What to Put in Your Organization’s Patient Authorization Form

Patient authorization will play a significant role in your compliance efforts because in many situations, the HIPAA privacy regulations require that a health care organization get a patient’s authorization before using or disclosing the patient’s protected health information (PHI). For instance, although you won’t need to get a patient’s authorization to use or disclose her PHI to treat her or bill for that treatment, you’ll have to get it before you can use her PHI for most marketing activities or disclose her PHI to an attorney.

So what must a HIPAA-compliant patient authorization include? And what happens if a patient refuses to sign it? The recent changes to the HIPAA privacy regulations—published in the Aug. 14, 2002, Federal Register—partially changed the answers to these and other questions about the HIPAA authorization requirements.

With the help of health information attorney M. Peter Adler and professional practice manager Gwen Hughes of the American Health Information Management Association (AHIMA), we’ll answer some key questions about the requirements as they now stand and about what a HIPAA-compliant patient authorization form should contain. Plus we provide you with a Model Form that you can adapt and use for your organization (see pp. 3–4).

What Are HIPAA’s Patient Authorization Requirements?
HIPAA’s patient authorization requirements are very specific about when a health care organization must get a written authorization from a patient, explains Hughes. An organization must get authorization from a patient only when it needs to use or disclose the patient’s PHI for a purpose not permitted or required elsewhere in the HIPAA privacy regulations, says Adler. So an organization needn’t get an authorization to carry out most treatment, payment, and health care operations. But it needs a patient authorization before it may release a patient’s PHI to a pharmaceutical company or disclose it to a life insurer requesting an applicant’s PHI. Authorization is also generally required when psychotherapy notes are requested, Adler points out.

What Must HIPAA Authorization Form Include?
Before the recent changes to the HIPAA privacy regulations, there were different requirements for authorizations depending on who requested the authorization and for what purpose. As a result, some organizations would have had to draft several different authorization forms. But the recent
changes to the regulations simplified the authorization requirements, in part, by eliminating the need for different forms. Now, all authorizations must contain the same core elements and statements. Our Model Form sets forth those elements.

Now, each patient authorization must:

- Be written in plain language—in a clear, concise, and readable manner;
- Say which “persons” or “class of persons” (that is, which individuals or organizations or group of individuals or organizations) may use or disclose the PHI (for example, “Mary Jones, MD” or “XYZ Surgery Center”) [Form, par. 2];
- Describe in detail the PHI that will be used or disclosed (such as “blood test results dated April 2, 2001”). Like our Model Form, your form can include check-off boxes to make it easier to fill out [Form, par. 3];
- Specify to whom (“persons” or “class of persons”) the PHI may be disclosed (such as “XYZ Insurance Company”) [Form, par. 5];
- Describe each purpose of the use or disclosure (such as, “to complete an application for life insurance”). The regulations state that if a patient initiates an authorization for his own purposes, the stated purpose may be “at the request of the individual” [Form, par. 6];
- State the patient’s right to revoke the authorization and either tell the patient how to do it or refer to the organization’s notice of privacy practices regarding revocation [Form, par. 7];
- State the consequences for the patient if the patient refuses to sign the authorization form [Form, par. 10]. With limited exceptions, an organization can’t refuse to treat the patient or pay for the treatment if the patient refuses to sign an authorization. Also, with limited exceptions, an organization can’t refuse to enroll the patient, drop the patient from enrollment, or make the patient ineligible for benefits, explains Hughes.

- Explain that once the PHI is disclosed in accordance with this authorization, it may be redisclosed to individuals or organizations that aren’t subject to the HIPAA regulations, which means the information may no longer be protected by HIPAA [Form, par. 9];
- Give the date or event when the authorization will expire (for example, “Dec. 31, 2003” or “at the end of the research study”). As our Model Form does, you may want to set an automatic expiration date (such as six months from the date the authorization is signed) that will apply only if the patient fails to specify an expiration date or event [Form, par. 8]. Your state law may also set requirements on expiration dates. You may need to include those in your authorization form;
- Be signed and dated by the patient or the patient’s representative and a copy provided to the patient or his representative; and
- If the authorization is signed by a personal representative of the patient, describe that person’s authority to act on the patient’s behalf.

