From time to time, a person or entity outside your health care organization may ask your organization to disclose to it a patient’s protected health information (PHI). But in many situations, that disclosure will require the patient’s authorization. The HIPAA privacy regulations bar a health care organization from disclosing PHI to an outsider without a valid patient authorization, except when the disclosure is for most treatment, payment, and health care operations purposes or is “otherwise permitted or required” by the regulations.

So, for example, a valid patient authorization would be required for a disclosure of PHI to an insurance company to which the patient has applied for insurance, a government agency conducting a suitability investigation of the patient, or the patient’s attorney. Otherwise, you could be accused of a HIPAA privacy violation and could expose yourself or your organization to fines, lawsuits, or imprisonment.

The elements required for a valid authorization received from an outsider are set out in the HIPAA privacy regulations. They’re the same for every organization, even though the policies and procedures for verifying the validity of the authorization may vary from organization to organization. To help you understand the elements that must be included in a patient authorization you receive from an outsider, we give you 11 rules to follow. There’s also a Trainer’s Quiz to help you test your knowledge.

**11 RULES TO FOLLOW WHEN VERIFYING THE VALIDITY OF AUTHORIZATIONS RECEIVED FROM OUTSIDERS SEEKING DISCLOSURE OF A PATIENT’S PHI**

To properly verify the validity of authorizations your organization receives from outsiders seeking disclosure of a patient’s PHI, follow these 11 rules.

**Rule #1: The Authorization Must Be in Writing and in Plain Language**

You may not rely on an outsider’s oral assurances that he or she has the patient’s written authorization to use and disclose the patient’s PHI. You must have written authorization before you can give the patient’s PHI to the outsider.
Example: Someone from a government agency calls you and tells you that the agency has the patient’s authorization to get a copy of her PHI from you to determine her eligibility for disability benefits. You can’t disclose the patient’s PHI to the agency in response to that phone call. You must ask the agency for a written authorization from the patient before you can respond to the request.

The patient's written authorization may be in the form of e-mail or electronic documents, according to the comments to the privacy regulations.

The authorization must be written in plain language. This means that the authorization must use common, everyday words, be organized in short sentences that use “you” and other pronouns, and be divided into short sections.

**Trainer Says:** Nothing in the HIPAA privacy regulations requires you to get the patient’s original authorization instead of a photocopy of that form. But your organization may have its own internal policies about whether you can accept photocopied authorizations, says health information manager Becky Buegel. For instance, her facility allows only originals to be accepted. This reduces the chance that an authorization has been changed without the patient’s knowledge, she says. So be sure you find out about and understand your organization’s policies before you accept a photocopied authorization.

**Rule #2: The Authorization Must Describe the Requested PHI in Detail**

The authorization must describe the PHI being requested with “sufficient specificity” to allow your organization to know what information the authorization is referencing. For example, the authorization may describe the information as “laboratory results from June 2002,” or “all laboratory test results,” or “results of MRI performed January 2001.” Your organization may then disclose only that described information.

From time to time, you may not understand which PHI is covered by the authorization (say, the PHI described in the patient authorization doesn’t match the PHI requested in the cover letter sent with that authorization). If you don’t understand which PHI is covered by the authorization, you must get clarification (orally or in writing) from either the patient or anyone else who authorized its disclosure.

The HIPAA privacy regulations set no limits on the amount of PHI the authorization can request. This means that a patient may authorize the disclosure of her entire medical record. But the preamble to the regulations states that the authorization must be specific enough to guarantee that the patient has a clear understanding that the entire record will be disclosed. For example, if the Social Security Administration requests all of a patient’s PHI from a health care organization in order to process the patient’s benefit application, the description in the patient’s authorization must specify “all PHI.”
Rule #3: The Authorization Must State Why the PHI Is Being Requested

The authorization must describe why the PHI is being requested (say, to determine a patient’s eligibility for disability insurance). For example, an insurer may ask participants to authorize their health plans to disclose PHI to the insurer’s subsidiary for the purpose of marketing life insurance to them.

Example: An insurer may ask participants to authorize their health plans to disclose PHI to the insurer’s subsidiary for the purpose of marketing life insurance to them.

