How to Avoid Common Mistakes When Giving Notice of Privacy Practices to Patients

One of the key steps direct treatment providers must take to comply with the HIPAA privacy regulations is to give each patient a written notice of its privacy practices. This notice tells the patient how the provider may use and disclose the patient’s protected health information (PHI), and spells out the patient’s privacy rights.

Unfortunately, many providers are making mistakes in complying with these requirements—mistakes that could turn out to be costly in the future. For example, some direct treatment providers believe that they don’t need to give each patient a take-home version of their notice of privacy practices—they think that having a laminated copy available for each patient to read is enough. Others believe that they can deny treatment to a patient who refuses to sign an acknowledgment that she received a copy of the notice. Making one of these mistakes could affect patient care or result in a privacy violation or patient’s lawsuit.

To help you avoid making these common mistakes, we give you 12 rules to follow. There’s also a Trainer’s Quiz on these rules to help you test your knowledge.

12 RULES FOR AVOIDING COMMON MISTAKES CONCERNING NOTICE OF PRIVACY PRACTICES

Rule #1: Give Each Patient Take-Home Copy of Notice of Privacy Practices, Not Just Copy to Look at On-Site

The HIPAA privacy regulations require a direct treatment provider to give each patient a take-home copy of its notice of privacy practices no later than when it first delivers service to the patient. It may not, as many organizations mistakenly do, just give a copy of its notice—say, a laminated page—to the patient to read in the office.

A health care provider has a direct treatment relationship with the patient if it provides services, products, diagnoses, or results direct to the patient. 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 services, products, diagnoses, or results to the other health care provider (as, say, a clinical lab might). An indirect treatment provider need only give its notice to the patient if the patient asks for it.

Your organization has met the requirement to give the patient the notice even if the patient: 1) refuses to accept the notice; 2) accepts the notice and then returns it to you or someone in your organization; or 3) reads the notice and then throws it in the trash. But leaving one copy—or even a stack of copies—of your organization’s
notice in the waiting room won’t meet this requirement, cautions IBM health care consultant Tom Hanks.

Example #1: Patient A visits Dr. X for the first time and is given a copy of Dr. X’s notice of privacy practices. Patient A reads the notice, then throws it in the trash. Dr. X has satisfied the requirement to give his notice to Patient A.

Example #2: Patient A visits Dr. Y for the first time. She’s given a laminated copy of Dr. Y’s notice of privacy practices and told to read the notice and return it to the receptionist. Dr. Y hasn’t satisfied the requirement to give his notice to Patient A, because he didn’t give her a copy of the notice to take with her.

The privacy regulations don’t require a direct treatment provider to give its notice of privacy practices to a patient during an emergency treatment situation. For instance, a hospital needn’t give its notice of privacy practices at the time a patient arrives at its emergency department needing an immediate appendectomy. But the regulations require the provider to give its notice to the patient as soon as possible after the emergency is over (say, after the patient is out of the surgical recovery room).

Trainer Says: Prison inmates don’t have a right to get a notice of privacy practices, says HIPAA consultant Errick Woosley. So if a patient is an inmate, your organization needn’t give the inmate a take-home copy of its notice.

Rule #2: Your Organization Needn’t Give Its Notice to Patient Each Time It Delivers Service to Patient

As stated above, the HIPAA privacy regulations require your organization to give its notice of privacy practices to a patient no later than the date it first delivers service to the patient. It needn’t, as some organizations mistakenly believe, give its notice at every treatment encounter with a patient. Nothing in the HIPAA privacy regulations prevents a provider from giving its notice of privacy practices at each treatment encounter, but it may cost you extra effort and money.

In some circumstances, though, your organization may tell you to give the notice at each encounter. It may be easier and more cost-effective for your organization. For example, a pharmacy may give its notice of privacy practices to each customer every time the customer comes in to pick up a prescription. And compliance coordinator and privacy officer Kelley L. Meeusen explains that his hospital decided that it was more economical to give a notice to every patient as part of the admissions process, rather than to implement a tracking system to determine whether the patient had previously gotten a notice.

