OCR Continues to Define Patient Access Guidelines

By Rita Bowen, MA, RHIA, CHPS, SSGB; Judi Hofman, BCRT, CHPS, CHP, CHSS; Susan Lucci, RHIA, CHPS, CHDS, AHDI-F; and Kelly McLendon, RHIA, CHPS

The Office for Civil Rights (OCR) has made it abundantly clear through numerous communications that providing individuals easy access to their own health information is one of OCR's most important mandates. Giving patients and their personal representatives access to their own information is a right prescribed by the HIPAA Privacy Rule. OCR has been reinforcing their positions on this subject with guidance posted on their website. Problems pertaining to access to health information are some of the most frequent complaints received by OCR from patients. These reported experiences have illustrated the need for more guidance on this topic to improve healthcare provider compliance.

OCR has acknowledged that issuing guidance can many times result in the need for further clarification. Questions and answers lead to additional questions, which in turn need to be addressed. The release of OCR guidance in February 2016 further clarified a patient's right to access their health information, and requires process changes to facilitate compliance. There appear to be several unintended challenges arising from the guidance in multiple areas, such as access requests for third parties designated to receive protected health information (PHI), and the fees permitted to be charged in fulfilling such requests. AHIMA, its component state associations (CSAs), vendors, and other entities have been collaborating with OCR regarding the need for more clarity on such matters.[1]

As of press time, official guidance and clarification on requests made by attorneys is still regarded as "fluid" by OCR since more information regarding detailed nuances of the guidance is still being determined. AHIMA is actively working with OCR, representing members while proactively providing OCR with input for future guidance and clarification.[2] The information access guidance provided by OCR does not have the force of law; it is not statutory obligation. However, it is recommended that the guidance be followed—especially as audit and enforcement actions may be based upon the positions as outlined by OCR. This article reviews some of the challenges and confusion around the guidance and provides clarification for health information professionals.

OCR Admits to 'Gray' Areas

As part of AHIMA's 14th Annual Hill Day and Leadership Symposium this spring, OCR Deputy Director Deven McGraw discussed OCR's newly published guidance, "Individuals' Right under HIPAA to Access their Health Information (45 CFR 164.524)," released January 7, 2016. According to OCR, complaints by individuals about denial of access to health data are the third most prevalent issue reported to the agency.

McGraw told symposium attendees that OCR has put much effort into this clarification document, but admitted there were still "gray" areas. She confirmed that there will be additional frequently asked question documents coming out in the near future. OCR wants to give patients more access to and control over their patient data while promoting more engagement with health outcomes. The agency says it is also becoming more cognizant of the implications for the healthcare providers that have to abide by the rules and provide the access because of the complaints received.

McGraw discussed the difference in the HIPAA Privacy Rule between an individual's right to request their own information versus a release of information requiring an individual's signed authorization. This is further complicated by the right of patients to have their information sent to a third party of their choice, such as an attorney. The HIPAA Privacy Rule guidance outlines that covered entities should obtain from the patient, in writing, their clear directive, specifically the name and address of the person to receive their information and the record format to be delivered. OCR expects that covered entities take reasonable steps to verify the identity of an individual granting a request for access. McGraw said that there will be identity proofing standards coming from OCR in the future to help with verification and authentication processes. There will also be clarification

on a timeline for subsequent enforcement action against covered entities that violate individual access, as outlined in the new access guidance. As of press time, a timeline was still not available.

