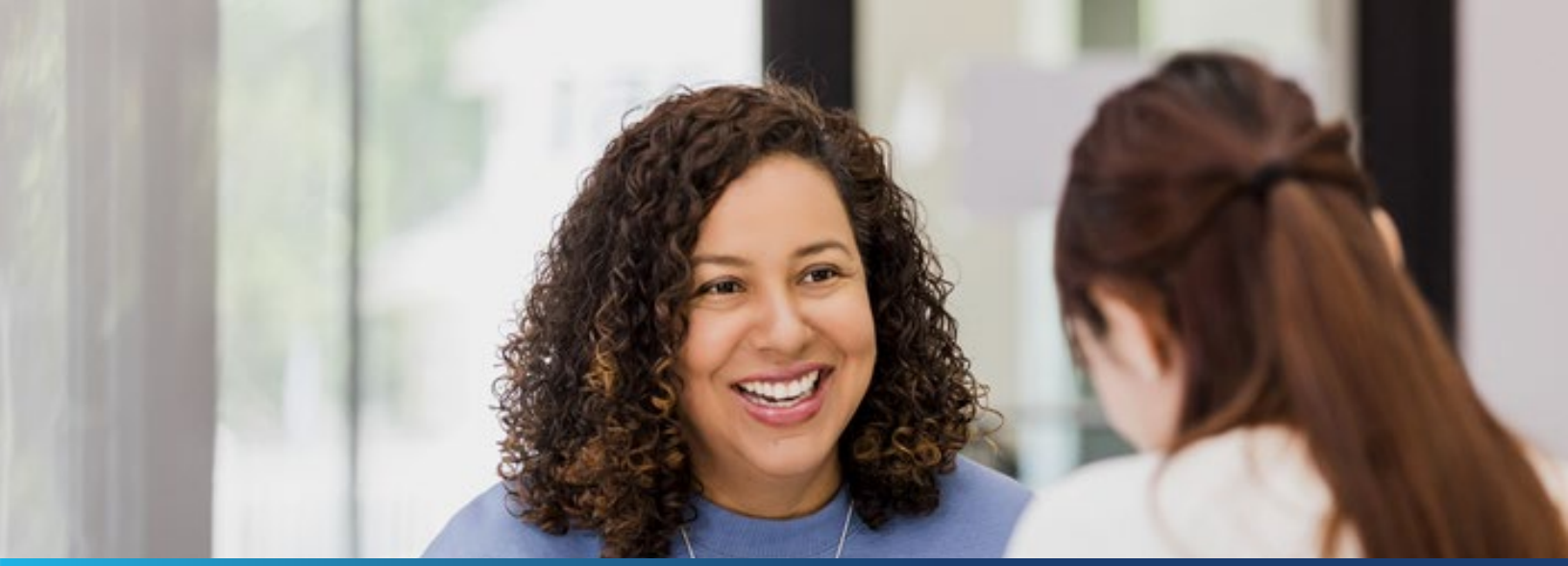

Understanding Information Blocking, Part 2, and HIPAA: An Overview for Health Care Providers

The 21st Century Cures Act Information Blocking Rule aims to promote patient access to health information and increase system interoperability by establishing penalties for actors who engage in "information blocking." Actors include health care providers, certain health IT developers, health information networks (HINs), and health information exchanges (HIEs).

What You Need to Know

Generally, information blocking includes practices that would "interfere with, prevent, or materially discourage the access, exchange, or use of electronic health information."[1] However, the Information Blocking Rule does not preempt privacy laws and regulations such as 42 CFR Part 2 and the Health Insurance Portability and Accountability Act (HIPAA). Entities covered by the Information Blocking Rule ("actors"), which includes health care providers, are still obligated to protect information covered by such laws.

[1] See 42 U.S.C. 300jj-52(a)(1).

Funded by Substance Abuse and Mental Health Services Administration

Information Blocking Exceptions

The Information Blocking Rule includes eight exceptions for permissible practices that may seem to meet the definition of information blocking but do not constitute information blocking. They include:[2]

- The preventing harm exception
- The privacy exception[3]
- The security exception
- The infeasibility exception[4]
- The health IT performance exception
- The licensing exception
- The fees exception
- The content and manner exception

The **privacy** and **infeasibility** exceptions are particularly instructive for individuals and entities that maintain data subject to heightened privacy protections such as Part 2, HIPAA's protections for psychotherapy notes, or state health privacy laws. Furthermore, health care providers should also be aware of the **fees exception** and its limitations.

The Privacy Exception

The privacy exception specifies that an actor is not required to use or disclose health information in a way that is prohibited under state or federal privacy laws.

A closer look:

If a provider is required by Part 2, HIPAA, or a different state or federal privacy law to obtain patient consent or authorization before providing access, exchange, or use of protected health information, the provider may only provide access to the information if the patient has provided consent or authorization. When patient information is covered by multiple privacy laws, the law that is more protective of patient privacy generally controls.

---

[2] For more information about the eight exceptions to the Information Blocking Rule, see Cures Act Final Rule: Information Blocking Exceptions

[3] 45 CFR §171.202.

[4] 45 CFR §171.204.

Key point: following a legal requirement to obtain patient consent prior to making a disclosure meets the "privacy exception" in the Information Blocking Rule and is not considered information blocking.

Example: If a health care provider is covered by both HIPAA and Part 2, and HIPAA permits the disclosure of the patient's SUD information without an authorization while Part 2 requires written consent prior to making the disclosure, the health care provider may **not** disclose the SUD information without the patient's written consent. The privacy exception applies in this instance and the health care provider is not violating the Information Blocking Rule by refusing to share the information when the relevant precondition – the patient's written consent – is not present.