Rule #3: Your Organization May Not Give Patients Summary Instead of Entire Notice

The comments to the HIPAA privacy regulations let your organization provide a “layered” notice of privacy practices to your patients, says Hanks. That is, your organization may create a top layer—one that briefly summarizes the longer, more detailed notice. But it can’t give just the top layer, as some organizations mistakenly do. If an organization uses the top layer, it must attach it to a copy of the entire notice, adds Hanks.

Example: XYZ Physician Practice has an eight-page notice of privacy practices that some patients find confusing. So XYZ decides to give patients a one-page summary of its notice. XYZ Physician Practice can’t give patients
Rule #4: Your Organization Can’t Post Its Notice Anywhere It Chooses—It Must Post Notice in Clear and Prominent Location at Each ‘Physical Service Delivery Site’

It’s likely that your organization has one or more “physical service delivery sites”—that is, one or more offices or facilities where it treats patients. If so, it must post its notice in “a clear and prominent location” at each site for all patients to see, says Hanks. It can’t, as some organizations mistakenly do, post a copy of its notice of privacy practices anywhere it wants in an office or facility, or just post it in the main office or facility.

Instead, the notice should be posted in a common area that’s reasonably accessible to all patients. For instance, a physician’s office may post its notice on or near a reception desk or on a wall in the patients’ waiting area, clearly in view. Similarly, a hospital may post its notice in the intake area where it’s clearly in view.

Rule #5: Your Organization Can’t Post Summary of Its Notice Instead of Entire Notice

If your organization is required to post its notice of privacy practices, it must post the entire notice. It can’t post just a summary of its notice, as some organizations mistakenly do.

The privacy regulations don’t spell out what form the posted notice must take. But the regulations do say that the posted notice must include the same information that’s distributed directly to the patient, not just a summary of that information. For example, your organization may simply post a copy of the same notice that it gives to patients. Or it may post a one-page poster of its entire notice.

Rule #6: If Your Organization Has Web Site, It Must Prominently Post Its Notice on Web Site and Make Notice Available Electronically Through Web Site

Some organizations mistakenly believe that posting their notice of privacy practices on their Web site is discretionary. But it’s not. If your organization has a Web site that describes its services, it must prominently place its notice of privacy practices on the Web site.

The regulations don’t define what a “prominent” location is. One way to ensure that your notice is posted prominently is to refer to it on your Web site’s home page—that’s the first page most people see when visiting your Web site—suggests data security and HIPAA compliance officer Chris Apgar.

The regulations also require your organization to make a copy of the notice available electronically through the Web site to any user who requests it. One way to do this is to include a statement on your Web site’s home page telling users how to get a copy of the notice. For instance, the statement could say “Click here to get a copy of XYZ Hospital’s notice of privacy practices.”

Rule #7: Your Organization Must Post Revised Notice and Make It Available to Anyone Who Requests It—but Needn’t Mail It to All Patients

The HIPAA privacy regulations don’t require your organization to mail a revised notice of privacy practices to all patients whenever the notice is revised, as some organizations mistakenly think they must, says Woosley. The comments to the HIPAA privacy regulations state that it would be unnecessarily burdensome to require providers to mail the notice to all current and former patients each time the notice is revised, because providers may have a difficult time identifying active patients.

Instead, your organization must make the revised notice available to any person who asks for it, as of the effective date of the revision. For instance, XYZ Hospital’s revised notice of privacy practices will take effect on Jan. 1, 2006. On that date, it must make the new notice available to any person who asks for a copy of the hospital’s notice of privacy practices.

If your organization maintains a physical service delivery site, the regulations also require your organization to post the revised notice in a clear and prominent location, where it’s reasonable to expect patients to see it (see Rule #4). The revised notice must be posted no later than the effective date of the revision.

Your organization must also make sure that the revised notice is given to new patients no later than when it first delivers service to them, and made available on its Web site,
according to frequently asked questions (FAQs) issued by HHS’s Office for Civil Rights (OCR).

