Get Patients to Acknowledge Receipt of Your Notice of Privacy Practices

The HIPAA privacy regulations require health care plans and providers to give their patients a written notice of privacy practices. The notice of privacy practices must tell the patient how the plan or provider may use and disclose the patient’s protected health information (PHI) and spell out the patient’s privacy rights under HIPAA. And now the privacy regulations require a health care provider that has a direct treatment relationship with a patient to take an extra step: The provider must make a “good-faith effort” to get the patient’s written acknowledgment that she received the provider’s notice of privacy practices.

This acknowledgment requirement is one of the major changes that were made to the HIPAA privacy regulations in August 2002. The acknowledgment requirement replaces the requirement, which had been in the earlier version of the privacy regulations, that a provider get a patient’s consent to use or disclose her PHI for treatment, payment, and health care operations.

If the HIPAA privacy regulations require your organization to get a patient’s acknowledgment, your failure to make a good-faith effort to do so may expose you or the organization to HIPAA penalties.

We’ll answer the most common questions about the acknowledgment requirement. We’ll also give you some examples of how to comply with this requirement.

Who Must Get Acknowledgment?

If your organization is a health care provider with a “direct treatment relationship” with a patient, the HIPAA privacy regulations require you to make a good-faith effort to get the patient’s acknowledgment that he has received your notice of privacy practices. According to the privacy regulations, a health care provider has a direct treatment relationship with the patient if it provides health care services, products, diagnoses, or results to the patient. For example, hospitals, surgeons, and physical therapists generally have a direct treatment relationship with their patients.

A health care provider that has an indirect treatment relationship with a patient doesn’t have to get the patient’s written acknowledgment. A health care provider has an indirect treatment relationship with the patient if it provides services, products, diagnoses, or results based on the orders of another health care provider—and delivers its health care products, services, diagnoses, or results to the other health care provider, rather than to the patient. For example, a radiologist or lab may have an indirect treatment relationship with a patient.

(continued on p. 2)
From Whom Must You Seek Acknowledgment?

Generally, you’ll get the acknowledgment from the patient. But there are a few exceptions. For example, if a patient is a minor, you must give the notice of privacy practices to a custodian in place of the parent (say, a court-appointed guardian).

PRIVACY PRACTICES (continued from p. 1)

What’s a Good-Faith Effort to Get Acknowledgment?

The HIPAA privacy regulations don’t spell out what a good-faith effort is. But the commentary to the regulations says that a provider satisfies the good-faith requirement if it mails a notice of its privacy practices to a patient before its first treatment encounter with that patient and includes an acknowledgment of receipt of the notice on a tear-off sheet or other document that the patient is asked to sign and mail back to the provider. The Department of Health and Human Services will provide future guidance on what’s a good-faith effort, according to the commentary.

What Must Acknowledgment Include?

The HIPAA privacy regulations don’t spell out what form the acknowledgment must take, its content, or how a provider may get the acknowledgment from a patient. You’ll need to determine the specific acknowledgment processes that your organization will use.

For instance, you may have a separate acknowledgment form for patients to sign when they receive your notice of privacy practices, according to the commentary to the privacy regulations. Or you may request that the patient initial a cover sheet attached to its notice of privacy practices.

Alternatively, the commentary says, if a pharmacist gives the pharmacy’s notice of privacy practices to a customer when he picks up his prescription, the pharmacist—who has a direct treatment relationship with the patient—may have the patient sign the same logbook he signs when he picks up his prescriptions, as long as the patient is clearly informed of the purpose of the written acknowledgment. For instance, the pharmacist may use a separate entry in a logbook for the patient’s acknowledgment.

But it may be more practical for a pharmacist to use a separate document for acknowledgments, says health information manager and privacy officer Peggy Presbyla. A provider is only required to get a patient’s acknowledgment one time, she points out. So keeping acknowledgments separate from other items signed by the patient makes it easier for a provider to comply with the HIPAA privacy regulations’ record-keeping requirements, she says.