Rule #4: The Authorization Must Identify Who’s Being Authorized to Disclose the Requested PHI

The authorization must include the name or other specific identification of the “persons or class of persons” being authorized to disclose the patient’s PHI. This may be an individual or organization, or a group of individuals or organizations.

Example: Patient A signs an authorization stating: “I, Patient A, authorize XYZ Hospital to disclose my most recent discharge summary to ABC Disability Insurer.”

If an authorization authorizes a class of persons (say, treating physicians) to disclose PHI to someone (say, an employer), the class must be described with “sufficient specificity” so that an organization presented with the authorization will know with “reasonable certainty” that the patient intended the organization to disclose the PHI.

The preamble to the privacy regulations gives the following example of an authorization that’s insufficiently specific: A patient gives a licensed nurse practitioner (who’s a health care provider under the privacy regulations) an authorization for “all physicians” to disclose PHI to the patient’s insurer. But the nurse practitioner, because she isn’t a physician, wouldn’t know with reasonable certainty that the patient intended for the practitioner to be included in the authorization as part of the physician class.

Rule #5: The Authorization Must State to Whom Your Organization May Make the Requested Disclosure

Similarly, the authorization must include the name or other specific identification of the “persons or class of persons” to whom your organization is authorized to disclose the required PHI. The identification of the authorized users or recipients, whether individuals, companies, government agencies, or other entities, must be stated with “sufficient specificity” to allow your organization to reasonably identify them.

Example: County Health Agency at 123 Main St., Anytown, USA, gives Dr. X at 456 Central Ave., Anytown, USA, a form authorizing Dr. X to disclose Patient A’s PHI to the agency. Dr. X can easily identify the agency as the entity to whom she’s being authorized to disclose Patient A’s PHI.

Rule #6: The Authorization Must State an Expiration Date or Expiration Event that Hasn’t Yet Passed

The authorization must state either:
- A date when the authorization expires (say, Jan. 1, 2004);
- A time period for which the authorization is valid (say, two years from the date the patient signed the authorization form); or
- An event directly related to the patient or the purpose of the disclosure upon the occurrence of which the authorization expires (say, “end of research study,” if the disclosure of the patient’s PHI is for research).

If the expiration date or event in an authorization you receive has passed, the authorization isn’t valid.

Trainer Says: Even if the stated expiration date hasn’t passed or the expiration event hasn’t occurred, the authorization still may not be valid, warns health care attorney Marc D. Goldstone. A federal or state law may limit the length of time for which an authorization is valid. For example, the preamble to the privacy regulations states that at least 15 states have adopted the National Association of Insurance Commissioners’ Insurance Information and Privacy Protection Model Act. The act specifies that authorizations signed for the purpose of collecting information in connection with an application for a life, health, or disability insurance policy can remain valid for no more than 30 months. If your state has adopted this law, the longest a patient’s authorization for the disclosure of PHI in connection with an insurance application may remain in effect is 30 months, even if the expiration date or event indicated on the form hasn’t occurred yet (say, until the patient terminates the coverage).
The authorization must state that the patient has the right to revoke the authorization in writing. But this right isn’t absolute. The privacy regulations create several exceptions to this right, which the authorization must describe. The authorization must state that the revocation right won’t apply to PHI that was disclosed before the revocation. And the patient must be told that the revocation won’t apply during a period that her insurer is permitted by law to contest a claim made under her policy.

Example: Patient A may sign an authorization saying: “I understand that I have the right to revoke this authorization at any time and must do so in writing. I understand that the revocation will not apply to PHI that has already been disclosed 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 made under my policy.”

The authorization must also include instructions on how the patient may revoke the authorization. For example, the authorization may include the following statement: “I must present my written revocation to the health information management department at XYZ Hospital, 123 Main St., Anytown, USA.”

From time to time, a health care organization’s notice of privacy practices will spell out the exceptions to the patient’s revocation right and describe how the patient may revoke the authorization. In that case, the authorization may simply refer to the organization’s notice rather than give the information on revocation itself.

The HIPAA privacy regulations don’t require your organization to verify the identity of the individual signing the authorization form if that individual is the patient. But if the patient’s personal representative signs the authorization, the regulations require the authorization to include a place for the representative to describe his authority to act for the patient.