Insider Says: If the authorization is for marketing purposes and the organization making the marketing communication is receiving some form of payment for it from an outside entity, the authorization must state that.
Get Patient Authorization that Meets HIPAA Requirements

Here’s a Model Form you can use to help you develop a HIPAA-compliant patient authorization form for your organization. It was adapted from a form created by Gwen Hughes of AHIMA. That form appeared in “Practice Brief: Required Content for Authorizations to Disclose,” published in the Nov./Dec. 2001 issue of Journal of AHIMA. Note that the form has been revised to include the recent changes to the HIPAA privacy regulations.

The Model Form starts with a heading in boldface type to help explain to the patient what he’s about to sign. The form then asks for patient information. It then states that the patient authorizes the use or release of his health information (par. 1). It has space to give the name and address of the person or organization entitled to make the disclosure (par. 2) and check-off boxes to describe the information to be used or disclosed (par. 3). It explains that sensitive health information may be included in the disclosure—this language is optional and may vary, depending on your state law (par. 4).

The form has space to state to whom the information may be disclosed (par. 5) and the purpose(s) of the disclosure (par. 6); describes the individual’s right to revoke the authorization, how the individual can revoke it, and the exceptions to that right (par. 7); and has space to set an expiration date or event (par. 8). The form explains the risk of redisclosure (par. 9) and has a choice of language about how signing it may affect health care treatment, payment, enrollment in a health plan, or eligibility for benefits (par. 10). It includes optional language naming the organization’s privacy contact (par. 11) and explaining that the patient will be given a copy of the authorization (par. 12).

The form includes lines for the individual or her representative and witness to sign and date. Show the authorization form to your attorney before using it.

---

**PATIENT AUTHORIZATION TO DISCLOSE HEALTH INFORMATION**

**Patient Name**

**Address**

**Health Record #** ___________________________ **Date of Birth** ___________________________

![Image of Model Form](image.png)

---

Optional I understand that the information in my health record may include information relating to sexually transmitted disease, acquired immunodeficiency syndrome (AIDS), or human immunodeficiency virus (HIV). It may also include information about behavioral or mental health services and treatment for alcohol and drug abuse.

(continued on p. 4)
This information may be disclosed to, and used by, the following individuals or organizations:
Name ____________________________________________________________________________________________________
Address __________________________________________________________________________________________________
__________________________________________________________________________________________________________
__________________________________________________________________________________________________________
This information is being disclosed for the following purpose(s): ______________________________________________
__________________________________________________________________________________________________________

I understand that I have the right to revoke this authorization at any time. I understand that in order to revoke this authorization, I must do so in writing and present my written revocation to [insert person or dept., e.g., the health information management dept., address], I understand that the revocation will not apply to information that has already been released in response to this authorization. I understand that the revocation will not apply to my insurance company when the law provides my insurer with the right to contest a claim under my policy.

Unless otherwise revoked, this authorization will expire on the following date, event, or condition: ________________

[Insert state law requirements regarding the authorization’s expiration, if needed.]

[Optional] If I fail to specify an expiration date, event, or condition, this authorization will expire six months from the date of signing.

I understand that once the information is disclosed pursuant to this authorization, it may be redisclosed by the recipient and the information may not be protected by federal privacy regulations.

[Choose one]
❑ I understand that I need not sign this form in order to ensure health care treatment, payment, enrollment in my health plan, or eligibility for benefits.

or
❑ I understand that if I refuse to sign this form, the organization can refuse (select all that apply):
❑ treatment  ❑ enrollment in the health plan  ❑ eligibility for benefits

[Optional] If I have questions about disclosure of my health information, I can contact [insert title, e.g., HIM director, privacy officer, or name and contact information, e.g. tel. #].

[Optional] I understand that I will be given a copy of this authorization form, after signing.

Signature of Patient or Legal Representative __________________________________________________________________ Date________________
If signed by legal representative, relationship to patient ____________________________ Date________________
Signature of Witness ____________________________________________________________________________________ Date________________

PATIENT AUTHORIZATION FORM (continued from p. 2)

What Else May Authorization Include?
The HIPAA privacy regulations say that a patient authorization may include other information, in addition to the elements required by the regulations, Hughes points out. But the additional language must be consistent with the HIPAA requirements, she adds. What might you want to add?

