Healthcare Law Alert – The CURES Act: What New York Health Care Providers Need to Know about Compliance and Enforcement of the Federal Information Blocking Rule

An onslaught of recently proposed federal regulations may leave New York health care providers understandably confused about what practices they should change in order to comply with the CURES Act and its key component, new federal rules and penalties attached to practices that constitute "Information Blocking." Requirements under the CURES Act have been promulgated through several federal rules and hundreds of pages in the Federal Register. Two rules issued on May 1, 2020, one from the Office of the National Coordinator for Health Information Technology (ONC) and one from the Centers for Medicare & Medicaid Services (CMS) make up the bulk of the new requirements. There is also a proposed enforcement rule from the Office of Inspector General of the Department of Health and Human Service (OIG), though OIG says its rule does not apply to health care providers who engage in Information Blocking.

The CMS final rule includes new Conditions of Participation for Hospitals, Psychiatric Hospitals and Critical Access Hospitals, requiring hospitals to send electronic admission, discharge and transfer (ADT) event notifications. The ADT event notification requirement builds on CMS's 2019 Discharge Planning final rule requiring hospitals to document all necessary medical information, including post-discharge goals and treatment preferences, in the patient's medical record. CMS has delayed implementation of the ADT event notification requirement until May 1, 2021.

While ONC's final rule includes new standards for certification for health IT developers, its main event is the promulgation of rules to deter Information Blocking. Information Blocking is defined generally as a practice that may interfere with the use, access or exchange of electronic health information (EHI), unless the activity complies with one of eight exceptions. Compliance with the ONC final rule is required beginning November 2, 2020. However, enforcement of the requirements has been delayed and will depend on publication of OIG's final enforcement rule. Even then, enforcement against health care providers remains uncertain given that the OIG proposed rule does not apply to them. OIG says in its proposed rule that it will coordinate with other agencies to identify future rulemaking to appropriately disincentivize health care providers from engaging in Information Blocking. This does not mean that health care providers should throw caution to the wind. In fact, it is clear from recent press releases that the Office for Civil Rights (OCR) is stepping up enforcement efforts on HIPAA access complaints, including announcing on October 9, 2020 that OCR had settled its ninth investigation under its HIPAA Right of Access Initiative. CMS has also previously established attestation requirements to support the prevention of Information Blocking by health care providers. (See OIG's proposed rule, 85 Fed. Reg. at 22,981, n.1).

So, against this background of an uncertain enforcement future, what should New York health care

providers know about the Information Blocking rule? First, the rule does not preempt New York law. ONC says repeatedly in its final rule that where a particular access, exchange or use of EHI is prohibited by applicable federal, state, or tribal law, restricted access does not constitute Information Blocking and compliance with an exception is not required. In addition, ONC says "nothing [in this rule] overrides Federal, State, or tribal law protections of patients' privacy preferences." (See ONC final rule, 85 Fed Reg. 25,830) Thus, if a health care provider is required by law to block access to an individual who is not a "qualified person" under N.Y. Public Health Law § 18, this is not information blocking and the health care provider need not demonstrate compliance with a particular exception. There are other exceptions that providers may be able to take advantage of based on current organizational policies and procedures. For example, the "Privacy Exception" allows providers to deny access where a "precondition" has not been satisfied, such as when patient consent or authorization may be required. Health care providers may demonstrate compliance through provider-specific documentation or organizational policies. Providers should review their patient access policies and procedures to determine whether additional specifics should be added to demonstrate compliance with an exception.

Health care providers should also be reassured that failure to comply with an exception is not fatal. ONC repeatedly makes the point in its final rule that practices that implicate the Information Blocking provision but do not meet an exception will be analyzed on a case-by-case basis to evaluate whether the actor had the requisite intent to engage in Information Blocking. While providers are better served to comply with an exception where possible, practices that are not discriminatory against particular actors, or meant to impede competition, may not be deemed Information Blocking. Health care providers also will not be subject to the maximum not-to-exceed $1 million per penalty fine under the Federal Civil Monetary Penalties law attached to Information Blocking violations. However, conduct that violates an individual's right of access could be subject to enforcement and penalties under HIPAA, which means that health care providers are best served to update their policies and procedures to ensure appropriate access under HIPAA and New York law despite the uncertainty surrounding enforcement of the Information Blocking rule against health care providers.

Please visit our Healthcare Law Practice Area to learn more about the legal services we can provide in this area. If you have any questions or would like more information on the issues discussed in this communication, please contact any member of our Healthcare Law practice.