HIPAA Privacy — Right to Access
Versus HIPAA Authorization

Sometimes we wish the Health Insurance Portability and Accountability Act (HIPAA) wasn’t so gray, and gave us clearer instructions on how to meet its requirements. Well here it is! The U.S. Department of Health and Human Services (HHS) has published the following guidelines that outline the differences between permitted HIPAA disclosures through an authorization and required disclosure under HIPAA right of access.

If patient requests for records and release of information falls within your job duties, this article is for you. It is well worth your time to go to the website listed here and read through the entire guidance.

If you are familiar with the release of information process for medical records, this guidance changes expectations for that process and differs from the old methods. Some changes include:

- If a patient requests access to his or her records, providers should not require a form to be completed with a signature
- While you always document the disclosure, you do not always have to have the patient’s signature
- You may use different forms for patient requests versus HIPAA authorizations

Requests for Access

Requiring a Written Request

A covered entity may require individuals to request access in writing, provided the covered entity informs individuals of this requirement. See 45 CFR 164.524(b)(1). Covered entities also may offer individuals the option of using electronic means (e.g., email, secure web portal) to make requests for access. In addition, a covered entity may require individuals to use the entity’s own supplied form, provided use of the form does not create a barrier to or unreasonably delay individuals from obtaining access to their patient health information (PHI), as described below.

Verification of Identity

The HIPAA Privacy Rule requires a covered entity to take reasonable steps to verify the identity of an individual making a request for access. See 45 CFR 164.514(h). The rule does not mandate any particular form of verification (such as obtaining a copy of a driver’s license). It generally leaves the type and manner of the verification to the discretion and professional
judgment of the covered entity, provided the verification processes and measures do not create barriers to or unreasonably delay individuals from obtaining access to their PHI, as described below. Verification may be done orally or in writing. In many cases, the type of verification may depend on how the individual is requesting and/or receiving access – whether in person, by phone (if permitted by the covered entity), by faxing or emailing the request on the covered entity’s supplied form, by secure web portal or by other means. For example, if the covered entity requires that access requests be made on its own supplied form, the form could ask for basic information about the individual that would enable the covered entity to verify that the person requesting access is the subject of the information requested or is the individual’s personal representative. For those covered entities providing individuals with access to their PHI through web portals, those portals should already be set up with appropriate authentication controls, as required by 45 CFR 164.312(d) of the HIPAA Security Rule, to ensure that the person seeking access is the individual or the individual’s personal representative. See [http://www.ahima.org/modelform](http://www.ahima.org/modelform)

**Unreasonable Measures**

While the Privacy Rule allows covered entities to require that individuals request access in writing and requires verification of the requesting person’s identity, a covered entity may not impose unreasonable measures on an individual requesting access that serve as barriers to or unreasonably delay the individual from obtaining access. For example, a doctor may not require individuals:

- Who want a copy of their medical record mailed to their home address to go to the doctor’s office to request access and provide proof of identity in person
- To use a web portal for requesting access, as not all individuals will have ready access to the portal
- To mail an access request, as this would unreasonably delay the covered entity’s receipt of the request and thus, the individual’s access

While a covered entity may not require individuals to request access in these manners, a covered entity may permit an individual to do so. Covered entities are encouraged to offer individuals multiple options for requesting access.

In addition, the Privacy Rule permits covered entities to disclose PHI for treatment, payment and health care operations without the need to first obtain a patient’s signature or authorization. See 45 CFR 164.506. As a result, if a patient wants their patient information shared among treating providers, the covered entities can and should do so. The patient should not have to facilitate this transmission by submitting an access request.

In summary: Providers should offer several ways for patients to request access to patient information. When a patient requests access, providers should consider their response so that it is not burdensome on the patient or cause delays for the patient to obtain the information. Not every request requires a signature from a patient on an official HIPAA authorization form. However, every request should include verifying the person requesting and should be documented. Providers can use their own form for that purpose. The entire guidance can be found at [https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html](https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html)
Frequently Asked Questions

Why should you depend on the individual’s right of access to facilitate the disclosure of PHI to a third party? Wouldn't it be easier to have the individual execute a HIPAA authorization to enable the covered entity to disclose PHI to a third party?

The PHI that an individual wants to have disclosed to a third party under the HIPAA right of access also could be disclosed by a covered entity pursuant to a valid HIPAA authorization. However, there are differences between the two methods – the primary difference being that one is a required disclosure and one is a permitted disclosure – that may make the right of access a more favorable choice for most disclosures the individual is initiating on her own behalf. These differences are illustrated in the following table:

<table>
<thead>
<tr>
<th>HIPAA Authorization</th>
<th>Right of Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Permits, but does not require, a covered entity to disclose PHI</td>
<td>Requires a covered entity to disclose PHI, except where an exception applies</td>
</tr>
<tr>
<td>Requires a number of elements and statements, which include a description of who is authorized to make the disclosure and receive the PHI, a specific and meaningful description of the PHI, a description of the purpose of the disclosure, an expiration date or event, signature of the individual authorizing the use or disclosure of his or her own PHI and the date, information concerning the individual’s right to revoke the authorization, and information about the ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization</td>
<td>May require request be in writing, signed by the individual, and clearly identify the designated person and where to send the PHI</td>
</tr>
<tr>
<td>No timeliness requirement for disclosing the PHI reasonable safeguards apply (e.g., PHI must be sent securely)</td>
<td>Covered entity must act on request no later than 30 days after the request is received</td>
</tr>
<tr>
<td>Reasonable safeguards apply (e.g., PHI must be sent securely)</td>
<td>Reasonable safeguards apply, including a requirement to send securely; however, individual can request transmission by unsecure medium</td>
</tr>
<tr>
<td>No limitations on fees that may be charged to the person requesting the PHI; however, if the disclosure constitutes a sale of PHI, the authorization must disclose the fact of remuneration</td>
<td>Fees limited as provided in 45 CFR 164.524(c)(4). Can only charge for labor, supplies and postage</td>
</tr>
</tbody>
</table>

Article prepared by Mollie McCammon, RHIA, CHP.

For more information about this issue of AFMC HealthIT HIPAAwatch, please visit afmc.org/healthit, email healthit@afmc.org or call 501-212-8616.