The Office of the National Coordinator for Health Information Technology

21ST CENTURY CURES ACT:
INTEROPERABILITY, INFORMATION BLOCKING, AND
THE ONC HEALTH IT CERTIFICATION PROGRAM PROPOSED RULE

Information Blocking Exception for Security-Related Practices

OVERVIEW

Under the proposed exception, it will not be information blocking for an actor to engage in practices that interfere with access, exchange, or use of electronic health information (EHI) and that are reasonable and necessary to secure EHI, subject to certain conditions.

While the importance of security practices cannot be overstated, the proposed exception is not available for all practices that purport to secure EHI. The exception operates to place a cap on what is reasonable and necessary by screening out practices that are unreasonably broad, onerous, and are not applied consistently by an organization, or that otherwise unreasonably interfere with access, exchange, or use of EHI.

To qualify for this exception, an actor's security-related practice must:

Satisfy Threshold Conditions

+

Implement a Qualifying Organizational Security Policy

or

Implement a Qualifying Security Determination

Objective

- Establish an exception that is sufficiently flexible to recognize all legitimate security practices.
- Protect reasonable and necessary security practices by actors, but not prescribe a "maximum" level of security or dictate a one-size-fits-all approach. Actors should determine the security-related practices appropriate for their organization, and those practices should be recognized provided that certain conditions are met.

"Actors" regulated by the information blocking provision:

- Health Care Providers
- Health IT Developers of Certified Health IT
- Health Information Exchanges
- Health Information Networks

Threshold Conditions

To qualify for this exception, an actor's practice must satisfy each of the following threshold conditions:

- The practice must be directly related to safeguarding the confidentiality, integrity, and availability of EHI;
- The practice must be tailored to the specific security risk being addressed;
- The practice must be implemented in a consistent and non-discriminatory manner.

Qualifying Organizational Security Policy

If the practice implements and conforms to an actor's written organizational security policy, that policy must:

- Have been prepared on the basis of, and directly respond to, security risks identified and assessed by or on behalf of the actor;
- Align with one or more applicable consensus-based industry standards or best practice guidance (e.g., NIST-800-53-4; the NIST Cybersecurity Framework; and NIST SP 800-100, SP 800-37, SP 800-39); and
- Provide objective timeframes and other parameters for identifying, responding to, and addressing security incidents.

HIPAA covered entities and business associates may be able to leverage their HIPAA Security Rule compliance activities and can, if they choose, align their security policy with those parts of the NIST Cybersecurity Framework that are referenced in the HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework to satisfy this condition.

Qualifying Security Determination

If the practice does not implement an organizational security policy, the actor must have made a determination, based on the particularized facts and circumstances, that:

- The practice is necessary to mitigate the security risk to EHI; and
- There are no reasonable and appropriate alternatives to the practice that address the security risk that are less likely to interfere with, prevent, or materially discourage access, exchange, or use of EHI.

The proposed exception recognizes that even a best practice risk assessment and security policy may not anticipate novel and unexpected threats.