Insider Says: Even if your organization is an indirect treatment provider or health plan, you may still want to get patients’ written acknowledgment of receipt of your notice of privacy practices—although there’s no HIPAA requirement to do so. For example, a health plan may want to get the patient’s written acknowledgment when she enrolls as a plan member and is given a copy of the plan’s notice of privacy practices.

© 2002 by Brownstone Publishers, Inc. Any reproduction is strictly prohibited. For more information call 1-800-643-8095 or visit www.brownstone.com
Similarly, when a patient is incompetent or is otherwise unable to make health care decisions, you should give the notice of privacy practices to—and seek to get an acknowledgment from—the patient’s personal representative. This is because the privacy regulations require a health care organization to treat a personal representative as the patient, says health care attorney Michael D. Bell. He explains that a personal representative is a person who has the legal authority to act on behalf of the patient in making decisions related to health care.

When Must You Seek Acknowledgment?

Generally, except in emergencies, the HIPAA privacy regulations require you to give the notice of privacy practices to a patient no later than the date you first deliver service to the patient after the HIPAA privacy compliance date (Apr. 14, 2003). The same is true for making a good-faith effort to get the patient’s acknowledgment of receipt of the privacy practices: It must be done no later than the date you first deliver service to the patient—except in emergencies (see below). Since you’ll typically ask a patient to acknowledge receipt of your notice of privacy practices at the same time you give the notice to him, this deadline shouldn’t pose any problems to you.

According to the commentary to the regulations, if your organization’s first treatment encounter with a patient is over the telephone, you must, on the day of the conversation, send two things to the patient (either by mail or electronically):

- Your notice of privacy practices; and
- Some means for the patient to acknowledge receipt of that notice.

**Example:** The same day a physician takes a call from a patient, he may send his notice of privacy practices, along with a tear-off sheet or other document (say, an acknowledgment form) that directs the patient to sign the acknowledgment and return it to the physician. If the physician does all this, he’ll be considered to have made a good-faith effort to get the patient’s acknowledgment, according to the commentary. And he won’t be in violation of the HIPAA privacy regulations if the patient chooses not to return the signed acknowledgment, the commentary says.

**Insider Says:** When a patient’s initial contact with your organization is simply to schedule an appointment, that’s not considered a first treatment encounter. And you don’t, at that time, have to send the notice of privacy practices to, or get an acknowledgment from, the patient. Instead, you may wait until the patient arrives at your office for his appointment to give the notice of privacy practices to him and seek his acknowledgment.

Can You Get Acknowledgment Electronically?

If your organization delivers its notice of privacy practices electronically to the patient, your computer system should be able to electronically capture the patient’s acknowledgment of receipt of its notice, the commentary says. Here’s how this would work: You send an e-mail to the patient that includes your notice of privacy practices. When the e-mail is delivered to the patient’s e-mail address, your computer should automatically generate a confirmation or “return receipt” that the e-mail was delivered. Your computer should have a way to log these return receipts.

**Example:** Patient A goes to XYZ Hospital’s emergency room with severe chest pains and is immediately treated there. At that time, XYZ Hospital isn’t required to give Patient A its notice of privacy practices, nor is it required to get acknowledgment of the patient’s receipt of that notice.

What about later, after the emergency has ended? The HIPAA privacy regulations require a provider to give the patient its notice of privacy practices as soon as is “reasonably practicable” after emergency treatment. Must you then seek to get the patient’s written acknowledgment of receipt of the notice? The regulations don’t say anything on this point. And privacy experts we spoke to disagreed on what you should do.

Since nothing in the HIPAA privacy regulations specifically requires you to then seek the patient’s acknowledgment, Aagaard says there’s no reason for you to do so. But health information manager and privacy officer Shari Grace believes that the emergency treatment exception applies only during the emergency. When the emergency is over, the provider should follow through with business as usual, she says. According to Grace, this means providing the patient with a notice of privacy practices and seeking a written acknowledgment of receipt.

Aagaard agrees that nothing in the HIPAA privacy regulations prevents a provider from seeking the acknowledgment as soon as is reasonably practicable after the emergency. But in that case, she doesn’t believe seeking an acknowledgment is required by the regulations.

