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

**Updated in April 2026 to address recent changes to the Information Blocking Rule*

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, health IT developers of certified health IT, 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."[i] 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). Information blocking does not include practices that are "required by law" or that meet an exception.[ii] Health care providers that are also actors are still obligated to protect information covered by such laws.

Information blocking exceptions

In addition to carving out practices required by law, the Information Blocking Rule has ten exceptions for permissible practices that may seem to otherwise meet the definition of information blocking but do not constitute information blocking. They include:[iii]

- The preventing harm exception
- The privacy exception[iv]
- The security exception
- The infeasibility exception[v]
- The health IT performance exception
- The protecting care access exception
- The licensing exception
- The fees exception[vi]
- The manner exception
- The TEFCA 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 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 has four sub-exceptions. The two that are most relevant to health care providers are (1) precondition not satisfied[vii] and (2) respecting an individual's request not to share information[viii]. The first 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, if for example, a precondition such as obtaining patient consent or authorization is not met. The second states an actor does not violate the Information Blocking Rule if it elects not to provide access, exchange or use of EHI because the individual has requested the actor not share the EHI and the actor has satisfied conditions including timely documenting the request.

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 that consent or authorization. In this instance, the provider does not violate the Information Blocking Rule because there is a condition precedent to the access, exchange or use that is not satisfied.

When patient information is covered by multiple privacy laws, the law that is more protective of patient privacy generally controls. For 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.

Furthermore, 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 Rule. Health and Human Services (HHS) 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.[ix] This flexibility may be helpful for providers that operate in multiple states with varying degrees of privacy protection in their laws.

Lastly, another example is if HIPAA permits a health care provider to make a disclosure of a patient's mental health records, but the patient has requested the provider not share this information and the provider has documented the request in a timely fashion. In this instance, the provider has met the relevant privacy sub-exception and is not required to share the records.

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.

Key point

Following a legal requirement to obtain patient consent or authorization prior to making a disclosure or respecting an individual's request not to share information meets the "privacy exception" in the Information Blocking Rule and is not considered information blocking when all conditions are met.

The infeasibility exception

The infeasibility exception applies under certain conditions. Of particular relevance to health care providers is the condition on segmentation. This specifies 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 (2) information that may be withheld pursuant to the preventing harm[x], privacy, or protecting care access[xi] exceptions.[xii]

A closer look

Practically, this means that the infeasibility exception may apply to electronic health portals that do not have the technological capacity to distinguish between various types of patient health information. For example, it may apply if the patient records include information protected by heightened privacy laws like 42 CFR Part 2 that require consent for the disclosure or if they contain records that the patient has expressed a preference not to disclose. 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 behavioral health clinic treated a patient for both SUD and mental health.[xiii] The electronic health record for the patient contains both mental health records covered by HIPAA and SUD information covered by HIPAA and Part 2. The clinic receives a request from a hospital for the patient's mental health records for treatment purposes. The clinic has no technologically feasible way to separate the mental health records from the records covered by Part 2, nor does it have a signed patient consent to share the Part 2 records.

Would withholding the Part 2 records and mental health records from the hospital be information blocking?

- NO. According to the infeasibility exception, if the clinic's electronic health record system does not have the capacity to unambiguously segment a patient's Part 2 data from the rest of their health information that they are permitted to share, the health care provider may decline to share the patient's records without violating the Information Blocking Rule.

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 and does not include any excluded fees.[xiv]

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. A provider will generally not violate the Information Blocking Rule by charging a reasonable fee to copy or access records, even when the fee results in a reasonable profit margin. However, this is not true in all instances, including for "electronic access" by an individual (or their personal representative or another person designated by the individual) to their electronic medical records, such as through a patient portal. The regulation states that the fees exception does not apply to a "fee based in any part on the electronic access of an individual's EHI by the individual, their personal representative, or another person or entity designated by the individual."[xv] "Electronic access" refers to an internet-based method that makes EHI available at the time it is requested and where no manual effort is required.[xvi]

Key Point

Health care providers can generally charge fees to access, exchange, or use electronic health information, including fees that result in a reasonable profit margin. Fees based on an individual gaining electronic access to their own EHI, however, are information blocking.

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.

Disclaimer

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

This resource was authored by:
Jacqueline Seitz, JD
Meghan Mead, JD
Stephen Murphy, JD
Amber Black, JD (former CoE-PHI Legal Subject Matter Expert)

References

[i] See 42 U.S.C. 300jj-52(a)(1); see also 45 C.F.R. Part 171.
[ii] 45 CFR §171.103.
[iii] For more information about the exceptions to the Information Blocking Rule, see Cures Act Final Rule: Information Blocking Exceptions https://www.healthit.gov/sites/default/files/page2/2020-03/InformationBlockingExceptions.pdf; HTI-3 Final Rule: Protecting Care Access https://www.healthit.gov/wp-content/uploads/2025/06/HTI-3_Final_Rule_Fact_Sheet.pdf.
[iv] 45 CFR §171.202.
[v] 45 CFR §171.204.
[vi] 45 CFR §171.302.
[vii] 45 CFR §171.202(b).
[viii] 45 CFR §171.202(e).
[ix] Assistant Secretary for Technology Policy, Frequently Asked Questions, Privacy Exception.
[x] 45 CFR §171.201.
[xi] 45 CFR §171.206.
[xii] 45 CFR §171.204(a)(2).
[xiii] 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.
[xiv] Cures Act Final Rule: Information Blocking Exceptions, Page 4, https://www.healthit.gov/sites/default/files/page2/2020-03/InformationBlockingExceptions.pdf.
[xv] 45 CFR §171.302(b)(2).
[xvi] 45 CFR §171.302(d).