wiley

NEWSLETTER

Compliance Roadblocks: Tackling Information Blocking Challenges in Health Care

October 2020

Privacy in Focus®

On May 1, 2020, the U.S. Department of Health and Human Services (HHS) signaled a paradigm shift in the manner in which patient electronic health information (EHI) is accessed, used, and disclosed. Transitioning from a landscape dominated by the Health Insurance Portability and Accountability Act (HIPAA), which *permits* the disclosure of protected health information in certain circumstances (*see* 45 C.F.R. Part 164), the new information blocking rule published by HHS's Office of the National Coordinator for Health Information Technology (ONC) (the "Information Blocking Rule") *mandates* timely and expeditious disclosure of EHI unless an exception applies (*see* 45 C.F.R. Part 171). With the November 2, 2020 deadline for information blocking compliance quickly approaching, health care actors have had to revamp their compliance and operational policies to align with this new framework. As health care actors work diligently to comply with the new information blocking landscape, we provide an overview of the Information Blocking Rule's key provisions and set the stage for a more in-depth analysis of information blocking compliance challenges in the next issue of *Privacy in Focus*.

What Is Information Blocking?

Information blocking, as defined by the Public Health Service Act, refers to any practice by a health care actor that is likely to interfere with, prevent, or materially discourage access, exchange, or use of EHI. (42 U.S.C. § 300jj-52(a)). Such information blocking "practices" include (i) activities that restrict authorized access, exchange, or use of EHI for treatment and other permitted purposes, (ii) implementing health information technology (IT) in nonstandard ways that increase

Practice Areas

Health Care

Privacy, Cyber & Data Governance

the complexity or burden of accessing, exchanging, or using EHI, and (iii) implementing health IT in a manner that is likely to restrict the access, use, or exchange of EHI with respect to exporting complete information sets or lead to fraud, waste, and abuse. (*Id.* § 300jj-52(b)). Liability for engaging in these information blocking practices only attaches upon satisfaction of a knowledge standard – i.e., that a health care actor knew (in the case of health care providers) or should have known (in the case of health IT developers, exchanges, and networks) that the practice was likely to interfere with, prevent, or materially discourage the access, exchange, or use of EHI. (*Id.* § 300jj-52(a)).

Are There Exceptions to Information Blocking Practices?

While the practices that are prohibited as information blocking are broad, ONC has identified eight exceptions to the information blocking definition. These exceptions apply to certain practices that are likely to interfere with, prevent, or materially discourage the access, exchange, or use of EHI, but that are reasonable and necessary activities for health care actors to engage in, provided certain conditions are satisfied. ONC has divided the information blocking exceptions into two broad categories: (i) exceptions that involve *not fulfilling* requests to access, exchange, or use EHI, and (ii) exceptions that allow health care actors to follow certain *procedures* that would otherwise be deemed information blocking when fulfilling requests to access, exchange, or use EHI.

The first category (i.e., exceptions that allow a health care actor not to fulfill a request for EHI) incorporates the preventing harm exception, privacy exception, security exception, infeasibility exception, and health IT performance exception. Pursuant to the preventing harm exception (45 C.F.R. § 171.201), a health care actor may engage in practices that are reasonable and necessary to prevent harm to a patient or another person even if such practices delay or restrict access to EHI. Similarly, the privacy exception (*id.* § 171.202) and security exception (*id.* § 171.203) permit a health care actor to refuse a request to access, exchange, or use EHI if doing so will protect an individual's privacy or the security of EHI, respectively. The infeasibility exception (*id.* § 171.204), as its name suggests, allows a health care actor to withhold EHI if its release is otherwise infeasible. Finally, the health IT performance exception (*id.* § 171.205) enables health care actors to take reasonable and necessary measures to make health IT temporarily unavailable or to degrade the health IT's performance if it will benefit the overall performance of the health IT. For each exception described above, specific conditions, or elements, must be satisfied for the exception to apply.

The second category (i.e., exceptions that allow a health care actor to engage in procedures that may delay access to EHI) contains the licensing exception, fees exception, and content and manner exception. The licensing exception enables a health care actor to license interoperability elements for EHI, even if doing so delays access to EHI. (*Id.* § 171.303). The fees exception, in turn, permits a health care actor to charge fees for the access, exchange, or use of EHI, including fees that create a reasonable profit margin. (*Id.* § 171.302). Finally, the content and manner exception limits the content that must be included in a health care actor's response to a request to access, exchange, or use EHI, and offers flexibility in the manner in which a health care actor fulfills such a request. (*Id.* § 171.301). Similar to the first category of exceptions, these exceptions require satisfaction of specific conditions prior to their use.

Assuming a health care actor fulfills all conditions of an enumerated exception, the otherwise prohibited practice no longer constitutes information blocking as a matter of law. This means the practice has guaranteed protection from civil monetary penalties or other disincentives. (85 Fed. Reg. 25642, 25649 (May 1, 2020)). A prohibited information blocking practice that satisfies *some*, but not all elements of an exception is not afforded this protection and such practices would be evaluated on a case-by-case basis to determine whether information blocking has in fact occurred (including an analysis of the health care actor's intent). (*Id.*).

When Must Health Care Actors Comply with the Information Blocking Rule?

ONC delayed the original compliance date for the Information Blocking Rule due to the pressures faced by health care actors from COVID-19. The current compliance deadline is November 2, 2020. (*Id.* at 25642). After this date, suspected instances of noncompliance with the Information Blocking Rule may be reported via ONC's complaint submission portal and will be investigated by HHS's Office of Inspector General (OIG). OIG may then refer noncompliant activities to relevant agencies for further investigation.

Are There Penalties for Noncompliance?

Failure to comply with the Information Blocking Rule may result in the imposition of civil monetary penalties or other disincentives. OIG must first establish these civil monetary penalties pursuant to a rulemaking. For health IT developers, exchanges, and networks, OIG published a proposed rule on April 24, 2020 to create new civil monetary penalty authorities for information blocking. (*See* 85 Fed. Reg. 22979 (Apr. 24, 2020)). This proposed rule does not, however, apply to health care providers (though health care providers must still comply with existing attestation requirements with respect to electronic health records technology). (*Id.* at 22981). ONC has indicated that it will exercise discretion such that conduct which occurs before the new civil monetary penalty rules are finalized will not be subject to information blocking civil monetary penalties. (85 Fed. Reg. at 25841).

What Compliance Challenges Are Health Care Actors Facing?

Health care actors are facing numerous challenges and compliance roadblocks when working to implement the expedited flow of information required by ONC's Information Blocking Rule. Full compliance with the ONC information blocking rule will require health care actors to engage in significant policy and procedure changes, an in-depth analysis of contractual arrangements and Business Associate Agreements, and new compliance training for staff. In addition, health care actors are having to grapple with legacy electronic health record systems, the scope of EHI to be released, and scanned records from other health care entities. We tackle these compliance challenges in next month's issue of *Privacy In Focus*.