(continued on p. 4)
Can You Treat a Patient Who Won’t Give a Written Acknowledgment?
From time to time, your organization may be unable to get a patient’s written acknowledgment of receipt of your notice of privacy practices. For example, a patient may refuse to sign an acknowledgment after being requested to do so. If that’s the case, you can still treat the patient. The HIPAA privacy regulations allow a direct treatment provider to use or disclose the patient’s PHI to carry out treatment, payment, and health care operations without the patient’s permission, says health care attorney Ralph L. Glover II. Your organization shouldn’t refuse to treat a patient who won’t give it a written acknowledgment, Glover says.

What if You Don’t Get Patient’s Acknowledgment?
If your organization doesn’t get the patient’s written acknowledgment, the HIPAA privacy regulations require you to document your good-faith effort to get the acknowledgment from the patient and the reasons you didn’t get it. For instance, you may use a tracking form that includes the date you gave the notice and acknowledgment to the patient, how these documents were delivered (say, in person or mailed), whether the patient signed and returned the acknowledgment and, if the acknowledgment wasn’t returned, a check-box of reasons (for example, “patient refused” or “failure to mail back”).

Example: Patient A calls XYZ Health Clinic for treatment purposes. After the phone call, XYZ mails Patient A its notice of privacy practices with an acknowledgment form. The form instructs Patient A to sign the acknowledgment and return it in the enclosed pre-addressed envelope. Patient A doesn’t send back the acknowledgment form. XYZ must document that an acknowledgment form was sent to Patient A with instructions to sign and return it in the enclosed envelope but that the patient failed to do so.

As long as you document your good-faith effort to get the patient’s acknowledgment, your failure to get it isn’t considered a violation of the privacy regulations, according to the commentary.

How Long Must You Keep Acknowledgment or Documentation of Your Effort to Get One?
Keep any written acknowledgment of receipt that you get from a patient for at least six years from the date the patient signs the acknowledgment. Or if you don’t get a patient’s acknowledgment and, instead, document your good-faith effort to get it and the reasons it wasn’t received, keep this documentation for at least six years from the date the good-faith effort was made.

If You Revise Your Notice of Privacy Practices, Must You Get a New Acknowledgment from the Patient?
From time to time, your organization may revise its notice of privacy practices. In that case, you needn’t get a new written acknowledgment from a patient who has already signed one.

Insider Sources
Jana Aagaard, Esq.: Senior Corporate Counsel, Catholic Healthcare West, Sacramento Office, 10540 White Rock Rd., Ste. 130, Rancho Cordova, CA 95670; jaagaard@chw.edu.
Michael D. Bell, Esq.: Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, PC, 701 Pennsylvania Ave. NW, Washington, DC 20004; (202) 434-7481; mdbell@mintz.com.
Ralph L. Glover II, Esq.: Michael Best & Friedrich, LLC, 401 N. Michigan Ave., Chicago, IL 60611; rl Glover@mbf-law.com.
Shari Grace, RHIA: HIM Director/Privacy Officer, Marshalltown Medical & Surgical Center, Marshalltown, IA 50158; sgrace@marshmed.com.
Peggy Presbyla, RHIA: HIM Director/Privacy Officer, James Square Health and Rehab Centre, 918 James St., Syracuse, NY 13203.

W A S H I N G T O N  P I P E L I N E

CMS to Enforce HIPAA Transaction and Code Set Standards
In an Oct. 15, 2002, press release, HHS announced that the Centers for Medicare & Medicaid Services (CMS) will be responsible for enforcing HIPAA’s transaction and code set standards (TCS). The TCS are the technical part of HIPAA and are designed to streamline and standardize the electronic filing and processing of health care claims. “To accomplish this will require an enforcement operation that will assure compliance and provide support for those who file and process health care claims and other transactions,” HHS Secretary Tommy Thompson said. “CMS is the agency best able to do this.”

The deadline for compliance with the TCS was Oct. 16, 2002, but small health plans and organizations that filed for an extension have an extra year to comply.

