

New ‘Information Blocking’ Compliance Obligations Take Effect April 5, 2021



April 2, 2021 | **CLIENT ALERTS**

The 21st Century Cures Act (Act) and a recently adopted final rule by the Office of the National Coordinator for Health Information Technology (ONC) in the U.S. Department of Health and Human Services will now prohibit so-called “information blocking.”

Broadly speaking, information blocking includes any practice that unreasonably limits the availability and use of electronic health information (EHI) for authorized and permitted purposes. For example, a health care provider could be engaged in information blocking if it takes several days to fulfill a patient’s request for EHI when in fact the provider could have, using reasonable efforts, fulfilled the patient’s request in a much shorter timeframe.

The final rule applies to health care providers, health information technology developers, networks and exchanges, although this alert will primarily focus on providers. The definition of “health care provider” is extremely broad and appears to include virtually every entity that furnishes health care, but notably does not mirror the definition of health care provider under HIPAA.

Due to the public health emergency, the original compliance deadline of November 2, 2020, was deferred until

April 5, 2021.

What is Information Blocking?

Information blocking is a practice by a health care provider which the health care provider knows is unreasonable and is likely to interfere with access to, exchange or use of EHI. In contrast, the standard for health information technology developers, networks and exchanges is broader, i.e., knows or should know.

The final rule, however, sets forth “exceptions” that, if satisfied, are not considered information blocking. These exceptions are discussed below and can be viewed in full in the regulations at [45 CFR 171.100](#).

Additionally, if a health care provider’s information blocking practice is required by state or federal law, then it also is not considered a violation of the rule.

Information Blocking Exceptions

The following exceptions apply and therefore do **not** constitute information blocking for purposes of this rule, as long as certain conditions are met:

- Preventing harm exception – Engaging in practices that are reasonable and necessary to prevent harm to a patient or another person.
- Privacy exception – Not fulfilling a request to access, exchange, or use EHI to protect an individual’s privacy.
- Security exception – Engaging in practices to interfere with the access, exchange, or use of EHI to protect the security of EHI.
- Infeasibility exception – Not fulfilling a request to access, exchange, or use EHI due to the infeasibility of the request.
- Health IT performance exception – Taking reasonable and necessary measures to make health IT temporarily unavailable for the benefit of the overall performance of the health IT.

In addition to the exceptions listed above, the final rule also sets forth the following three exceptions that involve procedures for fulfilling requests to access, exchange, or use EHI. As long as certain conditions are met, these do **not** constitute information blocking:

- Content and manner exception – Limiting the content of a response to a request to access, exchange, or use EHI or the manner in which a request is fulfilled.
- Fees exception – A health care provider’s practice of charging fees for accessing, exchanging, or using EHI.
- Licensing exception – A health care provider’s practice to license interoperability elements for EHI to be accessed, exchanged, or used.

Electronic Health Information

The final rule’s information blocking provisions apply to “electronic health information.” From the April 5, 2021, compliance date through October 6, 2022, EHI is limited to the information contained in the sixteen data classes for the United States Core Data for Interoperability (USCDI) standard. Those sixteen data classes include the following:

- Patient Demographics
- Vital Signs

- Allergies and Intolerances
- Medications
- Smoking Status
- Immunizations
- Procedures
- Care Team Members
- Clinical Notes
- Assessment and Plan of Treatment
- Goals
- Health Concerns
- Laboratory
- Problems
- Unique Device Identifiers (for a patient's Implantable Device)
- Provenance (i.e., the metadata of the records provided)

After October 6, 2022, however, the scope of EHI expands to include the full electronic “designated record set” within the meaning of HIPAA.

Fulfillment of a Request

Generally, a health care provider is required to fulfill a request to access, exchange or use EHI “in any manner requested.” If, however, the health care provider is technically unable to fulfill the request, the health care provider and requester can and should work on developing an alternative manner for the fulfillment of the request (such as the transmission of a secure file by e-mail).

In the extreme case where the health care provider and requestor cannot reach agreement on an alternative manner to fulfill the request, then, in that case, the health care provider would generally be required to fulfill the request for the EHI in the manner described in the final rule.

Non-Compliance Penalties

While the Act establishes a maximum civil monetary penalty of \$1,000,000 per violation for non-compliance by health information technology developers, networks and exchanges, the Act directs the Office of Inspector General (OIG) to refer health care provider non-compliance to the “appropriate agency” for the imposition of “appropriate disincentives.” Future rulemaking will define the meaning of “appropriate disincentives.” The Act directs the Secretary of Health and Human Services to ensure that health care providers are not penalized for the failure of developers of health information technology to meet applicable certification requirements.

Interaction with Other Laws

Health care providers should know that the final rule does not limit or impair other rights a patient might have under federal or state law.

Key Takeaways

- The Final Rule compliance deadline is April 5, 2021.
- Providers need to efficiently release EHI upon request in a way that is not “information blocking.”
- Providers can deny or delay fulfilling a request for EHI if required to do so by law or if one of the “exceptions” apply.

- EHI initially includes the sixteen data classes for the USCDI standard but expands after October 6, 2022, to include the entire electronic “designated record set.”
- Providers are required to fulfill a request to access, exchange or use EHI “in any manner requested.” If a provider is technically unable to fulfill the request, however, the provider and requester can and should work on developing an alternative manner for the fulfillment of the request.

Next Steps

To prepare for the final rule, health care providers should:

- Review current procedures for EHI requests and modify any practices that could be considered information blocking.
- Update current written policies to address potential information blocking issues.
- Provide training to employees who are responsible for responding to EHI requests.

Please contact either of the health law attorneys below for any questions regarding this client alert.