Rights of Personal Representatives

A patient's access to their own health information is a required type of disclosure. HIPAA (45 CFR 164.524 (c)(4)) also extends an individual's rights to the individual's personal representative, which generally is a person who has authority under applicable law to make decisions related to healthcare on the individual's behalf.[3] As outlined, and with few limited exceptions, the HIPAA Privacy Rule gives individuals "a legal, enforceable right" to access, inspect, copy, receive, or direct any records to a designated person or entity of their choice.[4]

Requests for medical records made by any other person or entities on the behalf of the patient require an individual/patient signed authorization form, which is another type of permitted disclosure. Patient access, as required, is significantly different than a permitted disclosure of PHI (45 CFR 164.502(a)(1)(iv)). When a disclosure is based upon a signed patient authorization form from a third party and the request is not made directly by the individual/patient, the personal access to medical records rules do not apply (45 CRF 144.524 (a)(1)). In the HITECH-HIPAA Omnibus Rule preamble, the individual written request for access to PHI to be sent to a designated person other than the individual "is distinct from the authorization form."[5]

The statutory and regulatory guidance permits an individual or their personal representative the authority to request that their patient information be sent to a third party. A patient can even request that medical records or other patient information be sent to their attorney through this pathway, but these requests must be clearly initiated by the patient. OCR has continued to clarify the difference between an individual's right to access their medical records and requests allowed under other provisions of the HIPAA Privacy Rule outside of treatment, payment, or healthcare operations (TPO) with a signed patient authorization requirement. OCR states that "[t]he rights under the individual assess provisions at 45 CFR 164.524(a)(1) apply only to individuals (or their personal representatives under 45 CFR 164.502(g)) who request access to their medical records."[6]

It is important to remember that a patient is not required to sign an authorization form containing all the HIPAA-required components when they are requesting their records for themselves or their personal representative. A covered entity may require use of a designated form "provided use of the form does not create a barrier to or unreasonably delay the individual from obtaining access to his or her PHI [personal health information]." Additionally, keep in mind that disclosure to the patient via their request is mandatory, with a time requirement of 30 days or less. However, if a state has a more stringent requirement for delivery of information to the patient, then that requirement must be observed.

A patient request can be made verbally and a covered entity may request the patient place the request in writing or provide signature validation. These additional steps should not be viewed by the patient as a barrier to obtaining their medical information or OCR may view that as an obstacle. A covered entity or business associate may not require in-person requests and verification, use of a web portal for the request, or require the request be sent by mail. Signature and patient ID validation is still required, therefore care must be taken to keep perceived barriers to access at a minimum while still applying appropriate safeguards to ensuring the requestor is who they claim to be.

Patients may designate a third party to receive their health information on their behalf. When this is done it is important to obtain from the patient in writing their clear directive, specifically the name and address of the person to receive their information and the record format it should be delivered in. Remember that for authorizations signed by the patient for their own information or their named personal representative, it is not recommended that providers ask for a description of the purpose for the information being provided. While asking this question is not prohibited, denying access due to an answer to this question is prohibited. Hence it's unwise to ask the question as someone may mistakenly act upon the answer in a manner that violates the rules.

Permissible fees for patient requests include:

- Photocopying time
- Scanning time
- Time converting electronic PHI to requested format
- Time transferring PHI from electronic health record to portal, portable media, personal health record, etc.
- Supplies (paper, CDs, USB drives, etc.)

- Time preparing explanation or summary (if requested by individual)

Fees not permitted (for the patient and/or their representative) include:

- Reviewing the request for access
- Searching for and retrieving the PHI
- Locating and reviewing the PHI in the record
- Segregating or otherwise preparing the PHI that is responsive to the request
- Reviewing records to ensure the information relates to the correct individual
- Charging for view, download, and transmit actions or onsite inspection

The regulation allows covered entities to select from one of three methodologies for permissible fees that can be imposed to the patient. These are actual cost (as detailed in the allowed and not allowed categories above); average cost (i.e., average time calculated); and a flat fee for electronic copies not to exceed a total of $6.50 per release (for labor, supplies and postage).

