Intersections of the ONC Information Blocking Rule and the HIPAA Privacy Rule May Create Overlapping Obligations

By Justin Joy, JD, CIPP

Health Information Accessibility, Interoperability, and Information Blocking

While there were likely earlier efforts, the policy of increasing health information exchangeability and system interoperability was stated over 25 years ago in the enactment of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Among the stated goals of the legislation was the implementation of standards to enable the efficient electronic exchange of health information, "consistent with the goals of improving the operation of the health care system and reducing administrative cost."[1] While these expressed goals were oriented more toward the financial aspects of the health care

system, namely health insurance claim processing and health plan administration, the HIPAA legislation also specifically directed the Secretary of the United States Department of Health and Human Services (HHS) to "study the issues related to the adoption of uniform data standards for patient medical record information and the electronic exchange of such information."[2]

Twenty years following the enactment of HIPAA, the 21st Century Cures Act was passed in 2016. The concepts set forth in the legislation concerning information exchanges and interoperability were not new. In many ways, the legislation was the next step toward increasing health information accessibility for patients and health care providers. Accordingly, the legislation provides for penalties for unreasonable impediments to information access, specifically, if operational practices are "likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information." [3] This impediment to information access, use and exchange is known as "information blocking." The law directed appropriate HHS agencies to "identify reasonable and necessary activities that do not constitute information blocking."[4]

On May 1, 2020, the HHS Office of the National Coordinator for Health Information Technology (ONC) issued its final rule on information blocking (the "Information Blocking Rule"). The American Medical Association's informational material on the regulation summarizes the definition of information blocking as:

> "[B]usiness, technical, and organizational practices that prevent or materially discourage the access, exchange or use of **electronic health information** (EHI) when an **Actor knows**, or (for some Actors like EHR vendors) **should know**, that these practices are **likely** to interfere with **access, exchange, or use** of **EHI**. If conducted by a health care provider, there must also be **knowledge that such practice is unreasonable** and likely to interfere with, prevent, or materially discourage access, exchange, or use of EHI."[5]

Among other individuals and entities, an "actor" under the Information Blocking Rule specifically includes "a health care provider."[6]

The AMA guidance material provides examples of specific circumstances when information blocking may occur: "Physicians can experience [information] blocking when trying to access patient records from other providers . . . [and] [p]atients can also experience [information] blocking when trying to access their medical records or when sending their records to another provider."[7] While there are many other aspects of the ONC's Information Blocking Rule, these two scenarios are the focus of the discussion below. The Information Blocking Rule specifically incorporates aspects of the HIPAA Privacy Rule, and as a result, an understanding of relevant provisions of the two regulations is required for effectuating compliance with both.

The Patient's Right to Access and Disclosures of PHI for Treatment Purposes under HIPAA

With relatively few exceptions, under the HIPAA Privacy Rule, patients or their proper personal representative, such as a parent of a minor patient, have a legally enforceable right to see and receive protected health information (PHI) in their "designated record set."[8] A HIPAA covered entity, such as a medical practice, may require a patient to make a request for access in writing, including on the group's own form, so long as patients are informed, perhaps in the group's notice of privacy practices, of the requirement for a written request. Relatedly, while covered entities must take reasonable steps to verify the identity of an individual making a request for access to PHI, the verification process cannot create barriers or unreasonable delays in obtaining access to PHI. If an access request is required to be made in writing, the form itself, or the process—including identity verification— for submitting the form, cannot impose unreasonable barriers on patients requesting access to their PHI. HHS has provided examples of what it deems to constitute unreasonable requirements. A medical practice may not require a patient, or their personal representative:

- Who wants a copy of her medical record mailed to her home address to physically come 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." **[9]**

While, in many cases, a patient may request access to their information to provide records to another provider themselves, no authorization is required for a provider to send a patient's PHI directly to another healthcare provider for the purposes of providing treatment.[10] One example provided by HHS of a disclosure for treatment purposes is a "primary care provider may send a copy of an individual's medical record to a specialist who needs the information to treat the individual."[11] Provided such a disclosure is made for the purpose of providing treatment to an individual, such a disclosure may be made without obtaining authorization[12] from the patient.

The Intersection of HIPAA and the Information Blocking Rule

The Information Blocking Rule specifically incorporates the HIPAA Privacy Rule in many aspects, including its scope of applicability. As an initial matter, the Information Blocking Rule regulates electronic health information (EHI). The Information Blocking Rule states, "EHI is defined as the electronic protected health information (ePHI) in a designated record set (as defined in the Health Insurance Portability and Accountability Act (HIPAA) regulations) regardless of whether the records are used or maintained by or for a covered entity."[13] Like the HIPAA Privacy Rule, there are numerous exceptions to the provision of access under the Information Blocking Rule including preventing harm to a patient or another person and privacy protection.[14] Unlike the HIPAA Privacy Rule, however,

which generally prohibits the disclosure of PHI unless permitted otherwise, the Information Blocking Rule requires the provision of unimpeded access to EHI unless an exception applies. In general, if a patient is entitled to access of PHI under HIPAA, the patient is likely entitled to unimpeded access to EHI under the Information Blocking Rule. Similarly, if PHI may be used or disclosed for treatment purposes without patient authorization under the Privacy Rule, the same EHI is likely subject to the Information Blocking Rule as to other providers who need access to the information.