Another example is if HIPAA permits a health care provider to make a disclosure of a patient's mental health records, but the applicable state law prohibits the disclosure absent a patient's written consent. If the health care provider has not obtained the patient's written consent as required by the state law, the health care provider is not required to share the records.

Lastly, a health care provider that operates in multiple states is permitted to adopt uniform policies and procedures that comply with the state that has the most restrictive privacy protective laws, without violating the information blocking rules. The Assistant Secretary for Technology Policy (ASTP) provided the following example: If State A has more stringent privacy protections (e.g. preconditions) for the disclosure of reproductive health information to law enforcement than HIPAA and State B, a health care provider can adopt the enhanced privacy protections of State A uniformly across their operations in State A and State B and this would not be considered information blocking.[5]

For more information about the Information Blocking Rule and its application to heightened privacy protections for SUD and MH treatment records, see our resource, **21st Century Cures Act Final Rule on Information Blocking**.

[5] Assistant Secretary for Technology Policy, Frequently Asked Questions, Privacy Exception.

The Infeasibility Exception

The infeasibility exception specifies, among other things, that an actor is not required to provide access to requested health information if the requested information cannot be unambiguously segmented from (1) information protected from disclosure by law or from (2) information that "the patient has expressed a preference not to disclose."[6]

A closer look:

Practically, this means that the infeasibility exception may often apply to electronic health portals that do not have the capacity to distinguish between various types of patient health information, for example, if the patient records include information protected by heightened privacy laws like 42 CFR Part 2 that require consent for the disclosure. The preamble to the final rule states that "an actor will be covered under this condition if the actor could not fulfill a request to access, exchange, or use electronic health information (EHI) because the requested EHI could not be unambiguously segmented from patient records created by federally assisted programs (i.e., Part 2 Programs) for the treatment of substance use disorder (and covered by 42 CFR part 2) or from records that the patient has expressed a preference not to disclose."[7]

To meet this exception, a health care provider must provide a written response to the requestor within 10 business days of receipt of the request with the reason(s) why the request is infeasible.

Key point: if a health care provider cannot segment Part 2-protected records (or records protected by another applicable law) or records that the patient has expressed a preference to not disclose, the infeasibility exception may apply.

Example: A Part 2 program[8] within a larger hospital system is asked to upload all patients' Part 2 records into the hospital's patient portal, which does not have processes in place to segment Part 2 records or flag whether certain individuals have the patient's consent to access Part 2 records.

---

[6] See 45 CFR § 171.204; 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program, 85 Fed. Reg. 25,642, 25,867 (May 1, 2020).
[7] 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program, 85 Fed. Reg. 25,642, 25,867 (May 1, 2020).
[8] A "Part 2 program" is a substance use disorder treatment provider that is both federally assisted and meets the definition of a "program" under 42 CFR § 2.11.

Would withholding the records from the portal be information blocking?

NO. According to the infeasibility exception, if the hospital's electronic health portal does not have the capacity to unambiguously segment a patient's Part 2 data from the rest of their health information, the health care provider must withhold the patient's Part 2 data from the portal.

Not only does the infeasibility exception permit the provider to withhold Part 2 protected information from such a portal, but federal law also prohibits the provider from disclosing protected information in this way.

Fees Exception

Actors may charge a fee for accessing, exchanging, or using the patient's information, provided that certain conditions are met, including that the fee be reasonably related to costs incurred.[9]

A closer look:

The Information Blocking Rule promotes the right of individuals to access their own health information, in accordance with HIPAA's right of access at 45 C.F.R. § 164.524. The fees exception does not apply to a fee for an individual (or their personal representative or another person designated by the individual) to obtain "electronic access" to their medical records, including sharing the information with an entity designated by the individual. ASTP has stated in the preamble to the regulation that "practices that involve an actor charging an individual (or the individual's personal representative or another person or entity designated by the individual) a fee to access, exchange, or use their EHI would be inherently suspect and would be extremely likely to implicate the information blocking provision."[10]

Key point: there may be certain circumstances where health care providers can charge fees to access, exchange, or use electronic health information. Fees based on an individual accessing their own electronic health information are likely to be information blocking.

---

[9] Cures Act Final Rule: Information Blocking Exceptions, Page 4, https://www.healthit.gov/sites/default/files/page2/2020-03/InformationBlockingExceptions.pdf.

[10] 21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program, 85 Fed. Reg. 25,642, 25,887(May 1, 2020).

For More Information

Resources:

This resource is one of many that are available within the Center of Excellence for Protected Health Information's resource library, which can be found at **coephi.org**.

Request technical assistance:

You can request brief, individualized technical assistance and join our mailing list for updates, including news about the publication of new resources and training opportunities **on our website**.

This resource was authored by:

Meghan Mead, JD

Stephen Murphy, JD

Jacqueline Seitz, JD

Amber Black, JD (former CoE-PHI Legal Subject Matter Expert)

Resources, training, technical assistance, and any other information provided through the Center of Excellence for Protected Health Information do not constitute legal advice. For legal advice, including legal advice on other applicable state and federal laws, please seek out local counsel.

This resource was supported by SAMHSA of the U.S. Department of Health and Human Services (HHS) as part of a financial assistance award with 100 percent funded by SAMHSA/HHS. The contents are those of the author(s) and do not necessarily represent the official views of, nor an endorsement, by SAMHSA/HHS, or the U.S. Government.