MURTHA CULLINA
ATTORNEYS AT LAW

NEWS ALERT

HEALTH CARE

Compliance Check-In: Are You Ready For The Information Blocking Rule?

By Daniel J. Kagan and Stephanie S. Sobkowiak | October 14, 2020

We are just weeks away from portions of the Office of the National Coordinator's ("ONC") Information Blocking Final Rule ("Final Rule") going into effect on November 2, 2020. While the Final Rule applies to health care providers, health IT developers, health information networks, and health information exchanges, this bulletin is designed as a reminder for health care providers.

For those who are unfamiliar, the Final Rule has two primary goals. First, it seeks to advance the interoperability of electronic health information ("EHI"). Said another way, it seeks to increase the ways patients can access, exchange, and use their EHI across different platforms. Second, as the name suggests, the Final Rule seeks to prohibit information blocking, which consists of activities that would otherwise interfere with, prevent or discourage the access, exchange or use of EHI.

There are eight exceptions to the Final Rule's prohibition on information blocking. When a health care provider's practices meet the conditions of an exception, then the provider is not engaging in information blocking. The exceptions fall into two categories. There are five exceptions that involve not fulfilling requests to access, exchange or use EHI: (1) preventing harm; (2) privacy; (3) security; (4) infeasibility; and (5) health IT performance. And, there are three exceptions that involve procedures for fulfilling requests to access, exchange or use EHI: (1) content and manner; (2) fees; and (3) licensing.

Of particular importance to health care providers are the preventing harm and privacy exceptions. The privacy exception recognizes that there is no requirement to provide an individual with the ability to access, exchange or use EHI if doing so would be prohibited under state or federal privacy laws. For example, if a state law has more restrictive measures in place prior to the release of EHI, *e.g.* mental health information, and the requestor has not satisfied those measures, *e.g.* through consent or another mechanism, then it is not information blocking to prohibit the access, exchange or use of EHI for that reason. Under the preventing harm exception, health care providers can deny access to EHI if they have a reasonable belief that blocking the EHI will substantially reduce a risk of harm, the practice is no broader than necessary, and the reason for blocking the EHI is one that could serve as grounds to block access to protected health information ("PHI") under HIPAA. Similar to HIPAA, a patient has a right to request a review of the denial of his/her request.

On the topic of access, the Office for Civil Rights ("OCR") recently announced two additional settlements under its HIPAA Right of Access Initiative, bringing its total to nine settlements since announcing this initiative as an enforcement priority in 2019. One of the core tenets of the Final Rule is to provide patients with increased access to their EHI. Accordingly, we will likely continue to see enforcement from both the OCR and ONC in situations where health care providers are not providing individuals with sufficient access to EHI/PHI and no exception applies.

In light of the above, now is a great time for health care providers to review their policies and procedures to ensure that they are ready to comply with the Final Rule. To comply with the privacy exception, health care providers should check their electronic health record platforms to ensure that they are following any federal and state laws that may be more restrictive than HIPAA. Additionally, and importantly, after the effective date, health care providers should be careful to ensure consistency in their application of the exceptions so that patients are not treated differently.

If you have any questions regarding the Information Blocking Final Rule or HIPAA access policies and procedures, please contact:
Stephanie S. Sobkowiak at 203.772.7782 or ssobkowiak@murthalaw.com
Daniel J. Kagan at 203.772.7726 or dkagan@murthalaw.com