If you get an authorization from a health care organization, it must tell the patient whether or not the organization can condition treatment, payment, enrollment in health plan, or eligibility for benefits on getting the authorization. In general, the privacy regulations prohibit the conditioning of treatment, payment, enrollment, or eligibility on getting an authorization.

Your supervisor should give you specific methods for verifying the authority of a personal representative. These may include contacting the person or entity requesting the disclosure to ask that they send you the applicable power of attorney, health care proxy form, or guardianship document, along with proof that the document is in effect, says Wagg.

Example: County Health Department sends XYZ Hospital an authorization authorizing XYZ to disclose Patient A’s most recent discharge summary to it. The authorization could say: "I understand that any disclosure of my PHI carries with it the potential for redisclosure by the recipient and the PHI may not be protected by the federal privacy rules.”
signed by Patient A’s brother, as the patient’s guardian. XYZ Hospital may ask the health department to send it a copy of the brother’s certificate of guardianship before disclosing Patient A’s PHI to it.

Rule #11: In General, the Authorization May Be Combined with Other Authorizations, but Not with Any Other Document

In general, the HIPAA privacy regulations allow a health care organization to combine an authorization with other authorizations to create a compound authorization. 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. But a compound authorization may not include the following authorizations:

■ An authorization for the disclosure of PHI for a research study (this authorization may be combined only with other types of written permission for the same research study—say, a consent to participate in the study);
■ An authorization for the disclosure of psychotherapy notes (this authorization may be combined only with another authorization for a disclosure of psychotherapy notes); and
■ An authorization that conditions the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits on that authorization’s being signed.

On the other hand, the regulations don’t allow an authorization to be combined with any other document (except for research-related permissions, as stated above). For example, the privacy regulations specify that an authorization can’t be combined with an organization’s consent form or notice of privacy practices.

TRAINER SOURCES

Becky Buegel, RHIA: Director of Health Information Management, Casa Grande Regional Medical Ctr., 1800 E. Florence Blvd., Casa Grande, AZ 85222.
Marc D. Goldstone, Esq.: Of Counsel, Hoagland, Longo, Moran, Dunst and Doukas, LLP, 40 Paterson St., New Brunswick, NJ 08903; mgoldstone@hoaglandlongo.com.
Gwen Hughes, RHIA: Business Development Consultant, Care Communications, 205 W. Wacker Dr., Ste. 1900, Chicago, IL 60606-1214; (312) 551-3100; ghughes@care-communications.com.

11 Rules for Verifying the Validity of Authorizations Received from Outsiders Seeking Disclosure of a Patient’s PHI

1. The Authorization Must Be in Writing and in Plain Language
2. The Authorization Must Describe the Requested PHI in Detail
3. The Authorization Must State Why the PHI Is Being Requested
4. The Authorization Must Identify Who’s Being Authorized to Disclose the Requested PHI
5. The Authorization Must State to Whom Your Organization May Make the Requested Disclosure
6. The Authorization Must State an Expiration Date or Expiration Event that Hasn’t Yet Passed
7. The Authorization Must State the Patient’s Right to Revoke the Authorization and Either Tell the Patient How to Do It or Refer to the Outsider’s Notice of Privacy Practices Regarding Revocation
8. The Authorization Must State that Once the Requested PHI Is Disclosed, the PHI’s Recipient May Redisclose It, and the Privacy Regulations May No Longer Protect It
9. The Authorization Must Tell the Patient Whether the HIPAA Privacy Regulations Allow the Outsider to Condition Treatment, Payment, Enrollment, or Eligibility for Benefits on the Authorization
10. The Authorization Must Either Be Signed and Dated by the Patient or Signed and Dated by Her Personal Representative and Describe the Representative’s Authority to Act for Her
11. In General, the Authorization May Be Combined with Other Authorizations, but Not with Any Other Document
We’ve given you an overview of how a health care organization may verify the validity of an authorization it gets from an outsider for the disclosure of a patient’s PHI. Now let’s see if you can apply the 11 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 11 rules for verifying the validity of an authorization your organization gets from an outsider for the disclosure of a patient’s PHI. Circle the answer you think is right. The correct answers (with explanations) appear after the quiz. Good luck!