According to the press release, CMS will conduct outreach activities in an effort to increase awareness of the TCS requirements and help health care organizations comply. It will also establish enforcement processes and develop regulations related to the TCS. The enforcement activities will
include responding to complaints and providing organizations with opportunities to show that they’re in compliance or planning corrective action, the press release said.

HHS’s Office for Civil Rights (OCR) will continue to be responsible for the enforcement of the HIPAA privacy regulations. According to the press release, CMS and OCR will work together on HIPAA outreach, enforcement, and other issues that affect both organizations.


**OCR Answers FAQs About HIPAA Privacy**

On Oct. 8, 2002, the HHS’s Office for Civil Rights (OCR) posted on its Web site a list of frequently asked questions (FAQs) and answers about the HIPAA privacy regulations. The OCR expects to update these FAQs and provide additional guidance in the future, according to the Web site. There are 23 FAQs and answers that address such varied topics as business associates, incidental uses and disclosures, small health plans, and third party administrators.

Here’s a summary of a few of the FAQs and OCR’s answers:

**When can a person submit a complaint about a possible privacy violation by a health care organization?** OCR said not before the compliance date of April 14, 2003. Beginning on April 14, a person may submit a privacy complaint to OCR, to the organization accused of violating patient privacy, or to both.

**Can a physician’s office use a patient sign-in sheet and call out patients' names in the waiting rooms?** OCR responded yes, provided that reasonable safeguards are in place and the information disclosed is limited. OCR gave an example to illustrate its answer: “…the sign-in sheet may not display medical information that is not necessary for the purpose of signing in (for example, the medical problem).”

**Must a health care organization monitor its business associates?** OCR replied no. The HIPAA privacy regulations require an organization to have written contracts with all its business associates to protect the privacy of PHI. But an organization isn’t required to monitor the way its business associates carry out privacy safeguards or abide by the privacy requirements of their contracts. OCR did note, though, that if an organization finds out a business associate has violated its contract, the organization is obligated to take steps to end the violation, and if unsuccessful, terminate the contract. And if termination isn’t feasible, the organization must report the privacy violation to OCR.

**Can a physician’s office fax patient medical information to another physician’s office?** OCR said yes. The privacy regulations permit a physician to disclose PHI to another health care provider for treatment purposes—and this disclosure may be made by fax. OCR added that the physician must have reasonable and appropriate safeguards in place to protect PHI that’s disclosed by fax. OCR gave examples of two such safeguards: having the sender confirm that the fax number to be used is correct, and “placing the fax machine in a secure location to prevent unauthorized access to the information.”

*Insider Says:* To read the FAQs, go to [www.hhs.gov/ocr/hipaa/whatsnew.html](http://www.hhs.gov/ocr/hipaa/whatsnew.html). Scroll down to “10/8/02 — New Frequently Asked Questions About the HIPAA Privacy Rule are now available” and click on “[DOC = 69KB].”

**New California Law Addresses HIPAA Preemption**

California recently passed a new law to help identify which of its medical privacy laws are preempted—that is, superseded—by HIPAA and which ones should be repealed in 2003 to conform to HIPAA. The new law, which goes into effect Jan. 1, 2003, says that California’s Office of HIPAA Implementation (CalOHI) will have the authority to:

- Determine which sections of California state law are preempted by HIPAA—because they’re not as strict as the HIPAA regulations; and
- Declare that those preempted sections of state law won’t be enforced. Eventually, the legislature is expected to repeal those sections.

The CalOHI was created to standardize HIPAA implementation across state agencies. The office will issue its findings so that both public and private entities can see how the state will interpret HIPAA. And it will assist organizations in complying with HIPAA by providing legal and technical advice. The office’s Web site has already begun to provide HIPAA resources, tools, and compliance advice.

How to Handle Patient Requests to Send PHI by Alternative Means or to Alternative Locations

From time to time, patients may ask your health care organization to communicate their protected health information (PHI) to them in a different way or to a different location from where you ordinarily would send it. For instance, a patient may ask you to send her appointment reminder in a closed envelope, rather than by the postcard that you usually use. Or the patient may ask you to send test results to a post office box, rather than to her home, as you usually would.