Considering the regulatory overlap of the HIPAA Privacy Rule and the ONC Information Blocking Rule, while certain regulatory defenses may be available in the future to health care provider actors that are not available to other entities covered by the Information Blocking Rule, a covered actor may violate both the HIPAA Privacy Rule provisions pertaining to patient access and the ONC rule pertaining to information blocking.

An everyday scenario that may implicate both the Privacy Rule and Information Blocking Rule is the provision of PHI/EHI to other providers for treatment purposes. Many medical groups request new patients sign or initial a document, which is typically in the form of a consent, expressly providing an acknowledgement of patient's permission to disclose PHI for treatment purposes. As addressed above, the HIPAA Privacy Rule specifically states that a covered entity "may obtain consent of the individual to use or disclose protected health information to carry out treatment," medical groups should make the distinction between consent and a disclosure authorization. The distinction becomes significant if a medical practice's procedure for requiring patient involvement for permissible disclosures for treatment purposes results in conduct a provider knows "is unreasonable and is likely to interfere with access, exchange, or use of electronic health information."[15] For example, it is unnecessary for a practice to require a patient to complete, sign, and return a disclosure authorization prior to every disclosure for treatment purposes. Such a practice could constitute impermissible EHI blocking under the Information Blocking Rule, and perhaps, if the patient had also requested the information, an unreasonable barrier to patient access to their PHI. While obtaining a patient's written consent for disclosure of PHI for treatment (and payment) purposes on new patient registration forms may help confirm patient understanding of permissible disclosures, medical practices should re-evaluate their procedures for requiring additional patient involvement for disclosures for treatment purposes or when patients have requested access to their own records.

Health information technology has been rapidly evolving in physician practices for well over a decade. After many years of inaction, federal regulations are catching up toward the goal of facilitating information exchangeability and system interoperability. It is important that physician practices understand their obligations under these regulations as they pertain to the use of their electronic health record systems. Practices should review existing procedures, and, as necessary, implement new or revised proper procedures to avoid problems such as the scenario above.[16] While enforcement of the Information Blocking Rule as to health care providers has yet to begin, as patients increasingly have and expect immediate access to their health information, especially in electronic form, providers are at an increased risk of patient complaints and related risks.

[1]. Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, § 262, 110 Stat. 1936, 2025.

[2]. Id. § 263 at 2032.

[3]. 21st Century Cures Act, Pub. L. No. 114-255, § 4004 (2016) (codified as 42 U.S.C § 300jj-52 (a)(1)).

[4]. Id. (codified as 42 U.S.C § 300jj-52 (a)(3)).

[5]. American Medical Association, "What is information blocking?" at 1, https://www.ama-assn.org/system/files/2021-01/information-blocking-part-1.pdf

[6]. 45 C.F.R. § 171.102.

[7]. "What is information blocking?" at 1.

[8]. The definition of a "designated record set" is stated in the HIPAA Privacy Rule. 45 C.F.R. § 164.501.

[9]. HHS, Individuals' Right under HIPAA to Access their Health Information 45 C.F.R. § 164.524, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access/index.html.

[10]. A patient's request for a provider to send a copy of the patient's PHI to a third party is likely to be deemed an access request. While these requests are required to be in writing, signed by the individual, and clearly identify the designated person or entity and location where the PHI is to be sent, similar considerations apply to minimizing barriers for honoring these requests. This is situation different, however, from a third party requesting the PHI using a HIPAA compliant disclosure authorization signed by the patient.

[11]. HHS, Uses and Disclosures for Treatment, Payment, and Health Care Operations, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/disclosures-treatment-payment-health-care-operations/index.html.

[12]. Of note, there is a legal distinction between a patient's consent, which may, but is not required to be, obtained and a valid HIPAA disclosure authorization. As stated by HHS, "A 'consent' document is ***not*** a valid permission to use or disclose protected health information for a purpose that requires an 'authorization' under the Privacy Rule . . ., or where other requirements or conditions exist under the [Privacy] Rule for the use or disclosure of protected health information" Id. (emphasis added). Relatedly, providers must be aware whether a patient has requested, and the practice has agreed, to place restrictions on disclosure of PHI, which would prevent disclosures, even for treatment purposes, except in the case of an emergency.

[13]. 45 C.F.R. § 171.103(a)(3).

[14]. A summary discussion of the exemptions is provided by ONC. https://www.healthit.gov/curesrule/final-rule-policy/information-blocking.

[15]. 45 C.F.R. § 171.103(a)(3).

[16]. The Information Blocking Rule contains specific provisions which contemplate the existence of relevant written policicies and procedures. See 45 C.F.R. § 171.202(b).
