COSMOS
Navigate the Compliance Universe

Complete Healthcare Compliance Manual 2024
Patient Privacy and Security: Right of Access

By Kimberly White,[1] CHC

What Is a Patient's Right of Access?

A patient's right to access their health records is critical to their ability to control their own healthcare. Efficient access to one's medical record assists in monitoring serious health conditions, tracking disease progression, enhancing doctor–patient communications, and adhering to treatment plans.

Yet, according to the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR), one of the most common patient complaints they receive relates to patients' inability to obtain access to their medical records. Historically, the OCR has focused its enforcement actions on privacy and security breaches rather than patients' right to access their health records, but this changed in 2019 with the Right of Access Initiative and significant penalties levied against healthcare institutions for noncompliance.[2]

With the OCR's announcement of the Right of Access Initiative, the OCR promised to vigorously enforce patients' right to receive their medical records quickly, without being overcharged, and in a readily producible format of their choosing. According to former OCR Director Roger Severino, "For too long, healthcare providers have slow-walked their duty to provide patients their medical records out of a sleepy bureaucratic inertia. We hope our shift to the imposition of corrective actions and settlements under our Right of Access Initiative will finally wake up healthcare providers to their obligations under the law."[3] The OCR has thus far made good on this promise, announcing 44 right-of-access settlements as of May 8, 2023.[4] This area of the law is proving to be a critical tool in the government's enforcement arsenal. In order to avoid hefty fines and provide more positive patient outcomes, entities should be aware of the legal requirements associated with their patients' right to prompt, affordable access to their medical records and establish policies and procedures to empower patients to exercise that right effectively and efficiently.

Risk Area Governance

HIPAA Privacy Rule

Pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), covered entities must provide individuals, upon request, access to the protected health information (PHI) about them in one or more designated record sets maintained by or for the covered entity.[5] This includes the right to inspect or obtain a copy (or both) of the PHI, as well as directs the covered entity to transmit a copy to a designated person or entity of the individual's choice. A designated record set may include medical and billing records, enrollment, payment, claims, or medical management record systems and other records used by a covered entity to make decisions about an individual's health.

Individuals do not have a right to access PHI contained in quality assessment or improvement records, patient safety activity records, or business planning, development, and management records because they are not used to making decisions about individuals. Expressly excluded from the patient's right of access are psychotherapy

notes and information compiled in reasonable anticipation of litigation.[6]

While covered entities should respond to a patient's request for access as soon as possible, access should be provided no later than 30 days after the patient makes the request.[7] If, however, an entity is unable to provide access during the 30-day timeline, they may extend the time by an additional 30 days if they notify the patient in writing during the initial 30-day period. They must advise the requestor of the reason for the delay and the date they will provide the patient with the requested access.

In securing a patient's right of access, a covered entity may not impose unreasonable measures on an individual requesting access that serve as barriers to, or which unreasonably delay, the individual from obtaining access. For example, a doctor may not require individuals who want a copy of their medical records mailed to their homes to physically come to the doctor's office and provide proof of identity in person; use a web portal for requesting access, as not all individuals will have ready access to the portal; or mail an access request, as this would unreasonably delay the access. However, a covered entity may require individuals to request access in writing, provided the covered entity informs individuals of this requirement before transmitting.[8] Again, this requirement should not create an artificial barrier to the patient's right of access. To better facilitate a patient's ability to request a medical record, a covered entity may also offer individuals the option of using electronic means, such as a secure web portal, to make requests for access.[9]

Form and Format

HIPAA's Privacy Rule requires a covered entity to provide an individual with access to PHI in the form and format requested—if readily producible in that form and format.[10] Notably, whether or not it is "readily producible" is based on the entity's capability to provide in the format requested, not its willingness. A covered entity is not required to purchase new software or equipment to cover all potential requests. As a baseline requirement, however, if the information is maintained electronically, the covered entity must have the capability to provide *some* form of electronic copy of PHI.

