Kim Stanger

Partner
208.383.3913
Boise
kcstanger@hollandhart.com

Healthcare Providers: Beware New Information Blocking Rule

Publication — 08/26/2020

Healthcare providers focusing on COVID-19 may have missed the final Interoperability and Information Blocking Rule that was published May 1, 2020 and takes effect **April 5, 2021**. (45 C.F.R. Part 171). The Rule implements the 21st Century Cures Act and furthers the government's efforts to enable the exchange of electronic health information ("EHI") to facilitate better outcomes, lower costs, and greater patient access to information. In general, the Rule prohibits covered actors from blocking the flow of EHI; violations may result in significant civil penalties as discussed below.

Application to Healthcare Providers. The Rule applies to healthcare providers, health IT developers of certified health IT,[1] health information exchanges, and health information networks (collectively referred to as "actors"). "Healthcare provider" is defined to include nearly any entity rendering healthcare, including physicians, practitioners, group practices, hospitals, long term care facilities, clinics, ambulatory surgery centers, and other entities determined appropriate by HHS.[2]

Prohibited Information Blocking. The Rule generally prohibits "information blocking," *i.e.*, a practice that the healthcare provider "knows[3]…. is unreasonable and is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information"[4] **unless** (i) the practice is required by law, or (ii) the practice fits within one of the exceptions listed below. (45 C.F.R. § 171.103(a)). Information blocking may occur, for example, when a healthcare provider refuses, ignores, delays, or imposes unreasonable conditions in response to requests to access or share EHI, including requests from patients, other providers, or payors. (*See* 85 FR 25811). It may occur when contracts, business associate agreements, license terms, or organizational policies unnecessarily restrict data sharing, or when technology is implemented, configured, or disabled so as to limit system interoperability. (85 FR 82511-12). The Rule generally prohibits any practices that increase the cost, complexity or burdens associated with accessing, exchanging or using EHI, or that limit the utility, efficacy or value of EHI such as diminishing the integrity, quality, completeness, or timeliness of the data. (85 FR 25809). Ultimately, "[a]ny analysis of whether an actor's practices constitute information blocking will depend on the particular facts and circumstances of the case," including whether the action rises to the level of an impermissible interference, whether the actor acted with the requisite intent, and whether the actor had control over the EHI or interoperability elements necessary to access, exchange or use the EHI in question. (85 FR 25811 and 25820).[5]

Permissible Information Blocking. The Rule does not prohibit

information blocking in the following circumstances:

1. The practice is required by law, including federal or state statutes, regulations, court orders, administrative decisions, *etc*. For example, healthcare providers may not share or allow access to EHI in a manner that violates HIPAA or similar state privacy laws. To trigger this defense to information blocking, however, the law must require the relevant conduct; actions that are taken pursuant to, but are not actually required by, applicable laws will not necessarily be protected. (85 FR 25794). As explained by HHS

> we do not require the disclosure of EHI in any way that would not … be permitted under the HIPAA Privacy Rule (or other Federal or State law). However, if an actor is permitted to provide access, exchange, or use of EHI under the HIPAA Privacy Rule (or any other law), then the information blocking provision would require that the actor provide that access, exchange or use of EHI so long as the actor is not prohibited by the law from doing so (assuming that no exception is available to the actor).

(85 FR 25812).

2. The healthcare provider did not know that the practice was "unreasonable and is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information." This knowledge/intent element will be an important defense for healthcare providers. The OIG has confirmed that it "will not bring enforcement actions against actors who OIG determined made innocent mistakes (*i.e.*, lack the requisite intent for information blocking)." (85 FR 22984).

3. The provider fits within a regulatory exception. The Rule includes eight exceptions — practices that HHS has determined to be reasonable and necessary even though they may interfere with information sharing. These exceptions function as safe harbors: so long as the healthcare provider's practice satisfies all of the specific, often technical elements of the relevant exception, the practice will not constitute prohibited information blocking. Failure to satisfy an exception does not necessarily mean that the provider has engaged in information blocking; instead, the provider's compliance would depend on the facts of the situation. (85 FR 25820). Five of the exceptions apply to the failure or refusal to fulfill requests to access, exchange or use EHI; three of the exceptions apply to situations in which the actor's conditions on access, exchange or use may interfere with data sharing.