Example: Dr. X revises his notice of privacy practices, effective Jan. 1, 2005. On Jan. 2, 2005, Dr. X treats Patient A for the first time. Dr. X must give Patient A a copy of his revised notice and post the revised notice in a clear and prominent location in his facility. Dr. X must also post his revised notice on his customer service Web site and make the revised notice available to anyone who requests it.

Rule #8: Your Organization Doesn’t Have to Get Signed Acknowledgment of Receipt of Notice from Each Patient, but Must Simply Make Good-Faith Effort to Get One

Many organizations believe that they must get each patient’s written acknowledgment of receipt of their notice of privacy practices. But the privacy regulations simply require your organization to make a good-faith effort to get the patient’s written acknowledgment that he has received the notice. This must be done at a time no later than when your organization first delivers service to the patient. But because 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 problem.

The regulations don’t define what a “good-faith effort” is. Presumably, if you have a face-to-face encounter with the patient and you hand the notice and an acknowledgment to her at that time, that’s a good faith effort. What if you mail the notice of privacy practices to the patient before your first treatment encounter with her? The comments say that a provider that does this satisfies the good-faith requirement if the notice includes an acknowledgment of receipt on a tear-off sheet or other document and asks the patient to sign it and mail it back.

According to the comments, if your organization’s first treatment encounter with a patient is over the telephone, it must, on the day of the conversation, send two things to the patient (either by mail or electronically): its notice of privacy practices; and a way for the patient to acknowledge receipt of that notice. If the provider does so, it will be considered to have made a good-faith effort to get the patient’s acknowledgment, according to the comments. It won’t be in violation of the HIPAA privacy regulations if the patient chooses not to mail the acknowledgment back, the comments say.

If you attempt to get an acknowledgment and the patient refuses to sign it, you can still meet the requirement, Hanks says. Document your good-faith effort by describing how you offered to get the patient’s written acknowledgment and how or why the patient refused to provide it, he explains. For instance, your organization may have a tracking form for you to fill out that includes the date the notice and acknowledgment were given to the patient, how they were delivered (say, in person or by mail), whether the acknowledgment was signed and returned by the patient, and if the acknowledgment wasn’t returned, a check box for reasons (for example, “patient refused,” or “failure to mail back”).

AT A GLANCE

12 Rules for Avoiding Common Mistakes Concerning Notice of Privacy Practices

1. Give Each Patient Take-Home Copy of Notice of Privacy Practices, Not Just Copy to Look at On-Site
2. Your Organization Needn’t Give Its Notice to Patient Each Time It Delivers Service to Patient
3. Your Organization May Not Give Patients Summary Instead of Entire Notice
4. Your Organization Can’t Post Its Notice Anywhere It Chooses—It Must Post Notice in Clear and Prominent Location at Each ‘Physical Service Delivery Site’
5. Your Organization Can’t Post Summary of Its Notice Instead of Entire Notice
6. If Your Organization Has Web Site, It Must Prominently Post Its Notice on Web Site and Make Notice Available Electronically Through Web Site
7. Your Organization Must Post Revised Notice and Make It Available to Anyone Who Requests It—but Needn’t Mail It to All Patients
8. Your Organization Doesn’t Have to Get Signed Acknowledgment of Receipt of Notice from Each Patient, but Simply Must Make Good-Faith Effort to Get One
9. Your Organization Mustn’t Ask for Signed Acknowledgment of Receipt Before Giving Patient Copy of Notice
10. Your Organization May Not Deny Treatment to Patient Who Refuses to Sign Acknowledgment
11. If Your Organization Revises Its Notice After It Gets Patient’s Acknowledgment of Receipt, It Doesn’t Have to Get New Acknowledgment from Patient

© 2004 by Brownstone Publishers, Inc. Any reproduction is strictly prohibited. Copying training program materials is a violation of federal law.
To subscribe, call 1-800-643-8095 or visit www.brownstone.com
In an emergency treatment situation, a direct treatment provider is excused from having to get the patient’s acknowledgment of receipt of the provider’s notice of privacy practices. So in an emergency, your organization doesn’t have to make a good-faith effort to get an acknowledgment, says health care attorney Jana Aagaard. But after the emergency has ended, the 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? Although the regulations don’t say anything on this point, December 2002 HHS guidance says your organization isn’t required to then seek to get the patient’s acknowledgment.