To the extent that the PHI is not readily producible by the covered entity, it may produce the information in a readable format as agreed to by the covered entity and the requesting individual. Where an individual requests access to PHI that is maintained electronically by a covered entity, the covered entity may provide the individual with a paper copy of the PHI to satisfy the request only in cases where the individual declines to accept any of the electronic formats readily producible by the covered entity.[11]

Manner of Access

Under the Privacy Rule, a covered entity must provide patients access to their PHI as requested.[12] This would include, for example, arranging a convenient time and place for the patient to pick up a copy of the PHI or having a copy of the PHI mailed or emailed. It should be noted that mail and email are generally considered readily producible by all covered entities. 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, when requesting PHI by email, an individual has the right to request that it be sent unencrypted. In such cases, the covered entity must provide the requestor a brief warning that there is a level of risk that the individual's PHI could be read or otherwise accessed by a third party while in transit and confirm that the individual still wants to receive their PHI by unencrypted email. If the individual consents, the covered entity must comply with the request. If the individual was warned of and accepted the security risks associated with the unsecured transmission, the entity is not responsible for breach notification or liable for disclosures that occur

while the PHI is in transit.

A Reasonable Cost-Based Fee

The Privacy Rule permits a covered entity to impose a reasonable, cost-based fee when providing a patient a copy of their medical record. Generally, this fee will be based on the cost of actual labor costs, supplies, postage, and (if requested by an individual) the preparation of an explanation or summary of the PHI.[13] A covered entity may also use average labor costs, supplies, and postage—or a flat fee—for electronic copies of PHI maintained electronically. The flat fee is capped at $6.50.[14] The OCR has tended to be strict in its interpretation of labor, stating that it only includes labor for creating and delivering the electronic or paper copy once the PHI that is responsive to the request has been identified, retrieved or collected, compiled and/or collated, and is ready to be copied. A covered entity may not account for such things as overhead, quality reviews, storage costs, maintaining systems, or costs associated with searching for and retrieving the PHI, even when such costs are permitted under state law.

Rather than calculating labor costs for each request, the OCR has said a covered entity may develop a schedule of costs for labor based on average labor costs to fulfill standard types of access requests, as long as the types of labor costs included are the ones that the Privacy Rule permits in a fee and are reasonable. Covered entities may then add to that amount any applicable postage or supply costs, such as thumb drives. According to the OCR, covered entities should not use a per-page fee except when the PHI is maintained in paper form and the individual requests a paper copy of the PHI or asks that the paper PHI be scanned into an electronic format. Therefore, OCR does not consider per-page fees for copies of PHI maintained electronically to be reasonable.[15]

The OCR has advised entities that, ideally, they should forego fees for all individuals to access their medical records. This is especially vital in situations where the financial standing of the individual requesting the record would make it difficult or impossible for the individual to afford the fee. Further, an individual should never be denied access to their medical record due to having not paid a bill for services provided by the covered entity. The OCR has said it will continue to assess whether covered entities are charging fees to individuals creating barriers to the right of access and will take enforcement action where deemed necessary.

Individual's Right to Direct the PHI to Another Person

An individual, or the individual's personal representative, may direct a covered entity to transmit the individual's PHI directly to another person or entity. Such a request must be in writing, signed by the individual, clearly identify the person or entity being designated to receive the PHI, and state where the PHI should be sent. A covered entity may accept an electronic copy of a signed request, as well as an electronically executed request that includes an electronic signature.

The OCR previously held the position that the same requirements for providing the PHI to the individual, such as fee limitations, apply when an individual directs that the PHI be sent to another person or entity, such as a law firm representing the individual.[16] On January 23, 2020, however, a federal court vacated the "third-party directive" within the individual right of access to the extent it expanded the Health Information Technology for Economic and Clinical Health Act (HITECH) beyond requests for a copy of an electronic health record with respect to PHI of an individual in an electronic format.[17] Further, the court stated that the fee limitations set forth at 45 C.F.R. § 164.524(c)(4) only apply to an individual's request for access to their own records and does not apply to an individual's request to transmit records to a third party. While the OCR did not appeal this decision during the applicable time frame, it is not yet known whether it will accept the court's decision or promulgate new regulations. In the meantime, however, the fee restrictions still apply to patients who request their own medical

records.

Entities should also be mindful of relevant state laws to the extent they are more stringent than, and not preempted by, HIPAA.