❑ If you request an authorization from a patient, you’re required to give the patient a copy of the signed authorization. So you may also want the authorization to state that, upon signing, the patient will get a copy of it [Form, par. 12].

❑ You may want to include contact information in the authorization in case the patient has any questions [Form, par. 11].
If your state law requires it, you may have to address the use or disclosure of sensitive health information (such as HIV status) [Form, par. 4]. For information on how this and other laws may come into play, see box, below.

Can HIPAA Authorization Be Combined with Another Document?

Generally, you may not combine one authorization with another authorization to create a compound authorization. But in three situations, the regulations permit the combination of an authorization with other authorizations or types of legal permission, says Hughes. The permitted exceptions involve:

1) **Authorizations for the use or disclosure of PHI created for a research study.** For example, you can combine a consent to use information in a research study with an authorization to disclose information acquired during the research.

2) **Authorizations for the use and disclosure of psychotherapy notes.** You may combine an authorization for a use or disclosure of psychotherapy notes with another authorization for a use or disclosure of psychotherapy notes. For example, a patient could authorize the disclosure of your organization’s psychotherapy notes about him to his regular physician and a second mental health professional. But you may not combine an authorization for disclosure of psychotherapy notes with an authorization for disclosure of the rest of the patient’s health record.

3) **Other permitted authorizations.** You may combine an authorization permitted by the regulations with any other permitted authorization, except when that authorization has conditioned treatment, payment, enrollment, or eligibility on the patient’s signing it. For example, an authorization to disclose a patient’s demographic information for marketing purposes can be combined in a single document with an authorization to disclose that same information for fundraising purposes.

When Is Authorization Invalid?

An authorization is invalid if it doesn’t have all the necessary elements, warns Hughes. An authorization is also invalid when:

- The expiration date or expiration event has passed;
- The authorization hasn’t been filled out completely;
- The organization knows that the authorization has been revoked;
- The authorization is inappropriately combined with another document;
- The organization knows that the information in the authorization is false.

The organization knows that “material”—that is, significant—information in the authorization is false.

**Insider Says:** Although many organizations now accept handwritten authorizations from patients, Hughes recommends stopping this practice. Most patients won’t know to include all the HIPAA-required elements (such as statements on revocation and expiration). If anything is missing, the authorization will be invalid and can’t be accepted after the April 2003 HIPAA-compliance date, she explains. Instead, to encourage patients to use your organization’s authorization form, make it readily available to them. For example, you can post it on your organization’s Web site, Hughes suggests.

---

**Make Sure Your Authorization Complies with Other Laws Besides HIPAA**

Other laws besides HIPAA apply to patient authorizations, says health information attorney M. Peter Adler. For example, various federal laws and regulations govern the release of alcohol and substance abuse records. And many state laws govern the release of medical records and set requirements for patient consents and authorizations, he explains.

Check with your attorney to find out what laws apply to your authorization and whether your state’s laws are more stringent—that is, more protective of patients’ rights—than HIPAA is. If they are, you may need to include additional language in your HIPAA authorization form to comply with state law, Adler advises. For instance, state authorization requirements may stipulate that you include a statement, like the one in our Model Form, notifying the individual that the health information to be disclosed may include highly sensitive information, such as HIV status, mental health, or substance abuse records [Form, par. 4].
Recent Reg Changes Clarify When Incidental Uses and Disclosures Are Permitted

When the HIPAA privacy regulations first came out, there was a lot of confusion over whether protected health information (PHI) could be used or disclosed in emergency rooms, waiting rooms, and other semi-private areas where it was likely to be overheard or seen by outsiders. Recent changes to the regulations have clarified that, subject to some conditions, these uses and disclosures—called “incidental uses and disclosures”—of PHI are permitted.

The recent changes were published in the Aug. 14, 2002, Federal Register. According to the preamble to the changes, HHS added the clarification so that communications essential to providing quality health care would continue to be allowed. We’ll explain what incidental uses and disclosures are and tell you what the HIPAA privacy regulations now require.

What’s an Incidental Use or Disclosure?
According to the HIPAA privacy regulations, an incidental use or disclosure of PHI “would be a secondary use or disclosure that cannot reasonably be prevented, is limited in nature, and that occurs as a by-product of an otherwise permitted use or disclosure.” For example, emergency room physicians often treat patients in joint treatment rooms that are separated only by partitions or curtains. As a result, the PHI that’s discussed with one patient may unavoidably be overheard by another patient. The recent changes to the privacy regulations say that this disclosure would be a permissible incidental disclosure.