Rule #9: Your Organization Mustn’t Ask for the Signed Acknowledgment of Receipt Before Giving Patient Copy of Notice

Make sure you give the patient a take-home copy of your organization’s notice of privacy practices before asking the patient to sign an acknowledgment, says Aagaard. Although this may seem like just a common sense approach, she says that some organizations view the acknowledgment as a paperwork requirement that is somehow disconnected from the actual provision of the notice. In fact, Aagaard notes that as a patient, she has seen organizations make two key mistakes. They’ve asked her to sign an acknowledgment before giving her a copy of the notice. And then, instead of giving her the notice, they’ve given her a laminated copy—not a take-home version—of the notice.

Rule #10: Your Organization May Not Deny Treatment to Patient Who Refuses to Sign Acknowledgment

Some organizations mistakenly believe they can deny treatment to a patient who doesn’t sign an acknowledgment of receipt of the notice of privacy practices. But the HIPAA privacy regulations don’t give your organization the right to deny treatment to a patient if that patient refuses to sign an acknowledgment of receipt, says Hanks. Rather, if a patient refuses to sign, the provider must simply document its good-faith effort to get the acknowledgment, and the reason the acknowledgment wasn’t obtained, he explains.

Rule #11: If Your Organization Revises Its Notice After It Gets Patient’s Acknowledgment of Receipt, It Doesn’t Have to Get New Acknowledgment from Patient

If your organization revises its notice of privacy practices, it may have many patients who got the original notice and signed an acknowledgment of receipt of that notice. Your organization must give these patients a copy of the revised notice of privacy practices only if they ask for one. But many organizations also think they must get another signed acknowledgment of receipt of the revised notice. That’s not required, according to the regulations. Your organization must get the patient’s acknowledgment (or document its good-faith efforts to do so) only once—when initially giving the patient its notice of privacy practices.

Rule #12: Your Organization’s Notice of Privacy Practices Can’t Substitute for Getting Patient’s Authorization for Use or Disclosure When HIPAA Privacy Regulations Require Authorization

The privacy regulations generally let health care providers use and disclose a patient’s PHI for treatment, payment, and health care operations. This means that your organization doesn’t need the patient’s authorization to use or disclose her PHI to treat the patient, bill the patient, or carry out such health care operations as quality assessment and improvement activities. But other uses and disclosures of a patient’s PHI (say, for marketing purposes) generally require the patient’s prior written authorization.

If the HIPAA privacy regulations require your organization to get a patient’s authorization before it can make a particular use or disclosure of her PHI, it must get that authorization before making the use or disclosure. It may not, as some organizations mistakenly do, list a use or disclosure in its notice of privacy practices and assume it’s relieved of getting the patient’s authorization. Simply informing the patient of the use or disclosure through your organization’s notice of privacy practices doesn’t eliminate the need for it to get the patient’s authorization, according to OCR’s FAQs. Instead, the FAQs note that the notice must reflect the uses and disclosures your organization may make without the patient’s authorization, as permitted by the privacy regulations, as well as state that any other uses or disclosures only will be made with the patient’s written authorization.

TRAINER SOURCES

Jana Aagaard, Esq.: Law Office of Jana H. Aagaard, 5321 Antique Ct., Carmichael, CA, 95608; jaagaard@chw.edu.
Chris Apgar, CISSP: HIPAA Compliance Officer, Providence Health Plan, 3601 SW Murray Blvd., Ste. 10, Beaverton, OR 97005; chris.apgar@providence.org.
Tom Hanks: Partner, Health Care Strategy & Change, IBM Business Consulting Services, One IBM Plz., Chicago, IL 60611; TomHanks@us.ibm.com.
Kelley L. Meeusen, RHIT: Health Information Compliance Coordinator & Privacy Officer, Harrison Hospital, 2530 Cherry Ave., Bremerton, WA 98310; kelleymeeusen@hmm.westsound.net.
Errick Woosley, MPA: Cadounate Consulting, LLC, 2067 Rock Creek Rd., Batesville, IN 47006; woosleew@aol.com.
We’ve given you an overview of common mistakes that organizations make concerning the notice of privacy practices and what the privacy regulations actually require a direct treatment provider to do. Now let’s see if you can apply these 12 rules to real-life situations that health care organizations like yours are likely to encounter. The TRAINER’s Quiz, below, will give you an opportunity to test your knowledge. Take it, and see how well you do.

