ONC's Seven Excepted Categories to Information Blocking

I. An Overview

The Law

The 21st Century Cures Act (Cures Act) was signed into law on December 13, 2016. Among the many health IT-related provisions it contains is one related to "Information Blocking" in Section 3022.

Who Must Comply?

The law lays out four types of actors for whom information blocking provisions and enforcement by the Office of the Inspector General (OIG) apply: 1) Providers; 2) Health IT Developers; 3) Health Information Networks (HINs); and 4) Health Information Exchanges (HIEs). See our related cheat sheet for an overview of these four actors and how the law and ONC define them.

Enforcement

The Cures Act authorizes the U.S. Department of Health & Human Services' (HHS) Office of the Inspector General (OIG) to investigate claims of information blocking. The law calls for civil monetary penalties for Health IT Developers, HINs and HIEs of up to $1 million per violation. These penalties do not apply to providers. HHS has yet to name the penalties a provider would face if they are charged with information blocking. The Centers for Medicare & Medicaid Services (CMS) will likely establish penalties for providers in the near future.

Overview of ONC's Role

The Office of the National Coordinator (ONC) proposes in their proposed rule, "21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program" published March 4 to establish seven exceptions to the information blocking provisions. The exceptions would apply to certain activities that may technically meet the definition of information blocking but that are reasonable and necessary to further the underlying public policies of the information blocking provision. Below is each exception, a discussion on the exception, and sub-exceptions/conditions that need to be met for the exception to apply.

Electronic Health Information

The definition of information blocking applies to electronic health information (EHI). ONC proposes defining this as: (i) electronic protected health information; and (ii) any other information that:

- Is transmitted by or maintained in electronic media;
- Identifies the individual, or with respect to which there is a reasonable basis to believe the information can be used to identify the individual; and

- Relates to the past, present, or future health or condition of an individual; the provision of healthcare to an individual; or the past, present, or future payment for the provision of health for an individual.

Structure of Exceptions

The seven named exceptions are intended to promote public confidence in health IT infrastructure by supporting privacy / security of EHI, protecting patient safety, and promote competition / innovation. Activities related to why information is not being shared must be both reasonable and necessary to advance aim of Information Blocking provision. And, each exception addresses a significant risk that regulated people/entities won't engage in these reasonable and necessary activities due to uncertainty around the breadth of the blocking provision. Finally, each exception is intended to be tailored through appropriate conditions so that its limited to reasonable and necessary activities and doesn't protect real Information Blocking practices.

Seven Exceptions

1. **Preventing Harm**
2. **Promoting the privacy of electronic health information** (In order for the exception to apply, the actor must satisfy at least one of the sub-exceptions):
    a. **Pre-condition not satisfied** (relates to federal or state law requiring a condition be met before sharing)
    b. **Developer not covered by HIPAA** (relates to when a health IT developer of certified health IT that is not covered by the HIPAA Privacy Rule)
    c. **Denying right to access** (relates to when a covered entity or business associate denies an individual's request for access to their ePHI)
    d. **Individual's request not to share** (relates to not providing access, exchange, or use of EHI pursuant to an individual's request)
3. **Promoting the security of electronic health information**
4. **Recovering costs reasonably incurred**
5. **Responding to Requests that are Infeasible**
6. **Licensing of interoperability elements on reasonable and nondiscriminatory terms**
7. **Maintaining and improving health IT performance**

II. Summary of Each Exception

Exception #1: Preventing Harm:

Risk of corrupt or inaccurate data being recorded or incorporated in a patient's electronic health record

This exception would apply in circumstances where information blocking would prevent inaccurate data being recorded into a patient's electronic health record.

The exception may apply to practices that prevent harm arising from corrupted or inaccurate EHI being recorded or incorporated in a patient's electronic health record.

This recognized risk is limited to corruption and inaccuracies caused by performance and technical issues affecting health IT. For example, this exception may be relevant if certified health IT were to incorrectly present an old and superseded version of a medication list, or when only partial copies of laboratory tests are being linked to a patient when the patient's record is exchanged. However, this recognized risk does not extend to purported accuracy issues arising from the incompleteness of a patient's electronic health record generally. Electronic health records, like the paper charts they replaced, are inevitably imperfect records. Many patients see multiple healthcare providers and so it is unlikely that any single healthcare provider's record will provide a complete picture of a patient's health. Some patients intentionally keep certain information secret even from their healthcare providers, and others fail to share potentially critical information with their healthcare providers because they forget to, or simply do not understand its clinical significance.

Risk of misidentifying a patient or patient's electronic health information

The exception may apply to practices that are designed to promote data quality and integrity and support health IT applications properly identifying and matching patient records or EHI.

Determination by a licensed health care professional that the disclosure of EHI is reasonably likely to endanger life or physical safety

The exception may permit certain restrictions on the disclosure of an individual's EHI in circumstances where a licensed health care professional has determined, in the exercise of professional judgment, that the disclosure is reasonably likely to endanger the life or physical safety of the patient or another person

Reasonable belief that practice was necessary to directly and substantially reduce the likelihood of harm.

To qualify for this exception, an actor must have had a reasonable belief that the practice or practices will directly and substantially reduce the likelihood of harm to a patient or another person.

Qualifying organizational policy

ONC anticipates that the actor would demonstrate that the practices it engaged in were consistent with an organizational policy that was objectively reasonable and no broader.

