Information Blocking

Information Blocking Exceptions:

Security Exception &
Health IT Performance Exception

(Part 2 of 8)

In **Part 1 of our series on the information blocking exceptions**, Gravely Group explained the rationale behind the creation of a set of exceptions for certain **Practices** that, while otherwise constituting information blocking, are nonetheless permitted because such Practices serve a greater public good. We also described the two categories of information blocking exceptions created by ONC, and we introduced the **eight information blocking exceptions from the Final Rule** and the operative question under each.

If you have not yet read **Gravely Group's overview of the information blocking exceptions**, we suggest you check it out!

In this post, we will cover two of the exceptions that involve not fulfilling a request to access, exchange, or use EHI:

The Security Exception
&
The Health IT Performance Exception

As we mentioned in the overview, **each of the information blocking exceptions is narrowly defined, and an Actor must meet every element of an exception in order to be certain that its Practice is protected from information blocking penalties or disincentives.** Meeting *most* of the requirements of an exception (or a combination of partial requirements from different exceptions) is NOT sufficient to fit within the "safe harbor" of an exception.

With that, let's dive into the first of our eight information blocking exceptions...

The Security Exception

The Security Exception focuses on **when an Actor's Practice that is likely to interfere with the access, exchange, or use of electronic health information (EHI) will *not* be considered information blocking because the Practice is reasonable and necessary to protect the security of the EHI.** In its Proposed Rule on information blocking, ONC explained that the intent of the

Security Exception is to provide Actors with flexibility in how they approach promoting the security of EHI, while preventing security measures that are overly broad, burdensome, and/or inconsistent.

To satisfy this exception, the Practice must be:

1. **Directly related** to safeguarding the **confidentiality, integrity, and availability** of EHI;
2. **Tailored** to the **specific, identified** security risk(s); *AND*
3. **Implemented consistently** in a **non-discriminatory** manner.

In addition to the above, there are further requirements that must be met depending on whether the Practice is based on an organizational security policy or whether the Practice is in response to an unforeseen threat to the security of the EHI.

If the Practice is based on an organizational security policy, that policy must:

- Be **in writing**;
- Address **specifically identified and assessed risk(s)**;
- Be based on **consensus-based standards and/or best practices**; *AND*
- Contain **objective timelines and other parameters** for identifying, responding to, and addressing security incidents.

If the Practice is in response to an unforeseen threat to the security of EHI, the Actor must make **an individualized determination**—based on the specific facts and circumstances—that:

1. The Practice is **necessary to mitigate** the security risk to the EHI; *AND*
2. There are **no reasonable alternatives** that would address the security risk while being less likely to interfere with the access, exchange, or use of EHI.

Health IT Performance Exception

The Health IT Performance Exception focuses on **when an Actor's Practice that is likely to interfere with the access, exchange, or use of electronic health information (EHI) will *not* be considered information blocking because the Practice is implemented to maintain or improve health IT performance.** ONC created this exception in recognition of the fact that Actors must periodically take actions to maintain or improve IT systems or networks and that such actions might interfere with an Actor's ability to fulfill requests for access, exchange, or use of EHI. Included in this concept of actions taken to maintain IT systems or networks is recognition of the importance of maintaining assured levels of performance.

Therefore, under the Health IT Performance Exception, an Actor may implement a Practice EITHER:

A. For the **maintenance or improvement** of health IT systems/networks that results in the **temporary unavailability or temporary degradation** of the Actor's health IT; *OR*

B. Against a **third-party application** that is **negatively affecting the performance** of the Actor's health IT

Provided that such Practice is:

1. Implemented to last **no longer than necessary** to complete the maintenance/improvements or to resolve any negative impacts;
2. Implemented in a **consistent and non-discriminatory** manner; *AND*
3. Implemented **consistent with existing service level agreements** or, if unplanned, as **agreed to by the Actor's customer**, where applicable.

Note that, if the unavailability of an Actor's health IT for maintenance or improvement is implemented to protect against a security risk, the Actor would need to meet all of the requirements of the Security Exception but not the Health IT Performance Exception.

UP NEXT ...

Gravely Group's next post in this series on the information blocking exceptions will cover the **Privacy Exception**. Stay tuned!