INSTRUCTIONS: Analyze the questions below according to the 12 rules we’ve given you for avoiding mistakes that organizations commonly make concerning their notice of privacy practices. Circle the answer you think is right. The correct answers (with explanations) appear after the quiz. Good luck!

<table>
<thead>
<tr>
<th>QUESTION #1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patient A goes to Dr. X for the first time. When she arrives at the office for her scheduled appointment, a nurse hands her a copy of Dr. X’s notice of privacy practices. She’s then asked to sign an acknowledgment that she got the notice. Patient A refuses to sign the acknowledgment. True or false: The HIPAA privacy regulations allow Dr. X to refuse to treat Patient A.</td>
</tr>
<tr>
<td>a. True.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>QUESTION #2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patient A goes to XYZ Mental Health Center for the first time and is given a summary of the center’s notice of privacy practices. True or false: XYZ Mental Health Center must give Patient A a copy of its entire notice of privacy practices.</td>
</tr>
<tr>
<td>a. True.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>QUESTION #3</th>
</tr>
</thead>
<tbody>
<tr>
<td>XYZ Medical Practice has a summary of its notice of privacy practices clearly posted on the wall next to its patient sign-in sheet. The practice also has its entire notice hanging on a back wall in the reception area behind a tall plant. True or false: XYZ Medical Practice has properly posted its notice of privacy practices.</td>
</tr>
<tr>
<td>a. True.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>QUESTION #4</th>
</tr>
</thead>
<tbody>
<tr>
<td>XYZ Ambulatory Care Center gives each patient its notice of privacy practices when the patient arrives for treatment. The notice explains what XYZ may do with the patient’s PHI, including uses and disclosures that require a patient’s authorization. True or false: As long as a use or disclosure is listed in XYZ Ambulatory Care Center’s notice of privacy practices, the notice can substitute for a patient’s authorization.</td>
</tr>
<tr>
<td>a. True.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>QUESTION #5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patient A visits XYZ Pharmacy for the first time. She’s handed a laminated copy of the pharmacy’s notice of privacy practices and is told to read the notice and return it to the counter. True or false: XYZ Pharmacy must still give each patient a take-home copy of its notice of privacy practices.</td>
</tr>
<tr>
<td>a. True.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>QUESTION #6</th>
</tr>
</thead>
<tbody>
<tr>
<td>On Jan. 2, 2005, Patient A goes to Dr. X for the first time. A nurse hands her a copy of Dr. X’s notice of privacy practices and gets Patient A to sign an acknowledgment of receipt of the notice. Dr. X later revises his notice of privacy practices, effective Jan. 1, 2006. On Jan. 2, 2006, Patient A returns to Dr. X for her annual exam. True or false: The HIPAA privacy regulations require Dr. X to give Patient A a copy of his revised notice and get her written acknowledgment of receipt of the notice.</td>
</tr>
<tr>
<td>a. True.</td>
</tr>
</tbody>
</table>
QUESTION #1
Correct answer: b
Reason: Rule #10 applies here.

Rule #10: Your Organization May Not Deny Treatment to Patient Who Refuses to Sign Acknowledgment

The HIPAA privacy regulations don’t give a health care provider (like Dr. X, here) the right to deny treatment to a patient who refuses to sign an acknowledgment of receipt. Rather, if a patient (like Patient A, here) refuses to sign an acknowledgment, the provider must simply document its good-faith effort to get the acknowledgment, and the reason it wasn’t obtained.