Here are some examples of situations in which an incidental disclosure may occur:

- Discussion of a patient at a nursing station that might be overheard by personnel not involved in the patient’s care;
- The use of joint treatment areas;
- The use of sign-in sheets and the calling out of names in waiting areas; and
- Discussion of a patient’s condition held during training rounds.

When Are Incidental Uses and Disclosures Permitted?
According to the HIPAA privacy regulations, an incidental use or disclosure is permissible when all three of the following conditions have been met:

1) The use or disclosure is “incidental to” a permitted use or disclosure. That is, the use or disclosure is made as a by-product of a use or disclosure that’s permitted or required by the HIPAA privacy regulations.

Example: A patient’s PHI is discussed for treatment purposes by two nurses at a nurses’ station. A snippet of that discussion is overheard by a passerby. Since the conversation itself is a permitted disclosure of PHI for treatment purposes, this is an incidental disclosure.

2) Reasonable safeguards have been applied. The organization must have already taken reasonable steps to safeguard PHI from unnecessary disclosures.

Example: In the circumstance given in the example above, the hospital must have previously implemented adequate safeguards to protect PHI at the nurses’ station so that incidental disclosures would be minimized. For instance, it may have advised staff to speak softly in areas that may be accessible to visitors.

Other safeguards that could be implemented at a nurses’ station to prevent incidental disclosures might include adjusting computer monitors so that they’re out of view, requiring staff to keep documents containing PHI in covered folders or file cabinets, and locating fax machines and printers away from high traffic areas.

3) The minimum necessary standard has been implemented (where it’s applicable). The organization must make reasonable efforts to limit the use and disclosure of PHI to the minimum amount of information necessary to accomplish the purpose of the use or disclosure. This is known as HIPAA’s “minimum necessary standard.”

Must an Accounting to Patient Include Incidental Disclosures?
The HIPAA privacy regulations give patients the right to request and get an accounting of the disclosures a health care organization has made of their PHI. The recent changes clarify that incidental disclosures of PHI don’t have to be included in a patient’s accounting of disclosures. Although this situation wasn’t addressed when the recent changes to the HIPAA privacy were first proposed in March 2002, it was added to the final version of those changes that appeared on Aug. 14, 2002.

In the preamble to the recent changes, HHS explains that incidental disclosures are often unknown at the time they occur. So it’s impractical to require their inclusion in an accounting. HHS also points out that incidental disclosures are most often made as part of a permitted disclosure, and organizations don’t include permitted disclosures in an accounting.
**Student, Intern, Trainee Access to Health Information**

Q Can students, interns, and trainees working at our organization review and use our patients’ private health information?

A Yes, as long as you set up certain procedures to ensure privacy under HIPAA, says health care attorney Jay Silverman. Students, interns, and trainees learning under supervision to practice or improve their skills can access patients’ medical information and records to the same extent as other staff. So just as with permanent staff members, you must train students about your organization’s privacy policies and procedures before giving them access to patients’ private health information, and keep a record of that training, Silverman says. You should also require them to sign a confidentiality or nondisclosure agreement, and stress the consequences if they violate their confidentiality obligations.

**Reporting PHI to Cancer and Other Registries**

Q Do we need to get patient authorization before reporting protected health information (PHI) to a cancer or other disease-specific registry?

A No. Patient authorization isn’t required before a health care organization can disclose PHI to a public registry, explains Becky Buegel, director of health information management for Casa Grande Regional Medical Center. The HIPAA privacy regulations permit PHI to be used or disclosed for “public health activities” without patient authorization, she explains. And public health activities include reporting PHI to government agencies that are authorized by law to collect such information for the purpose of controlling or preventing disease or injury.

One example is a disease-specific registry that’s operated by a state agency (such as the Illinois State Cancer Registry). Because registries like this are meant to serve a public health purpose—that is, preventing or controlling disease—HIPAA permits health care organizations to disclose PHI to them, without requiring patient authorization. In fact, many states (like Illinois) make such reporting mandatory for its hospitals and other health care facilities.