> **(a) Preventing harm.** A healthcare provider may block EHI if he or she has a reasonable belief that the practice will substantially reduce a risk of harm to a patient or other person, *e.g.*, to avoid the risk that corrupt or inaccurate data will be incorporated in the patient's electronic health record, or upon a determination by a licensed healthcare professional that disclosure is likely to endanger life or physical safety of the patient or others. (*See* 84 FR 7524). The regulation has specific criteria that must be satisfied when evaluating the reasonableness of the practice and the risk of harm. (45 C.F.R. §

171.201; *see* 85 FR 25821-44).

(b) Protecting the patient's privacy. A healthcare provider may block EHI if (i) state or federal privacy laws impose preconditions to access that have not been satisfied; (ii) HIPAA allows the provider to deny access to the individual; or (iii) the patient has requested that her/his information not be shared. In each of these situations, the provider must satisfy additional regulatory conditions. (45 C.F.R. § 171.202; *see* 85 FR 25844-25859).

(c) Protecting the security of the EHI. A healthcare provider may block EHI if necessary to safeguard the confidentiality, integrity and availability of the EHI consistent with (i) its organizational security policies or (ii) a specific determination that there are no reasonable, less obstructive alternatives to secure the EHI. (45 C.F.R. § 171.203; *see* 85 FR 25859-65).

(d) Access is infeasible. A healthcare provider may block access to EHI if (i) extraordinary circumstances beyond its control prevent the provider from fulfilling the request; (ii) the provider cannot segregate the requested EHI from other information that is not subject to access; or (iii) the provider demonstrates that responding to the request is not feasible due to, *e.g.*, the type of information, cost, available resources, control of the relevant platform, *etc*. Within ten (10) days of the request, the provider must notify the requestor in writing of the reason for failing to provide the access requested. (45 C.F.R. § 171.204; *see* 85 FR 25865-70).

(e) Maintenance and improvement. A healthcare provider may temporarily block access to EHI if necessary for maintenance and improvement of the health IT. (45 C.F.R. § 171.205; *see* 85 FR 25870-75).

(f) Content and manner. A healthcare provider must generally provide access to the EHI content in the manner requested unless the provider is technically unable to fulfill the request or cannot reach agreeable terms with the requestor to fulfill the terms; however, the limits on fees or licenses described below do not apply. If the provider cannot grant access as requested or agreed, the provider must take reasonable steps to fulfill the request in an alternative manner consistent with specified technical standards. (45 C.F.R. § 171.301; *see* 85 FR 25875-79).

(g) Fees. A healthcare provider may charge reasonable fees for accessing, exchanging or using EHI so long as they are based on the provider's costs and applied in a non-discriminatory manner as more fully described in the regulations. (45 C.F.R. § 171.302; *see* 85 FR 25879-88).

(h) Licensing. A healthcare provider may license interoperability elements so long as the provider begins licensing negotiations within ten days from the request and the license satisfies specified regulatory standards. Among other things, any royalty must be

reasonable, and the license terms must be non-discriminatory. (45 C.F.R. § 171.303; *see* 85 FR 25888-97).

Penalties. On April 24, 2020, the Office of Inspector General ("OIG") published a proposed rule that would allow the OIG to impose a fine of up to $1,000,000 for information blocking. (85 FR 22979; proposed 42 C.F.R. § 1003.1410). Under the proposed rule, the OIG would consider the following factors in determining the amount of the penalty: (i) the nature and extent of the information blocking; (ii) the resulting harm, including (a) the number of patients affected, (b) the number of providers affected, and (c) the number of days the information blocking persisted. (85 FR 22991; proposed 42 C.F.R. § 1003.1420). In the meantime, persons wishing to submit an information blocking complaint may do so through the HealthIT.gov website at https://www.healthit.gov/topic/information-blocking.