QUESTION #1
A clerk from State Department of Insurance calls the director of XYZ Hospital’s Health Information Management (HIM) office and asks her for a copy of Patient A’s PHI. The clerk explains to the HIM director that the PHI is needed to evaluate Patient A’s claim for disability benefits. She assures the HIM director that she has gotten Patient A’s written authorization for XYZ to disclose the PHI to her. True or false: It was proper for the HIM director to disclose the PHI to the clerk?
   a. True.
   b. False.

QUESTION #2
County Welfare Office sends XYZ Hospital an authorization that authorizes XYZ to disclose to it all of Patient A’s PHI. A person other than Patient A has signed the authorization, and the authorization includes no information about the signer. True or false: The authorization as it now stands is invalid?
   a. True.
   b. False.

QUESTION #3
Midwife X treats Patient A during her pregnancy and delivers her baby. The following year, the disability insurance company to which Patient A is applying sends Midwife X an authorization form authorizing “all treating physicians” to disclose to it PHI from the last two years. True or false: The authorization describes who may receive the disclosed PHI with sufficient specificity to allow Midwife X to disclose Patient A’s PHI.
   a. True.
   b. False.

QUESTION #4
The Social Security Administration sends Dr. X an authorization authorizing Dr. X to disclose to it all of Patient A’s PHI. True or false: The authorization is invalid because it doesn’t describe the PHI to be disclosed with sufficient specificity?
   a. True.
   b. False.

QUESTION #5
XYZ Insurance Co. sends an authorization form to ABC Radiology on behalf of Patient A. The form is signed and dated by Patient A and authorizes ABC to send Patient A’s X-ray and imaging reports from July 2000 through July 2005 to XYZ for the purpose of determining Patient A’s eligibility for insurance. The authorization also states that the patient’s failure to sign the authorization may result in XYZ’s refusal to provide insurance. What additional elements must the authorization form include to comply with the HIPAA privacy regulations?
   a. The authorization must include an expiration date or expiration event that hasn’t passed.
   b. It must include a statement of the patient’s right to revoke the authorization in writing and the exceptions to that right.
   c. It must include a statement that any PHI disclosed could potentially be redisclosed by the recipient of the PHI and no longer protected under the HIPAA privacy regulations.
   d. All of the above.
The HIPAA privacy regulations require a patient’s authorization to disclose PHI to a person or entity outside your organization to be in writing. Because the HIM director didn’t get a written authorization from the clerk on behalf of Patient A, she couldn’t disclose the patient’s PHI to the clerk.

Wrong answer explained:

a. The HIM director shouldn’t have relied on the oral assurances of the clerk that she had the patient’s written authorization for the disclosure of the patient’s PHI. As stated above, the HIM director needed to get a written authorization before giving the PHI to the clerk.

The HIPAA privacy regulations require a class of persons authorized to disclose a patient’s PHI (like “all treating physicians” here) to be stated with “sufficient specificity” so that whoever is presented with the authorization will know with “reasonable certainty” that the patient intended to authorize them to disclose the requested PHI. In this case, Midwife X wouldn’t know with reasonable certainty that the patient intended for her to be included in the authorization as a “treating physician,” since she isn’t a physician.

Wrong answer explained:

a. As stated above, Midwife X can’t be sure that the authorization includes her as a “treating physician.”
TRAINERS' ANSWERS & EXPLANATIONS

QUESTION #5
Correct answer: d
Reason: Rules #6, #7, & #8 apply here.

Rule #6: The Authorization Must State an Expiration Date or Expiration Event that Hasn't Yet Passed

Rule #7: The Authorization Must State the Patient's Right to Revoke the Authorization and Either Tell the Patient How to Do It or Refer to the Outsider's Notice of Privacy Practices Regarding Revocation

Rule #8: The Authorization Must State that Once the Requested PHI Is Disclosed, the PHI's Recipient May Redisclose It, and the Privacy Regulations May No Longer Protect It

To comply with the HIPAA privacy regulations, the authorization must also include the following elements: 1) a statement of an expiration date or expiration event that hasn’t yet passed; 2) a statement of the patient’s right to revoke the authorization in writing and the exceptions to that right; and 3) a statement that the PHI used or disclosed may be subject to redisclosure by XYZ Insurance Co. and no longer protected under the HIPAA privacy regulations.

Wrong answers explained:
a, b, & c. As explained above, d is the correct answer because it includes all three of these answers.