Changes to HHS Omnibus Rule give a patient the right to direct the covered entity to transmit PHI about themselves directly to another person or to a third-party entity designated by the individual. The individual’s request to direct the PHI to another person must be in writing, signed by the individual, and clearly identify the designated person and where to send the PHI.

A covered entity may accept an electronic copy of a signed request (e.g., PDF or scanned image), as well as an electronically executed request (e.g., via a secure web portal) that includes an electronic signature or a faxed or mailed copy of a signed request. The same requirements for providing the PHI to the individual, such as the fee limitations and requirements for providing the PHI in the form and format and manner requested by the individual, apply when an individual directs that the PHI be sent to another person. See 45 CFR 164.524(c)(3).

The following are just a few examples of how these provisions apply:

- A patient requests in writing that the hospital where she recently underwent a surgical procedure use its Certified EHR Technology (CEHRT) to send her discharge summary to her primary care physician, or to her own personal health record, and she supplies the corresponding direct address (an electronic address for securely exchanging health information using the direct technical standard).

- A patient sends a written request to his long-time physician asking the physician to download a copy of the PHI from his electronic medical record and email it in encrypted form to XYZ Research Institution, at XYZResearch@anywhere.com, so XYZ Research Institution can use his health information for research purposes.

- A patient requests in writing that her ob-gyn digitally transmit records of her latest pre-natal visit to a new pregnancy self-care app that she has on her mobile phone. The ob-gyn’s EHR has the ready capability to establish the connection in a manner that does not present an unacceptable level of security risk to the PHI in the EHR or other of the ob-gyn’s systems, based on the ob-gyn’s Security Rule risk analysis.

In each of these three examples, the covered entity has the capability to transfer the PHI in the requested manner and doing so would not present an unacceptable level of security risk to the PHI in the covered entity’s systems. Thus, after receiving the patient’s written request, the covered entity has 30 days (or 60 days if an extension is applicable) to send the PHI to the designated recipient as directed by the individual. However, in most cases, it is expected that the use of technology will enable the covered entity to fulfill the individual’s request in far fewer than 30 days.
OCR has posted “Questions and Answers About HIPAA’s Access Right” on its website https://bit.ly/2HKiNuS.

One section of the FAQ titled “Right to Have PHI Sent Directly to a Designated Third Party” has several important questions with answers to regarding the release of PHI to third parties. We encourage you to read through the entire list of Q&As on the website listed above.

**When do the HIPAA Privacy Rule limitations on fees that can be charged for individuals to access copies of their PHI apply to disclosures of the individual’s PHI to a third party?**

The fee limits apply when an individual directs a covered entity to send the PHI to the third party. Under the HIPAA Privacy Rule, a covered entity is prohibited from charging an individual who has requested a copy of her PHI more than a reasonable, cost-based fee for the copy that covers only certain labor, supply, and postage costs that may apply in fulfilling the request. See 45 CFR 164.524(c)(4). This limitation applies regardless of whether the individual has requested that the copy of PHI be sent to herself, or has directed that the covered entity send the copy directly to a third party designated by the individual (and it doesn’t matter who the third party is).

**What is a covered entity’s obligation under the Breach Notification Rule if it transmits an individual’s PHI to a third party designated by the individual in an access request, and the entity discovers the information was breached in transit?**

If a covered entity discovers that the PHI was breached in transit to the designated third party, and the PHI was “unsecured PHI” as defined at 45 CFR 164.402, the covered entity generally is obligated to notify the individual and HHS of the breach and otherwise comply with the HIPAA Breach Notification Rule at 45 CFR 164, Subpart D. However, if the individual requested that the covered entity transmit the PHI in an unsecure manner (e.g., unencrypted), and, after being warned of the security risks to the PHI associated with the unsecure transmission, maintained her preference to have the PHI sent in that manner, the covered entity is not responsible for a disclosure of PHI while in transmission to the designated third party, including any breach notification obligations that would otherwise be required. Further, a covered entity is not liable for what happens to the PHI once the designated third party receives the information as directed by the individual in the access request.

**Source:**


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