von Briesen
von Briesen & Roper, s.c. | Attorneys at Law

New Information Blocking Rules: Will You Be Ready?

Nov 03 2020

Practice Area: Health Law & Health Information Privacy and Security

Healthcare providers are subject to a vast array of privacy laws but, until recently, still had discretion in fulfilling requests for information. Now, new rules governing "information blocking" will curtail this discretion and impose new compliance risks in fulfilling requests for healthcare information. "Information blocking" is the prohibited practice of interfering with access, exchange, or use of electronic health information ("EHI"). This *Legal Update* will outline (1) who must comply with the new rules, (2) the basic requirements of the new information blocking rules, (3) the relevant exceptions to these requirements, and (4) practical considerations for health care providers seeking to comply with the new rules by the compliance date in April 2021.

1. Who Must Comply with the New Rules?
The new rules apply to "actors" which include health care providers, health IT developers, and health information networks or exchanges.[1] This *Legal Update* will focus on the requirements as applied to health care providers. The new rules define "health care provider" broadly to include most provider types such as hospitals, nursing homes, and practitioners.[2] The final rule indicates the definition could be expanded to include additional provider types in the future "if the scope of health care providers subject to the information blocking provision does not appear to be broad enough in practice to ensure that the information blocking provision applies to all health care providers that might engage in information blocking."[3]

2. What is Information Blocking?
Generally, information blocking is any act or omission that a healthcare provider knows is unreasonable and likely to interfere with, prevent, or materially discourage access, exchange, or use of EHI.[4] The proposed rule offered some helpful examples of what might constitute information blocking. For example, a provider might impermissibly block information where it has capabilities to release information on the same day a request is made, but yet delays release of information for several days.[5] In another example, a provider might impermissibly block information if it refuses to release information to an unaffiliated provider for treatment purposes without the individual's written consent.[6]

This otherwise broad prohibition is limited in a few respects. First, a healthcare provider has not impermissibly blocked information if it lacked the requisite intent element (knowledge) that the act or omission was likely to interfere, prevent, or discourage access to EHI. Second, the prohibition only applies to blocking of EHI. Ultimately, EHI includes any PHI that would be included in a designated record set regardless of whether such records are used or maintained by or for a covered entity.[7] Third, the final rule promulgated a number of regulatory exceptions which define practices that explicitly fall outside of the scope of data blocking, as described below. Finally, the final rule also provides that failure to meet the conditions of an exception does not automatically mean a practice constitutes information blocking. Instead, a practice failing to meet all conditions of an exception will be evaluated on a case by case basis to determine if blocking occurred.

3. What are the Exceptions?

The final rule provided eight exceptions which do not constitute data blocking. The exceptions are grouped into two categories: exceptions that involve not fulfilling requests and exceptions that involve procedures for fulfilling requests. Below is a list and brief summary of each of the exceptions.[8] Note that each exception has a number of technical regulatory conditions which must be met for a practice to meet the exception and fall outside the definition of data blocking.[9]

- Situations where a denial of a request is not considered information blocking: The regulatory exceptions provide that an actor's denial of a request is not information blocking when an actor:
    - Preventing Harm: Engages in practices that are reasonable and necessary to prevent harm to a patient or another person.
    - Privacy: Does not fulfill a request to access, exchange, or use EHI in order to protect an individual's privacy.
    - Security: Interferes with the access, exchange, or use of EHI in order to protect the security of EHI.
    - Infeasibility: Does not fulfill a request to access, exchange, or use EHI due to the infeasibility of the request.
    - Health IT Performance: Takes reasonable and necessary measures to make health IT temporarily unavailable or to degrade the health IT's performance for the benefit of the overall performance of the health IT.

- Exceptions that Involve Procedures for Fulfilling Requests. The regulatory exceptions provide an actor's failure to fulfill requests is not information blocking when an actor:
    - Content and Manner: Limits the content of its response to a request for access, exchange, or use EHI or the manner in which it fulfills a request to access, exchange, or use EHI.
    - Fees: Charges fees, including fees that result in a reasonable profit margin, for accessing, exchanging, or using EHI.
    - Licensing: Licenses interoperability elements for EHI to be accessed, exchanged, or used.

4. Practical Considerations.

In response to these new rules, every health care provider should (1) analyze which rules apply specifically to them, (2) review current practices for compliance, and (3) update policies and implement additional training relevant staff.

- Analyze What Rules Apply. Determine if you fall within the regulatory definition of a certain type of "actor" to which the rules apply. The administrative remedies vary by which rules apply and could inform your organization's risk tolerance in implementing new procedures to comply with these rules.
- Review Current Practices. Conduct a thorough review of current practices to understand whether any might constitute data blocking. If a current practice could constitute data blocking, consider whether the practice can fit within an exception or might be modified to some extent to fit within an exception. This review should include all privacy and security policies and procedures implicated by patients or other providers' requests for EHI.
- Update Policies and Implement Training. If any policies or practices might constitute data blocking and do not fall squarely within an exception, update policies to meet the conditions of an applicable exception. Provide updated training to relevant staff who may receive or process requests for information.

---

[1] 45 CFR §§ 171.101, 171.102. Health IT developer of certified health IT means an individual or entity, other than a health care provider that self-develops health IT for its own use, that develops or offers health information technology and which has one or more Health IT Modules certified under a program for the voluntary certification of health information technology that is kept or recognized by the ONC Health IT Certification Program. Health information network or health information exchange means an individual or entity that determines, controls, or has the discretion to administer any requirement, policy, or agreement that permits, enables, or requires the use of any technology or services for access, exchange, or use of electronic health information among more than two unaffiliated individuals or entities that are enabled to exchange with each other and that is for a treatment, payment, or health care operations purpose.

[2] 45 CFR § 171.102; 42 U.S.C. § 300jj(3). Among other provider types included in the health care provider definition are home health, other long term care facilities, health care clinics, community mental health centers, renal dialysis facilities, blood centers, ambulatory surgical centers, emergency medical services providers, federally qualified health centers, group practices, pharmacists, pharmacies, laboratories, physicians, rural health clinics, therapists, and more.

[3] 85 FR 25642, 25795 (May 1, 2020).

[4] 42 U.S. Code § 300jj–52(a)(1)(B)(2); 45 CFR § 171.103(a)(3). Note that the regulatory definition of information blocking varies slightly for other "actors" but that is beyond the scope of this *Legal Update*.

[5] 84 FR 7424, 7518 (May 3, 2019).

[6] *Id*.

[7] 45 CFR § 171.102. EHI expressly excludes psychotherapy notes or information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding. Also note, until May 2, 2022, EHI is further limited to data elements represented in the USCDI standard adopted in § 170.213. 45 CFR § 171.103(b).

[8] The list of exceptions and paraphrased rules are reproduced in part from the Office of the National Coordinator for Health Information Technology fact sheet on information blocking exceptions (https://www.healthit.gov/sites/default/files/cures/2020-03/InformationBlockingExceptions.pdf).

[9] 45 CFR Part 171, Subparts B and C.
