you want your mother's PHI handled? Use your patients' PHI much like you would the health information of someone you care a lot about. Help patients get the best care possible while protecting their health information from inappropriate use or disclosure.

**Here are HIPAA resources if you need further information**:

| | |
|---|---|
| *HIPAA Privacy Standards: A Compliance Manual for Pharmacists*<br>National Association of Chain Drug Stores | Detailed information on HIPAA, including sample notices of privacy and authorization forms. $295 for NACDS members and $350 for non-members at www.nacds.org. |
| HIPAA/Privacy Briefing Room<br>www.ascp.com/public/ga/hipaa | American Society of Consultant Pharmacists resource page for HIPAA, including in-depth analysis of the rule. |
| Office for Civil Rights (DHHS)<br>www.hhs.gov/ocr/hipaa | The official government site for HIPAA news and updated guidances on the law. |
| DHHS Administrative Simplification Site<br>http://aspe.os.dhhs.gov/admnsimp | Health and Human Services (HHS) comments, updates, FAQs, and implementation guides for HIPAA administrative simplification provisions. |
| National Committee on Vital and Health Statistics<br>www.ncvhs.hhs.gov | Provides HIPAA updates and links to resources. |
| American Medical Association<br>www.ama-assn.org/ama/pub/category/4234.html | AMA HIPAA resource page, including sample forms and notices. |
| American Hospital Association<br>www.hospitalconnect.com/aha/key_issues/hipaa/index.html | AHA HIPAA resource page, including sample forms and notices. |
| HIPAA Central<br>www.smed.com/hipaa/index.php | Offers HIPAA online learning center, assessment tools, information about education seminars, and general HIPAA news. |

*The reader is responsible for utilizing professional judgment and confirming and interpreting the findings presented here before utilizing the information.*

**Sources**

Bell MD. HIPAA: HHS publishes final modifications to the privacy regulations. (Presentation). NACDS Pharmacy and Technology Conference. San Diego, August 12, 2002.

Department of Health and Human Services Fact Sheet. Modifications to the standards for privacy of individually identifiable health information – final rule. August 9, 2002. Available at: www.hhs.gov/news/press/2002pres/20020809.html. Accessed August 19, 2002.

Department of Health and Human Services. 45 CFR Parts 160 and 164. *Fed Regist* 2002;67(157):53182-53273.

Giacalone RP, Cacciatore GG. HIPAA and its impact on pharmacy practice. *Ohio Pharmacist* 2002;51(7):16-24.

McDermott, Will, & Emery. *Health Law Update* 2002;19(6). August 21, 2002. Available at: www.mwe.com/news/hlu1906.htm. Accessed August 22, 2002.

Mintz, Levin, Cohn, et al. *HIPAA Privacy Standards: A Compliance Manual for Pharmacists*. 2nd Ed. National Association of Chain Drug Stores, 2002.

Palacioz K. National Health Information Privacy. *Pharmacist's Letter* 2002;18(7):180701.

***Pharmacist's Letter / Prescriber's Letter*** *~ The most practical knowledge in the least time…*
3120 West March Lane, P.O. Box 8190, Stockton, CA 95208 ~ TEL (209) 472-2240 ~ FAX (209) 472-2249




*More. . .*

# Accreditation for CE Self-Study Course #02014 ~ Volume 2002 ~ Course No. 14

**How to Get CE Credit**
The cost to obtain CE credit from this course is $9.50 for subscribers of *Pharmacist's Letter*, $19.00 for non-subscribers. This is a printed version of the online CE course, available at www.pharmacistsletter.com. To get credit, submit your answers for the quiz questions through our website at www.pharmacistsletter.com. Your answers will be graded automatically, and you will be able to generate your statement of credit if you pass. Call us at 209-472-2240 if you need assistance.

**Needs**
With the Health Insurance Portability and Accountability Act (HIPAA) now finalized, health care providers need to be compliant with the privacy rules by April 2003. Pharmacists and pharmacy staff need educational programs to become familiar with the requirements, terminology, and concepts of the new privacy rules.

**Target Learners**
This activity is intended for a pharmacist, pharmacy student, technician, or pharmacy employee in any practice setting who will be required to comply with the new HIPAA requirements.

**Learning Objectives**
Upon completion of this course, the learner will be able to:
1. Explain the basic concepts and requirements of HIPAA.
2. List three requirements that determine if patient information is protected health information.
3. Explain the appropriate and inappropriate use of protected health information.
4. Identify three situations that do not require the use of minimum necessary information.
5. Describe four requirements of a hospital's or pharmacy's Notice of Privacy Practices.