Must you agree to these requests? The HIPAA privacy regulations give patients the right to ask a health care organization to communicate their PHI by alternative means and to alternative locations. But they don’t necessarily require you to accommodate every request you get. We’ll tell you about the requests that a patient has a right to make according to the HIPAA privacy regulations. And we’ll give you practical guidance to help you deal with these requests and decide which ones to accommodate.

Requests Patients Have a Right to Make

According to the HIPAA privacy regulations:

Alternative means. A patient may ask your health care organization to communicate her PHI to her by alternative means. For instance, a patient may ask you to call her with test results instead of mailing them to her.

And a patient may ask your organization not to send PHI by a particular means. For example, a patient may ask her gynecologist not to use postcards when sending her an appointment reminder.


Alternative locations. A patient may ask a health care organization to send his PHI to alternative locations. For example, a patient may ask you to communicate with him at his place of employment, by mail to a designated address (say, a friend’s house), or by phone to a designated number (say, his cell phone number rather than his home phone number).

And a patient may ask a health care organization not to send his PHI to a particular location. For example, a patient who doesn’t want his family members to know about a certain treatment may request that you not communicate with him about that treatment at his home address or phone number.

Consider Requiring Written Requests

As a general rule, a patient’s request for a confidential communication can be oral or written. But the HIPAA privacy regulations let your organization require that a request be written. It’s a good idea to do this. Having the patient’s request in writing will reduce the likelihood of any mistakes or misunderstandings.

If you require a written request, make sure you spell this out in your notice of privacy practices, even though the regulations don’t specifically say you must, says Gwen Hughes, professional practice manager with the American Health Information Management Association. For example, your notice of privacy practice could say the following:

Model Language

You have the right to request that your protected health information be provided by alternative means or at alternative locations. Any such request should be submitted in writing to [insert name and address of department and title of contact person].

Special Rules for Providers

According to the HIPAA privacy regulations, the requests you must accommodate vary depending on what type of an organization you are. If you’re a health care provider, you must accommodate a patient’s request to communicate her PHI by alternative means or to alternative locations, if the request is “reasonable.”

Consider only administrative difficulty. The comments to the HIPAA privacy regulations let a health care provider determine whether a request is reasonable based solely on the administrative difficulty of complying with the request. So, for instance, if your organization determines that it would have administrative difficulty in complying with a patient’s request, it may deny the request. For example, a patient may ask your organization to send any correspondence electronically. But if your physicians don’t have e-mail capabilities, you would have administrative difficulty in complying with the patient’s request and could deny the request.

Don’t ask for a reason. Don’t ask the patient to give a reason for the request as a condition for accommodating the request, warns HIPAA Project Manager Christine Jensen. It doesn’t matter why the patient is asking you to provide the PHI by alterna-
tive means or at alternative locations. As long as the request is reasonable from an administrative ease stand-
point, you must accommodate it—regardless of the patient’s motive for her request, she explains.

» Don’t consider patient’s “rea-
son” in your decision. Don’t deny a pa-
tient’s request because you don’t think the patient has a good reason—either stated or unstated—for the request. The comments to the HIPAA privacy regulations caution that a provider can’t refuse to accommodate a request based on its perception of the merits of the patient’s reason for making the request, notes Jensen.

Special Rules for Health Plans
A health plan must accommodate rea-
sponsible requests by patients to get their PHI communications sent by alterna-
tive means or to alternative addresses only if the patient states that the disclo-
sure could put her in danger. So a health plan may require a patient to give it a statement that disclosure of her PHI could put her in danger. And the plan can make receipt of that statement a condition for granting the accommo-
dation, says health care attorney Jana Aagaard. But, she explains, a health plan can’t refuse to accommodate a request based on its perception of whether the patient is in actual danger.

A health plan can determine rea-
sonableness in the same way as a health care provider can. That is, a health plan can decide whether a request is reasonable based on the administrative difficulty of complying with the request.