The patient access language in HIPAA is straightforward, but the interpretation is complex and requires assurance that release of information requests are truly directed by the patient to someone who is making a healthcare decision on their behalf. The OCR guidance has provided some answers, but many questions remain. For example, what does a covered entity do when an attorney request is sent without the current contact information of the patient? Questions are likely to arise regarding identity-proofing standards as well. Seldom is an attorney the patient's personal representative as defined by HIPAA, although they may hold themselves out to be. When this question arises, what fees are appropriate becomes an issue. More guidance has been promised from OCR, and until then covered entities should review and, if necessary, update patient right to access policies and procedures and forms to ensure they include the latest guidance and apply reasonableness to all practices in order to avoid future access complaints.

Summary of Patient Access Dos and Don'ts

Patient (Individual) Access Request vs. Third Party Request for Disclosure of PHI

Patient (Individual) Access Request	Authorization for Third Party Disclosure
Disclosure is mandatory	Disclosure is discretionary
Reasonable + cost based fee	State fee (if applicable), reasonable cost of prep and transmittal or special authorization form (if no state fee applicable)
Timing requirement (30 days + extension)	No timing requirement for responding
a. Verbal request is allowable b. Written patient access request form can be required c. Use of an authorization form is not allowed	Authorization form required

Form vs. Form

Element	Patient (Individual) Access Request	Authorization for Third Party Disclosure
Patient ID	Recommended	Recommended
Description of PHI	Recommended	Required
ID of Discloser	Not Required	Required
Name of Recipient	Required (if recipient is third party)	Required
Description of Purpose	Not Recommended	Required
Expiration Date/Event	Not Recommended	Required

Signature/Date	Required if recipient is third party Can be required by discloser	Required
Rights and Warning ('Legalese')	Not necessary, could be viewed as an "obstacle"	Required
Form and format	Recommended	Not required, but might be a good idea
Warning if unsecure transmission	Recommended	Not required, but might be a good idea
Patient Request vs. Third Party Request		
Requestor	**Recipient**	**Type of Request**
Patient	Patient	Patient Access Request
Patient	Third Party	Patient Access Request; in writing with certain elements
Personal Representative	Personal Representative	Patient Request
Personal Representative	Third Party	Patient Access Request; in writing with certain elements
Third Party	Third Party	Authorization to Disclose to Third Party
Patient or Personal Rep forwarded by Third Party	Third Party	Patient Request; in writing with certain elements

Notes

[1] US Department of Health and Human Services. "Individuals' Right Under HIPAA to Access Their Health Information 45 CFR § 164.524." www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/.

[2] AHIMA. Comment letter to Office for Civil Rights Director Jocelyn Samuels on February 2016 guidance, April 20, 2016. http://bok.ahima.org/PdfView?oid=301448.

[3] US Department of Health and Human Services. "Individuals' Right Under HIPAA to Access Their Health Information 45 CFR § 164.524."

[4] Ibid.

[5] US Department of Health and Human Services. "Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule." *Federal Register* 78, no. 17 (January 25, 2013). www.gpo.gov/fdsys/pkg/FR-2013-01-25/pdf/2013-01073.pdf.

[6] Greene, Adam. "Are Attorneys Entitled to a 'HIPAA Rate'?" Davis, Wright, Tremaine LLP Privacy and Security Law Blog. November 5, 2015. www.privsecblog.com/2015/11/articles/healthcare/are-attorneys-entitled-to-hipaa-rate/.

Rita Bowen (rbowen@mrocorp.com) is vice president, HIM policy and compliance, at MRO. Judi Hofman (JudiHofman@catholichealth.net) is the regional privacy officer at Catholic Health Initiatives Franciscan Health. Susan Lucci (slucci@justassociates.com) is the chief privacy officer at Just Associates. Kelly McLendon (kmclendon@complianceprosolutions.com) is the managing director at Compliance Pro Solutions.

Article citation:
Bowen, Rita K.; Hofman, Judi; Lucci, Susan; McLendon, Kelly. "OCR Continues to Define Patient Access Guidelines" *Journal of AHIMA* 87, no.9 (September 2016): 36-39.