COSMOS
Navigate the Compliance Universe

Complete Healthcare Compliance Manual 2024
Health Information Management: Patient Access, Information Blocking, and the 21st Century Cures Act

By Patricia A. Markus,[1] JD, CIPP/US

What Are the Patient Access and Information Blocking Requirements of the 21st Century Cures Act?

Since 2003, under the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, individuals have had the right to access and obtain a copy of their own protected health information (PHI) from a healthcare provider or a provider's business associate, subject to a few narrow exceptions.[2] However, due to a misunderstanding of HIPAA requirements and, in some cases, a desire to protect against competition, providers over the last few years have repeatedly been fined by federal regulators for Privacy Rule infractions. These include failing to provide access to PHI in a timely manner; denying access when access is permitted; failing to provide access in the format requested; failing to provide access to individuals' personal representatives as required by HIPAA; and charging excessive fees for copies of medical records.[3]

More recently, regulations under the 21st Century Cures Act (Cures Act), which prohibit healthcare providers from engaging in "information blocking," have complicated whether and how providers give access to individuals' electronic health information (EHI).[4] The final rule addresses interoperability, information blocking, and the Office of the National Coordinator for Health Information Technology (ONC) Health IT Certification Program under the Cures Act. The final rule was published in the *Federal Register* on May 1, 2020, and, following a six-month implementation delay due to COVID-19, became effective on April 5, 2021.[5] The information blocking provisions of the Cures Act responded to concerns about healthcare industry practices that were unreasonably limiting the availability and use of EHI for permitted purposes, including use by individuals and other appropriate persons within the healthcare ecosystem.[6] These industry practices include contract terms, policies, or processes that interfered with individuals' rights to access their own PHI for permitted purposes under HIPAA; fees that made the access, exchange, or use of PHI cost prohibitive; and nonstandard implementation of health information technology that substantially increased the cost, complexity, and burden of sharing health data.

A significant emphasis in the Cures Act's Information Blocking Rule is ensuring the rights of individuals and their personal representatives to access their PHI without unnecessary delay, without special effort on the individuals' part, and at a minimal cost or, in certain circumstances, no cost. This protection of individuals' right of access expands upon the right originally set forth in the HIPAA Privacy Rule and furthered by the Health Information Technology for Economic and Clinical Health Act (HITECH). The Information Blocking (IB) Rule builds upon this right of access; it prohibits charging individuals, their personal representatives, or another person or designated entity for providing "electronic access" to the individual's EHI.

Compliance with the IB Rule requires a paradigm shift in the way healthcare industry stakeholders and compliance officials think about when and how to make EHI available to third parties. For 19 years, the healthcare industry worked with the HIPAA Privacy Rule, which specifies when PHI **may** be used and disclosed.

The IB Rule, on the other hand, **requires** healthcare providers and others governed by the rule to make EHI available for access, use, or disclosure when appropriate to do so and when not otherwise prohibited by law. Thus, the analysis regarding whether to use and disclose PHI in certain situations transitions from the HIPAA-based presumption that PHI **should not** be used or disclosed unless doing so is specifically permitted or required, to a presumption that EHI **must** be made available unless the access, use, or disclosure is specifically *prohibited* by law or if the circumstances surrounding the decision not to make EHI available fit within an exception to the definition of information blocking.

The IB Rule includes a significant number of defined terms that need to be understood to determine what conduct may be problematic and what conduct may fall within one of its eight exceptions. Before the enforcement mechanisms for the IB Rule are finalized, compliance officers need to understand the requirements of the IB Rule and the limitations of its exceptions. Simultaneously, compliance officers must watch for guidance to be issued by the ONC and other agencies within the U.S. Department of Health and Human Services (HHS) that address how to comply with different aspects of the rule and its exceptions.

Risk Area Governance

The IB Rule generally prohibits "actors" from engaging in "information blocking." Its definition of "actor" includes a healthcare provider, a developer of certified health IT, and a health information network or a health information exchange (HIE). (Health information *networks* and health information *exchanges* are collectively referred to as HIEs).[7] **The term "information blocking" is defined, in part, as a practice that, except as required by law or covered by an exception set forth in the IB Rule, "is likely to interfere with access, exchange, or use of electronic health information."**[8] "Interfere with" means to prevent, materially discourage, or otherwise inhibit.[9] A "practice" is defined as "an act or omission by an actor."[10]

The IB Rule is an intent-based statute. This means that an actor engages in information blocking only if the actor (while engaging in a practice that is likely to interfere with access, exchange, or use of EHI) has the level of intent specified in the IB Rule. *Healthcare providers* engage in information blocking only if they know that the practice is unreasonable and is likely to interfere with the access, exchange, or use of EHI.[11] *Health IT developers and HIEs* engage in information blocking only if they know or should know that a practice is likely to interfere with the access, exchange, or use of EHI.[12]

EHI was not defined in the Cures Act or the other statutes to which it refers,[13] so a definition of EHI was included in the IB Rule.[14] The definition of EHI is a subset of electronic protected health information (ePHI) as defined in the HIPAA Privacy Rule,[15] in that EHI is limited to ePHI that would be included in a designated record set (DRS), whether or not the actor is a HIPAA-covered entity.[16] The Privacy Rule defines a designated record set as follows:

1. A group of records maintained by or for a **covered entity** that involve:
    i. Medical and billing records about individuals and maintained by or for a covered healthcare provider;
    ii. Enrollment, payment, claims adjudication, and case or medical management record systems that are maintained by or for a health plan or are used, in whole or in part, by or for the covered entity to make decisions about individuals.
2. The term "record" here means any item, collection, or grouping of information that includes protected

health information and is maintained, collected, used, or disseminated by or for a **covered entity**.[17]

The definition of EHI specifically *excludes* psychotherapy notes and information compiled in anticipation of or for use in a civil, criminal, or administrative action or proceeding.[18]

The ONC did not limit the scope of EHI to records that are used or maintained by or for covered entities: "actors" who are regulated by the IB Rule include noncovered entities such as HIEs, certified health IT developers, and healthcare providers who do not take insurance. This, in turn, means that what constitutes EHI is much broader than the definition of ePHI under HIPAA: EHI may encompass medical and billing records, health plan records, and other records used to make decisions about individuals when such records are maintained by developers of certified health IT, HIEs, and healthcare providers that are not covered entities.