Information Blocking Reminders Related to API Technology

October 2024

How do Conditions and Maintenance of Certification requirements help to prevent and address information blocking and other impediments to information sharing?

Developers participating in the ONC Health IT Certification Program have both initial and ongoing obligations as part of their compliance with the Conditions and Maintenance of Certification requirements. One of those is the Information Blocking Condition of Certification, which states that a health IT developer may not take any actions that constitute "information blocking" as defined in § 171.103. There are no accompanying Maintenance of Certification requirements beyond compliance with the Condition. The Certification Companion Guide for the § 170.401 Information Blocking Condition of Certification requirement provides additional information specific to this Certification Program requirement.

Health IT developers of certified health IT must also comply with the § 170.402 Assurances Condition and Maintenance of Certification requirements. One of the Assurances Condition of Certification requirements is that a developer must provide assurances that the developer will not take any action that constitutes information blocking, or any other action that may inhibit the appropriate exchange, access, and use of electronic health information (EHI).

As part of the Assurances Condition of Certification, a developer must also not take any action that could interfere with a user's ability to access or use certified capabilities for any purpose within the full scope of the technology's certification.

Among other Conditions and Maintenance of Certification requirements, to achieve and maintain certification of its products, a Health IT developer of certified health IT:

- Must not engage in information blocking (as defined in 45 CFR 171.103); and
- Must not take any other action that may inhibit the appropriate access, exchange, and use of electronic health information (EHI); and
- Must not take any action that could interfere with a user's ability to access or use certified capabilities.

What API-related practices can implicate the information blocking definition?

Any practice likely to interfere with access, exchange, or use of EHI can implicate the information blocking definition.

Through rulemaking and the publication of additional educational resources, ASTP has provided examples of API-related practices that could implicate the information blocking definition (45 CFR 171.103) to illustrate and help actors and other interested parties understand foundational concepts. This fact sheet assembles a non-exhaustive selection of examples, such as:

Limiting or Restricting the Interoperability of Health IT

- Any action by a Certified API Developer to withhold or restrict the public availability of service base URLs that can be used by patients to access their EHI (85 FR 25813).
- API Information Sources (such as health care providers) who locally manage their FHIR servers without Certified API Developer assistance refusing to provide to Certified API Developers the FHIR service base URL(s) that is/are necessary for patients to use to access their EHI (85 FR 25813).
- A health system with locally hosted EHR technology certified to § 170.315(g)(10) choosing not to automatically publish its service base URLs, and instead only providing them to specifically approved apps (84 FR 7518).

> Anyone can monitor the public availability of service base URLs. To ensure service base URL lists continue to be available and accessible to the public, ASTP has made two monitoring tools available: Lantern and the CHPL Service Base URL List Uptime report. For additional information on these tools, see our blog post.

- A health care provider choosing not to enable the capability for patients to directly transmit or request for direct transmission of their EHI to a third party, when their EHR developer's patient portal offers this capability (84 FR 7519).
- A health care provider has 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 takes several days to respond (84 FR 7519). We also noted that it would likely be an interference where a delay occurs in providing a patient's EHI via an API to an app that the patient has authorized to receive their EHI (IB.FAQ22.1.2021MAR).
- A health care provider imposing pre-conditions on the access, exchange, and use of EHI that are not required by the HIPAA Privacy Rule or the law of any jurisdiction in which they operate – such as demanding HIPAA Business Associate Agreements (BAAs) when HIPAA would not require them.

Impeding Innovations and Advancements in Access, Exchange, or Use or Health IT-Enabled Care Delivery

- A developer of certified health IT refusing to license or grant the rights necessary to distribute applications that use an API's interoperability elements, or refusing to provide the services that are necessary to enable such applications to be used in production environments (84 FR 7519).
- A Certified API Developer refusing to register and enable an application for production use within five business days of completing its verification of an API User's authenticity (45 CFR 170.404(b)(1)(ii)).
- A developer of certified health IT that requires third-party applications to be "vetted" for security before allowing patients to use such applications to receive EHI via technology certified to § 170.315(g)(10) (IB.FAQ51.1.2023MAY).
- A developer of certified health IT charging app developers a substantial fee to list their app on the developer's platform unless the app developer agrees not to deploy the app in any other EHR developers' "app stores." (84 FR 7520).

Burdensome or Discouraging Terms, Delays, or Exercising Influence Over Customers and Users

- A developer of certified health IT who maintains an "app store" requiring through its terms and conditions a "competing" app to grant the developer the right to use the app's source code (84 FR 7520, 84 FR 7519).
- A delay in providing a patient's EHI via an API to an app that the patient has authorized to receive their EHI (IB.FAQ22.1.2021MAR).
- As a condition of disclosing interoperability elements to third-party developers, an EHR developer requiring third-party developers to enter into business associate agreements with all of the EHR developer's covered entity customers, even if the work being done is not for the benefit of the covered entities (84 FR 7520; see also HIPAA FAQ).
- An actor's refusal to register a software application that enables a patient to access their EHI would effectively prevent its use given that registration is a technical prerequisite for software applications to be able to connect to certified API technology. As a result, such refusals in the context of patient access unless otherwise addressed in this rule would be highly suspect and likely to implicate information blocking. We note, however, for the first and second example that neither app registration nor the public availability of a FHIR service base URL means that an application will be able to access any EHI. On the contrary, the application would be unable to do so unless a patient authenticates themselves via an appropriate workflow or, in the case of a health care provider, the application is appropriately configured to work within the provider's IT infrastructure. (85 FR 25813)

It is important to remember that Certified API Developers can implicate the information blocking condition (45 CFR 170.401) in addition to the information blocking definition (45 CFR 171.103) through non-conformity with other Certification Program requirements.

Where can developers of certified health IT learn more about what constitutes information blocking?

The Information Blocking Condition of Certification requirement (§ 170.401) references information blocking as defined in statute (42 U.S.C. 300jj–52) and regulations (§ 171.103). ASTP has published resources relevant to all actors subject to the information blocking regulations and others interested in information sharing. These resources include fact sheets, webinars, frequently asked questions, and more, accessible at www.healthit.gov/informationblocking.

Who can report possible information blocking to HHS, and how might they do that?

Anyone who believes they may have experienced or observed information blocking by any actor is encouraged to share their concerns with us through the Information Blocking Portal on ASTP's website, HealthIT.gov.

By law, information received by ASTP in connection with a claim or suggestion of possible information blocking that could identify who submitted the claim is exempt from mandatory disclosure under the Freedom of Information Act.

ASTP has authority to review claims of potential information blocking against health IT developers of certified health IT that may constitute a non-conformity under the ONC Health IT Certification Program. Separately, the HHS Office of the Inspector General (OIG) has authority to investigate claims of potential information blocking across all types of actors: health care providers, health information networks and health information exchanges, and health IT developers of certified health IT. Therefore, ASTP shares every claim of potential information blocking with OIG. ASTP does not assess the merits of any claim before sharing it with OIG.

Information blocking reporting resources:

- Fact Sheet: Information Blocking Portal Process
- FAQs on Reporting Claims of Information Blocking
- View data about claims