Information blocking rule establishes new data sharing principles for health care industry

Takeaways

- Disclosures of electronic health information (EHI) permitted by HIPAA and state law are now required (unless an exception applies) under new rule
- Providers and certain health IT companies must strategically evaluate how to protect IP interests yet maintain competitively neutral EHI data sharing practices
- Enforcement framework, which includes civil money penalties, remains in flux

Who is the rightful owner of electronic health information? Who should control when, how, and with whom that information is shared? These are critical, and valuable, questions for an industry with a compound annual growth rate of data that exceeds manufacturing, financial services, and entertainment and media.

In its information blocking rule, the Office of the National Coordinator for Health Information Technology (ONC) offers a definitive response – **the patient** – and responds to concerns that some individuals and entities are engaging in practices that unreasonably limit the availability, interoperability, and use of patients' electronic health information.

Key stakeholders in the health care industry – providers and certain health IT companies and developers – are now **prohibited** from engaging in practices likely to interfere with the appropriate access, exchange, or use of patients' electronic health information.

Under the new rule, if the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or applicable state privacy laws **permit** the disclosure of electronic health information, the information blocking rule likely will **require** such disclosure. The rule does include important exceptions that offer regulated actors certainty that their practices will not be considered information blocking when meeting the conditions of one (or more) exception. Yet, leveraging these complex exceptions will require advance planning.

What is information blocking?

Information blocking is a business practice **likely to interfere with, prevent, materially discourage, or otherwise inhibit the access, exchange, or use of electronic health information** (EHI). Information blocking does not include practices that either (1) are required by law or (2) comply with an exception to the information blocking rule.

Put simply, information blocking encompasses activities that make the access, exchange, use, or interoperability of health data more difficult. The definition also encompasses an intent requirement, which is different depending on the identity of the regulated actor.

Who must comply, and what are the associated intent requirements?

The information blocking rule applies to health care providers, health information networks (HINs) and health information exchanges (HIEs), and ONC-certified health IT developers.

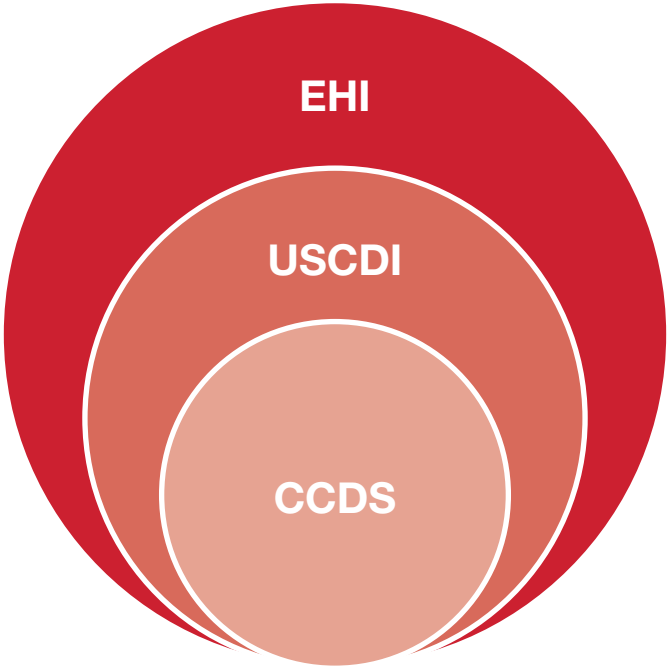
For health care providers, a practice meeting the regulatory definition will be considered information blocking if the health care provider knows such practice to be unreasonable and likely to interfere with access, exchange, or use of EHI.

For ONC-certified health IT developers, HINs, or HIEs, a practice meeting the regulatory definition will be considered information blocking if the regulated actor knows, or should know, that such practice is likely to interfere with the access, exchange, or use of EHI.

Developers must take note that if their products include any ONC-certified health IT, they must comply with the information blocking rule with respect to all of their health IT products and services – even those that are not certified.

What is electronic health information (EHI)?

The information subject to the information blocking rule will change over time as the industry prepares for full compliance.



USCDI

Until Oct. 5, 2022, EHI is limited to the data elements included in the **U.S. Core Data Interoperability (USCDI) standard**, version 1. The USCDI differs from and replaces the Common Clinical Data Set (CCDS) standard – most notably through the addition of clinical notes – that is referenced in ONC's existing certification criteria for certified health IT.