Even though disclosures to public registries mandated by law don’t require patient authorization, your organization must keep track of such disclosures, Buegel points out. Should a patient request an accounting of your disclosures of her PHI—which is the patient’s right, under HIPAA—the accounting must include any disclosures made to public registries, she explains.

**Insider Says:** If your organization’s disclosure of PHI is to a private (or non-governmental) registry, such as a private research registry, you’ll likely need a prior authorization, Buegel says. In the commentary to the HIPAA privacy regulations, HHS points out that only disclosures made to a governmental or public registry are excepted from HIPAA’s authorization requirements.

---

**Example:** To comply with the minimum necessary standard, an ambulatory surgery center adopts a policy or policies granting its nontreating personnel (such as reception staff) very limited access to PHI (such as restricting access to a patient’s name, admission date, and physician’s name).


**Can an Incidental Use or Disclosure Violate HIPAA?**

Yes. Even if a use or disclosure is incidental, it isn’t permitted and may violate the privacy regulations if an organization fails to either adopt reasonable safeguards or implement the minimum necessary standard.

---

**Example:** A medical office has its computer screens facing the reception area, in plain view of its patients. A patient waiting in the reception area easily views the test results of another patient. Since the medical office failed to implement reasonable safeguards (such as relocating the computers or using screen covers or screen savers), the disclosure of the patient’s test results would likely be a HIPAA privacy violation.

---

**Insider Sources**

Becky Buegel, RHIA: Director of Health Information Management, Casa Grande Regional Medical Center, 1800 E. Florence Blvd., Casa Grande, AZ 85222.


---

© 2002 by Brownstone Publishers, Inc. Any reproduction is strictly prohibited. For more information call 1-800-643-8095 or visit www.brownstone.com
Hold Business Associate Training Program for Department Heads

The HIPAA privacy regulations require that you have written contracts with your business associates. But before you do that, you’ll need to educate your staff on the business associate requirements. And since department heads are more likely to deal directly with business associates than are other employees, start by holding a business associate training program just for your department heads. A training program is essential for two reasons—it will help fulfill HIPAA’s requirement to provide privacy training to your staff. And it will help you identify your business associates.

But how long should this training program be, and what topics should be covered? With the help of health information attorney Edward Shay, we’ll give you some tips on setting up a training program.

**Keep it short.** Limit the training program to one short session—say, 30 to 45 minutes, recommends Shay. Department heads will be a lot more cooperative about fitting a short meeting into their schedule than a long one. Plus you should be able to adequately cover all the basics in that time frame while keeping their attention, he adds.

**Give them the key terminology.** Explain some of the key terms used in the HIPAA privacy regulations, recommends Shay. For instance, explain the meanings of the terms “protected health information” (PHI), “de-identified,” “business associate,” and “disclosure.” And use those terms often throughout the program to reinforce the lesson.

**Give examples of business associate contracts.** Give the department heads some real-life examples of your organization’s contracts that include business associate functions. And point out how the department heads should treat a business associate contract under the HIPAA privacy regulations. This will help them to recognize which outside parties have to be treated as business associates.

Here are some typical contracts that you may want to include in your examples:

- A managed care contract that permits the plan to see patient records for credentialing purposes;
- A contract for radiologists to provide hospital-based imaging services, which includes administrative, supervisory, and teaching duties;
- A vendor contract for off-site medical records storage; and
- An emergency room staffing contract.

**Make them work through actual scenarios.** One of the best ways to help your department heads understand what you’re teaching them is to have them work through realistic scenarios, suggests Shay. You can do this by describing—orally or on a worksheet—some possible business associate contracts, he says. Once they’ve heard or read the facts, require your department heads to: identify the various parties and their respective responsibilities; determine whether the parties are your organization’s business associates; and identify the PHI and where it’s going. By the time they leave the program, your department heads should have a clear understanding of what a business associate is and how to work with one, he adds.

**Insider Says:** At the end of the training session, survey your department heads about possible business associates, recommends Shay. This is an excellent opportunity to ask them to identify and give you details about the parties they deal with who may be business associates. In future issues of the *Insider,* we’ll provide you with a model survey you can use for this purpose and give you tips on complying with the business associate requirements, which were changed in August.

**Insider Source**  