Wrong answer explained:

a. As explained above, a health care provider can’t refuse to treat a patient because the patient has refused to sign an acknowledgment of receipt of the provider’s notice of privacy practices.

QUESTION #2
Correct answer: a
Reason: Rule #3 applies here.

Rule #3: Your Organization May Not Give Patients Summary Instead of Entire Notice

The HIPAA privacy regulations require direct treatment providers (like XYZ Mental Health Center, here) to give each patient a take-home copy of its entire notice of privacy practices. A provider can’t give patients just a brief summary of the entire notice.

Wrong answer explained:

b. A direct treatment provider may attach a summary of its notice of privacy practices to a copy of the entire notice—but it can’t give patients just the summary of its notice.

QUESTION #3
Correct answer: b
Reason: Rule #4 applies here.

Rule #4: Your Organization Can’t Post Its Notice Anywhere It Chooses—It Must Post Notice in Clear and Prominent Location at Each “Physical Service Delivery Site”

The HIPAA privacy regulations require direct treatment providers with a physical service delivery site (like XYZ Medical Practice, here) to post its entire notice of privacy practices at the site, not just a summary of the notice. And it must post that entire notice in a clear and prominent location. In this case, XYZ’s notice is hidden behind a tall plant and not in a clear location. So XYZ Medical Practice’s notice isn’t properly posted.

Wrong answer explained:

a. As stated above, a direct treatment provider (like XYZ Medical Practice, here) must post its notice of privacy practices—not just a summary of the notice—in a clear and prominent location. If the notice is hidden behind a tall plant, it’s difficult for patients to read and so isn’t in a clear location.

QUESTION #4
Correct answer: b
Reason: Rule #12 applies here.

Rule #12: Your Organization’s Notice of Privacy Practices Can’t Substitute for Getting Patient’s Authorization for Use or Disclosure When HIPAA Privacy Regulations Require Authorization

If the HIPAA privacy regulations require a direct treatment provider (like XYZ Ambulatory Care Center, here) to get a patient’s authorization before it can make a particular use or disclosure of her PHI, the provider’s notice of privacy practices can’t substitute for getting the patient’s authorization. Simply informing the patient of the use or disclosure through its notice of privacy practices doesn’t eliminate the need for it to get the patient’s authorization.
Wrong answer explained:
a. A direct treatment provider (like XYZ Ambulatory Care Center, here) can’t eliminate the need to get a patient’s authorization to make a use or disclosure of her PHI by listing the use or disclosure in its notice of privacy practices.

QUESTION #5
Correct answer: a
Reason: Rule #1 applies here.

Rule #1: Give Each Patient Take-Home Copy of Notice of Privacy Practices, Not Just Copy to Look at On-Site

The HIPAA privacy regulations require a direct treatment provider (like XYZ Pharmacy, here) to give each patient a take-home version of its notice of privacy practices. XYZ Pharmacy won’t meet this requirement by handing patients a laminated copy of its notice that remains at the pharmacy.

Wrong answer explained:
b. As stated above, a direct treatment provider must give its notice to the patient for the patient to take with her.

QUESTION #6
Correct answer: b
Reason: Rules #7 and #11 apply here.

Rule #7: Your Organization Must Post Revised Notice and Make It Available to Anyone Who Requests It—but Needn’t Mail It to All Patients

Rule #11: If Your Organization Revises Its Notice After It Gets Patient’s Acknowledgment of Receipt, It Doesn’t Have to Get New Acknowledgment from Patient

The HIPAA privacy regulations require a direct treatment provider to make its revised notice available to any person who asks for it, as of the effective date of the revision. But the regulations don’t require a provider (like Dr. X, here) to give the revised notice to a patient and get an acknowledgment of receipt of the revised notice if the patient got a prior notice of privacy practices and signed an acknowledgment of receipt of that notice.

Wrong answer explained:
a. As stated above, a direct treatment provider who gave a patient a prior notice and got the patient’s signed acknowledgment needn’t give the patient a copy of its revised notice and get the patient’s acknowledgment of receipt of that revised notice.