EHI

As of Oct. 6, 2022, EHI is defined as **electronic protected health information (ePHI) included in a designated record set** – in other words, ePHI to which a patient has a right of access. Although this definition draws upon key concepts and definitions from HIPAA, it applies regardless of whether HIPAA applies.


“These are critical, and valuable, questions for an industry with a compound annual growth rate of data that exceeds manufacturing, financial services, and entertainment and media.”

"The rule does include important exceptions that offer regulated actors certainty that their practices will not be considered information blocking when meeting the conditions of one (or more) exception."

What are the exceptions?

There are eight exceptions to the information blocking rule, which can be broken down into two categories: (1) exceptions that involve **not fulfilling** requests to access, exchange, or use EHI and (2) exceptions that involve procedures for **fulfilling** requests to access, exchange, or use EHI.

Exceptions that involve not fulfilling requests to access, exchange, or use EHI

1. Preventing harm exception
Engaging in reasonable and necessary practices to prevent harm to a patient (or another)

2. Privacy exception
Not fulfilling a request in order to protect an individual's privacy

3. Security exception
Interfering with the access, exchange, or use of EHI in order to protect the security of EHI

4. Infeasibility exception
Not fulfilling a request due to the infeasibility of the request

5. Health IT performance exception
Taking reasonable and necessary measures to make health IT temporarily unavailable or degrading the health IT's performance for the benefit of the overall performance of the health IT

...provided certain conditions are met

Exceptions that involve procedures for fulfilling requests to access, exchange, or use EHI

6. Content and manner exception
Limiting the content of a response to a request to access, exchange, or use EHI, or changing the manner in which the request is fulfilled

7. Fees exception
Charging fees, including fees that result in a reasonable profit margin, for accessing, exchanging, or using EHI

8. Licensing exception
Licensing interoperability elements for EHI to be accessed, exchanged, or used

...provided certain conditions are met

Must regulated actors license their intellectual property to requestors of EHI?

No, but operationalizing a compliance strategy that protects investments in health IT will require advance planning and discipline. Regulated actors cannot assert ownership rights to the EHI itself, which belongs to the patient. Furthermore, licenses to interoperability elements – proprietary data formats, processing mechanisms, and exchanges – must be offered on nondiscriminatory and competitively neutral terms. In other words, these terms must be based on objective and verifiable criteria that are uniformly applied and not related to the requestor's intended use of the EHI.

How will the information blocking rule be enforced?

Enforcement of the rule will depend on the type of regulated actor, and many of the details are yet to be finalized.

Health care providers could be subject to appropriate disincentives to be determined in future rulemaking by the Department of Health and Human Services (HHS). Additionally, the Centers for Medicare & Medicaid Services (CMS) will publicly report eligible clinicians, hospitals, and critical access hospitals that may be information blocking based on their attestation to certain Merit-based Incentive Payment System (MIPS) and Promoting Interoperability Program requirements, starting with 2019 performance year data.

Developers of certified health IT, HINs, and HIEs could be subject to civil monetary penalties (CMPs) up to $1 million per violation levied by the HHS Office of Inspector General (OIG), as well as separate enforcement by ONC related specifically to certified health IT.

OIG is scheduled to publish its final rule implementing information blocking CMPs in August 2021. Enforcement of information blocking CMPs will not begin until the CMP rule is final. Further, the OIG will exercise enforcement discretion such that conduct occurring before the CMP rule is final will not be subject to information blocking CMPs.

Deeper dive

Explore related content from Reed Smith lawyers:

Information Blocking, Interoperability, and Patient Access – How to prepare for the new rules now, 11 March through 6 May 2021 – Watch the five-part webinar series

Nancy Bonifant Halstead
Partner
Washington, D.C

Nancy Bonifant Halstead is a partner in the firm's Life Sciences Healthy Industry Group. She focuses her practice on the intersection of health care and technology, in particular on digital health compliance, privacy, and interoperability strategies.

Vicki J. Tankle
Associate
Philadelphia

Vicki J. Tankle is an associate in the firm's Life Sciences Health Industry Group. Her practice focuses on advising health industry clients on regulatory, enforcement and transactional matters, with a focus on health information, privacy, tech, and data.

Lauren M. Bentlage
Associate
Washington, D.C.

Lauren M. Bentlage is an associate in the firm's Life Sciences Health Industry Group. She advises clients in the health care industry on regulatory compliance, enforcement, and privacy issues and, more recently, has focused on the interoperability and information blocking rules.