What You Must Do. April 5 is just around the corner. Providers and other actors should begin not to prepare for and implement the new rule by doing the following:

- **Take advantage of the new rule.** Providers should determine how the new Rule may benefit them by allowing them to obtain access to previously unavailable patient information. They should identify the information they may need to provide care more effectively and compete more efficiently. Savvy providers may differentiate themselves by being able to collect and utilize the improved flow of information for the benefit of their patients.
- **Identify and educate stakeholders.** The new Rule may affect many departments within a healthcare organization, including information technology, medical records, marketing, compliance, contracting, and more. Providers should identify and educate those persons and departments that will be responsible for making and responding to requests.
- **Review EHI practices.** Providers will need to review and update their policies and practices concerning requests for access by patients and third parties to avoid any information blocking issues. Among other things, they should ensure that their policies and practices do not inappropriately delay or impose unreasonable restrictions or roadblocks to information sharing. They should also establish processes for evaluating and responding to requests to access information and appropriate costs or limitations associated with such access. They should identify system capabilities as well as limitations that may justify a denial of a request to share information.
- **Review EHI system functionality.** Providers should review the functionality of their EHI platforms to ensure that that have not configured or disabled functionality in a way that would constitute information blocking. If necessary, they may need to enable previously unused functionality.
- **Review contracts for offending terms.** Providers should review their contracts relevant to EHI to ensure that they do not contain terms that would trigger the information blocking rule, including

licensing agreements, software services, business associate agreements, and other EHI contracts. Providers may need to educate and push back vendors who include terms that would prohibit information sharing.

- **Respond appropriately to requests for information sharing.** When a request to access is made, providers should ensure that the request is directed to the right person—a person who understands the Rule and the EHI system's functionality—to determine whether and in what manner the Rule would apply, then ensure that a timely and appropriate response is made.
- **Watch for more guidance.** We anticipate additional guidance as well as the final enforcement rule. Providers should continue to monitor industry association bulletins and other sources for developments concerning the Rule.

[1]Significantly, "health IT developers" do not include healthcare providers that self-develop health IT for their own use. (45 C.F.R. § 171.102, definition of health IT developer of certified health IT).
[2]"The term 'healthcare provider' includes a hospital, skilled nursing facility, nursing facility, home health entity or other long term care facility, healthcare clinic, community mental health center … , renal dialysis facility, blood center, ambulatory surgical center …, emergency medical services provider, Federally qualified health center, group practice, a pharmacist, a pharmacy, a laboratory, a physician [including MDs, DOs, dentists, podiatrists, optometrists, and chiropractors], a practitioner [including physician assistants, nurse practitioners, clinical nurse specialists, certified registered nurse anesthetists, certified nurse midwives, clinical social workers, clinical psychologists, and registered dieticians], tribal organization, a rural health clinic, … an ambulatory surgical center, … a therapist and any other category of healthcare facility, entity, practitioner, or clinician determined appropriate by the Secretary." (42 U.S.C. § 300jj; 45 C.F.R. § 171.102).
[3]For health IT developers, health information networks or health information exchanges, information blocking occurs if "such developer, network or exchange knows, **or should know**, that such practice is likely to interfere with, prevent, or materially discourage access, exchange, or use of electronic health information." (45 C.F.R. § 171.103(a)(2), emphasis added).
[4]"Electronic health information" ("EHI") generally means electronic protected health information to the extent that it would be part of a designated record set as defined in HIPAA, excluding (i) psychotherapy notes, and (ii) information compiled in reasonable anticipation of or for use in litigation. (45 C.F.R. § 171.102). EHI would not include information that is not individually identifiable or has otherwise been de-identified. (85 FR 25804). During the phase in period until May 2, 2022, EHI only includes the specific data elements represented in the USCDI standard adopted in § 170.213." (45 C.F.R. § 171.103(b)).
[5]The HHS commentary to the proposed and final Rule contain helpful examples of prohibited information blocking. (*See, e.g.*, 84 FR 7518-21 and 85 FR 25811-18).