**Principal Author**
Jeff M. Jellin, Pharm.D., Editor
Stephen C. Burson, R.Ph., Associate Editor, Director of Continuing Education

**Contributors / Reviewers**
David B. Brushwood, R.Ph., J.D., University of Florida College of Pharmacy
John Gorman, President and CEO, Gorman Health Group, LLC
Jason R. Moore, R.Ph., Pharmacy Operations, Wal-Mart

**Disclosure**
The author of this activity and its publisher, Therapeutic Research Center, do not have any financial interest related to the field of study covered by this CE activity.

**Time to Complete**
It should take participants about one hour to read the material and answer the questions.

**Date of Release**
This continuing education activity was released on September 21, 2002.

**Date of Expiration**
September 30, 2004.

**Date of Last Review**
Under the policies of *Pharmacist's Letter/Prescriber's Letter*, our educational courses are reviewed 24-26 months after original publication. If a course is reprinted within 26 months of its first publication, all information will be reviewed and revised, if necessary, to assure that participants will receive up-to-date information.

**Credit for Pharmacists**
*Pharmacist's Letter* is accredited by the American Council on Pharmaceutical Education as a provider of continuing pharmaceutical education. This course has been assigned universal program number 422-000-02-023-H03. If you want to earn 1 hour of CE credit (0.1 CEUs) from this course, answer the quiz questions. Credit will be awarded to participants who answer at least 70% of the quiz questions correctly. Pharmacists required to report law CE for Arizona, Idaho, Massachusetts, New Mexico (out-of-state licensees only), and Oregon can use this course for their requirement. This course has been approved by the Idaho State Board of Pharmacy and the Oregon Board of Pharmacy.

**Software Requirements**
To view this course and submit your answers online, it is best to use a computer with Internet Explorer 5.0 and above or Netscape Navigator 4.0 and above. It is required that you have "cookies" enabled in your web browser. Your connection to the Internet should at least be a 28K dial-up connection. You may also need the FREE Adobe Acrobat Reader, available at www.adobe.com.

*More. . .*

**CE Questions Quiz #02014**

1. If your hospital or pharmacy is considered a "hybrid entity," which of the following employees must be trained to comply with the new HIPAA privacy rules?
A. Employees working in the hospital gift shop
B. Check-out clerks working at the front of a grocery store
C. Pharmacy technicians
D. All of the above

2. Patient medical information is considered protected health information under HIPAA if it is:
A. patient-specific information created or received by a hospital or pharmacy.
B. concerning a patient's health condition in the past, present, or future.
C. information that can identify the patient.
D. All of the above

3. When should you give the minimum necessary information when discussing a patient's drug therapy with another person?
A. When talking with the patient's physician
B. When counseling the patient about the medication
C. When communicating with the patient's insurance payer
D. All of the above

4. A patient requests a list of any disclosures you've made about their health information in the past six years. How long do you have to provide the patient with a list of all the non-routine uses of their health information?
A. 14 days
B. 30 days
C. 60 days
D. 90 days

5. Under the revised HIPAA privacy rules, getting a patient to sign a consent form before using their protected health information is:
A. mandatory.
B. optional.
C. optional only under emergency situations.
D. not allowed.

6. When are you required to give or mail your Notice of Privacy Practices to a patient and receive acknowledgement that the patient has received it?
A. The same day when you first provide treatment or services
B. Within one week of when you first provide treatment
C. As soon as reasonably possible for emergency treatment or services
D. Both A and C

7. Which of the following would be adequate evidence of your attempt to obtain written acknowledgement of your Notice of Privacy Practices?
A. Documentation of why the patient did not sign the acknowledgement
B. A copy of the notice or a short summary that is signed by the patient
C. A privacy notice log book signed by the patient
D. All of the above

8. HIPAA requires that you keep a copy of the patient acknowledgements of your Notice of Privacy Practices for at least:
A. 180 days.
B. 3 years.
C. 6 years.
D. 10 years.

9. Which of the following situations would be considered marketing and require written authorization by a patient to disclose their health information?
A. Explaining to the patient how to use a blood glucose monitor for diabetes
B. Sending patient refill reminders
C. Recommending the generic version of a drug
D. Giving a drug company representative a list of patients using a competitor's drug

10. A 68-year-old patient requests that you release her medical records to her sister. When filling out the authorization form to disclose the patient's information, the patient is NOT required to state the exact purpose for the release.
A. True
B. False