Insider Says: A health plan may choose to adopt a blanket policy that says it will grant reasonable requests without requiring the patient to make a statement regarding danger.

How Health Plan Can Get Statement of Danger
The HIPAA privacy regulations don’t spell out how a health plan should get that statement of danger from a patient. But some methods you can use include:

■ Asking the patient whether she could be in danger if her PHI is dis-
closed; or

■ Developing an alternative means/location request form for pa-
tients that covers this, suggests Aagaard. The patient would then need to complete the form and return it to you. The form could say:

Model Language
You have the right to request that your protected health information be communicated by alternative means or to an alternative address. The HIPAA privacy regulations require us to honor your request only if disclosure of all or part of your PHI to which the request pertains could put you in danger. If disclosure of your PHI could put you in danger, please check this box.

You May Refuse to Accom-
modate Requests that Lack Certain Information
The HIPAA privacy regulations let you refuse to accommodate a patient’s request if the patient doesn’t give you certain information, when appropri-
ate. For example:

■ A health care organization isn’t required to accommodate a patient’s request to send PHI by alternative means or to alternative addresses if the patient doesn’t give the organization, when appropriate, information as to how payment for any health care services provided to her will be handled. In other words, if the patient asks your organization not to send the bill to her home or work address, she must give you another address where you can send the bill, says Hughes. Otherwise, you don’t have to accom-
modate the request.

■ Your health care organization doesn’t have to accommodate a patient’s request if the patient doesn’t specify an alternative address or method of contact. For example, if a patient says that he doesn’t want to be contacted at his usual address or phone number but refuses to give you another way to get in contact with him, you don’t have to accommodate that request.

Insider Sources
Jana Aagaard, Esq.: Senior Corporate Coun-
sel, Catholic Healthcare West, 10540 White Rock Rd., Rancho Cordova, CA 95670.
Gwen Hughes, RHIA: Professional Practice Manager, AHIMA, 233 N. Michigan Ave., Ste.
2150, Chicago, IL 60601-5519.
Christine Jensen, RN: HIPAA Project Manag-
er, Denver Health, 777 Bannock St., MC 1932, Denver, CO 80204.
Federal Court Lets Government Subpoena Records

During a federal grand jury investigation, the government subpoenaed certain medical records from a Virginia hospital. The hospital refused to produce the records, claiming that doing so would violate the physician-patient privilege, the patient’s right to privacy, and the HIPAA privacy regulations.

The court disagreed with the hospital and ordered the hospital to produce the records. It held that federal law and courts don’t recognize physician-patient privilege; the government’s interests in getting the medical records in this case outweighed the patient’s right to privacy; and the HIPAA privacy regulations specifically allow the release of medical records in response to a grand jury subpoena [In re: Grand Jury Subpoena John Doe No. A01-209].

State Court Says DA’s Records Subpoena Intrudes on Patient Rights

An unidentified man stabbed another man to death in New York City. The police’s only information about the assailant was that it was a Caucasian male between 30 and 45 years old, who may have been bleeding when he left the scene.

Hoping to identify the assailant, the DA’s office subpoenaed 23 New York hospitals to turn over records of any white males between the ages of 30 and 45 who sought treatment on the day of the crime, or the next day, for a “laceration, puncture wound or slash, or other injury caused by or possibly caused by a cutting instrument and/or sharp object, said injury being plainly observable to a lay person.”

New York City Health and Hospitals Corporation (HHC), which ran four of the hospitals, refused to turn over emergency room triage logs containing patient information, claiming that doing so would violate the state’s physician-patient privilege.

New York’s top court agreed with HHC and ruled that the hospitals didn’t have to respond to the subpoenas. The court said that state law recognized physician-patient privilege and that the hospitals probably couldn’t gather the class of records the subpoena sought just by having a layperson (a hospital employee) look at the records.

Since the hospitals would have to analyze the records from a medical perspective, the DA’s request was too great an intrusion into patients’ rights [In the Matter of the Grand Jury Investigation in N.Y. Cty.].

Show Your Lawyer

Here are the court cases and/or laws referred to in this issue.