

Patient Access Playbook: Information blocking

What is information blocking?

The 21st Century Cures Act (Cures Act) was signed into law on Dec. 13, 2016. Included within the law are provisions related to “information blocking.”

The law outlines the four types of “Actors” for whom information blocking provisions are applicable and for whom enforcement actions apply:

- Providers
- Health information technology (health IT) developers
- Health information networks (HINs)
- Health information exchanges (HIEs)

Physicians, health IT developers of certified health IT (e.g., EHR vendors), HIEs and HINs will be subject to information blocking requirements as it relates to the sharing of electronic health information (EHI) data starting **April 5, 2021**.

Currently, only a subset of the patient’s entire electronic medical record is considered EHI. This subset is called the U.S. Core Data for Interoperability (USCDI). Many EHRs can already support most of what is outlined in the USCDI, but those that cannot are being updated to support of all data elements in the USCDI. This will take time and, for some smaller EHR vendors, may take several months. Make sure to check with your EHR vendor on their progress and ask about their efforts to help you comply with the information blocking rule. After October 6, 2022, all physicians must make all of their patients’ ePHI (not just the ePHI in the USCDI) available for access, exchange and use.

While the Cures Act specifies penalties for health IT developers, HINs and HIEs, Congress left it up to the Department of Health and Human Services (HHS) to issue regulations on “disincentives” and enforcement policies for physicians. At this time, HHS has not yet released information on physician penalties.

Information blocking practices can be an Actor’s acts or omissions—essentially anything that interferes with the access, exchange or use of EHI. However, just because an action interferes with the access, exchange or use of EHI does not mean the practice is automatically considered an information blocking violation—facts and circumstances unique to each action should be considered. For instance, physician Actors must have the required **knowledge and intent** to interfere with

access, exchange or use of EHI. Information blocking practices may include but are not limited to:

- | Limiting or restricting the interoperability of health IT;
- | Implementing health IT in ways that are likely to restrict the access, exchange or use of EHI;
- | Acts that lead to fraud, waste or abuse or impede care delivery enabled by health IT (for example, modifying EHR data reported to federal payment programs such as MIPS) and
- | Having the capability to provide same-day access to EHI in a form and format requested by a patient or a patient’s health care provider but taking several days to respond.

Physicians may implicate the information blocking rule if they knowingly take actions that interfere with exchange, access and use of EHI, even if no harm materializes.

For nearly all EHI requests, physicians must respond and release patients’ medical records unless an appropriate exception can be identified and used. ONC has identified in regulation “reasonable and necessary” activities that are not information blocking (i.e., information blocking exceptions). For instance, medical practices may need to restrict access to patient records in their EHR due to data privacy or security reasons—such as when a patient’s consent is required but not documented or in instances of cybersecurity threats. Individuals or other entities may also request medical records from a physician’s office in a manner not supported by their EHR—such as requesting documents over application programming interfaces (APIs) when APIs are not supported by the practice’s EHR. There are eight information blocking exceptions (PDF), spanning across two categories:

- | Not fulfilling requests to access, exchange or use EHI
 - | Preventing harm exception
 - | Privacy exception
 - | Security exception
 - | Infeasibility exception
 - | Health IT performance exception
- | Procedures for fulfilling requests to access, exchange or use EHI
 - | Content and manner exception
 - | Fees exception
 - | Licensing exception

ONC makes clear that an Actor’s failure to meet an exception does not automatically mean that the Actor has engaged in information blocking. Just because there is no relevant exception or a physician fails to meet all requirements of an applicable exception, does not mean that the physician will necessarily be found to have engaged in information blocking. The federal body tasked with enforcement and investigations—the Office of the Inspector General (OIG)—must still determine that the action taken by the physician meets the definition of information blocking.

Where to start?

Physicians should start by identifying whether their organization already has a compliance program, even if it has not yet begun to work on information blocking compliance. This is important because your existing compliance program will have structure, policies, procedures and resources that will lay the foundation for information blocking compliance. Info blocking regulations and requirements are new for everyone; do not be surprised if your organization's compliance professionals are not knowledgeable about the information blocking rule. If your organization does not have a compliance program, then it is important to stand one up—both for information blocking compliance and for compliance with laws like HIPAA.

You should consider starting with your organization's policies that currently address requests for access, exchange, or use of patient medical information. This is particularly important for situations where patients or their non-clinical caregivers are requesting electronic information. Medical practices are urged to review all policies related to their responses to information requests and update their policies and procedures as needed. This should include both HIPAA policies and those governing confidential or sensitive patient information, including information related to adolescent health. Your policies must address each of the information blocking exceptions prior to the exception's use. You should detail how each exception can be met to ensure that the exception is applied as narrowly as possible and in a non-discriminatory manner.

The AMA has created a two-part educational resource to help physicians and their medical practices understand the requirements and develop an information blocking compliance program. Part 1 outlines what information blocking is, key terms to know, examples of information blocking practices and a summary of exceptions for when physicians may restrict access, exchange and use of EHI. Part 2 helps physicians start down the path of compliance, including questions to consider, considerations for maintaining a compliance program and next steps. AMA is also offering an online Continuing Medical Education resource to help physicians learn while receiving CME credit. Additional information can be found at infoblockingcenter.org.

The AMA also provides a toolkit on sharing clinical notes with patients (PDF).

Download the playbook

The Patient Access Playbook (PDF) focuses on dispelling HIPAA myths and helping physicians understand their obligations to provide patients with access to their health information.