Qualifying individualized finding

ONC recognizes that some healthcare providers (such as small practices) may not have comprehensive and formal policies governing all aspects of EHI and patient safety. Additionally, even if an organizational policy exists, it may not anticipate all the potential risks of harm that could arise in real-world clinical or production environments of health IT. In these circumstances, in lieu of demonstrating that a practice conformed to the actor's policies and that the policies met the conditions described above, the actor could justify the practice or practices directly by making a finding in each case, based on the particular facts and circumstances, that the practice is necessary and no broader than necessary to mitigate the risk of harm.

Exception #2: Promoting the Privacy of EHI

ONC proposes to establish an exception to the information blocking provision for practices that are reasonable and necessary to protect the privacy of an individual's EHI, provided certain conditions are met.

In contrast to the other exceptions defined in this proposed rule, this proposed exception has been structured with discrete "sub-exceptions." An actor's practice must qualify for a sub-exception in order to be covered by this exception. The sub-exceptions have, to a large extent, been crafted to closely mirror privacy-protective practices that are recognized under state and federal privacy laws.

ONC has proposed four sub-exceptions that address the following privacy protective practices:

(1) Pre-condition not satisfied: Not providing access, exchange, or use of EHI when a state or federal law requires that a condition be satisfied before an actor provides access, exchange, or use of EHI, and the condition is not satisfied;

(2) Developer not covered by HIPAA: Not providing access, exchange, or use of EHI when the actor is a health IT developer of certified health IT that is not covered by the HIPAA Privacy Rule in respect to a practice;

(3) Denying right to access: A covered entity, or a business associate on behalf of a covered entity, denying an individual's request for access to their electronic PHI in the circumstances provided in 45 CFR 164.524(a)(1), (2), or (3) (proposed at § 171.202(d)); and

(4) Individual's request not to share: Not providing access, exchange, or use of EHI pursuant to an individual's request, in certain situations (proposed in § 171.202(e)).

In order for the exception to apply, the actor must satisfy at least one of the sub-exceptions

Specific terminology used for the purposes of this proposed exception

The rule explains the definitions and terminology used to better clarify that ONC's goal is to ensure that this privacy exception extends protection to information about, and respects the privacy preferences of, all individuals, not only those individuals whose EHI is protected as ePHI by HIPAA covered entities and business associates.

Interaction between information blocking, the exception for promoting the privacy of EHI, and the HIPAA Privacy Rule

ONC strives to make this exception compliant with all HIPAA Privacy rules. Actions taken to remain within the HIPAA guidelines are valid exceptions to the information blocking provision.

Promoting patient privacy rights

The information blocking provision would not require that actors provide access, exchange, or use of EHI in a manner that is not permitted under the HIPAA Privacy Rule or other privacy laws. Actions taken to promote a patient's privacy rights are exceptions to the information blocking provision.

Privacy Practices Required by Law

An actor will not be engaging in information blocking if a state or federal privacy law imposes a precondition to the provision of access, exchange, or use, and that precondition has not been satisfied.

Details on 4 Sub-exceptions

Sub-exception #1 to proposed privacy exception: Precondition not satisfied

ONC proposes to establish a sub-exception to the information blocking provision that recognizes that an actor will not be engaging in information blocking if an actor does not provide access, exchange, or use of EHI because a necessary precondition required by law has not been satisfied. This exception will apply to all instances where an actor's ability to provide access, exchange, or use is "controlled" by a legal obligation to satisfy a condition, or multiple conditions, prior to providing that access, exchange, or use.

Conditions to be met to qualify for the sub-exception

In most circumstances, an actor would be in a position to influence whether a precondition is satisfied. ONC wishes for actors to think about patient privacy as they act within the information blocking provision. Actions in line with promoting patient privacy will be acceptable exceptions.

Organizational policies and procedures

If an actor seeks to qualify for this sub-exception, in part, by implementing and conforming to organizational policies and procedures, such policies and procedures must be in writing, and specify the criteria to be used by the actor, and, if applicable, the steps that the actor will take, in order to satisfy the precondition relied on by the actor not to provide access, exchange, or use of EHI. It would not be sufficient for an actor to simply identify the existence of the precondition in their organizational policies and procedures.

Documenting criteria and rationale

ONC proposes that that an actor can seek to qualify for this sub-exception, in part, by documenting how it reached its decision that it would not provide access, use, or exchange of EHI on the basis that a precondition had not been satisfied.

Meaningful opportunity to provide consent or authorization

If the precondition that an actor purports to have satisfied relies on the provision of a consent or authorization from an individual, it is a condition of this sub-exception that the actor must have done all things reasonably necessary within its control to provide the individual with a meaningful opportunity to provide that consent or authorization. This condition will be relevant when, for example, a state privacy law or the HIPAA Privacy Rule requires an individual to provide their consent and/or HIPAA authorization before identifiable information can be accessed, exchanged, or used for specific purposes.

Practice must be tailored to the specific privacy risk or interest being addressed

To qualify for this sub-exception, an actor's privacy-protective practice must be tailored to the specific privacy risks that the practice addresses. This condition necessarily presupposes that an actor has carefully evaluated the privacy requirements imposed on the actor, the privacy interests to be managed by the actor, and has developed a considered response that is tailored to protecting and promoting the privacy of EHI.

Practice must be implemented in a consistent and non-discriminatory manner

ONC proposes that in order for a practice to qualify for this sub-exception, the practice must be implemented in a consistent and non-discriminatory manner. This condition would provide basic assurance that the purported privacy practice is directly related to a specific privacy risk and is not being used to interfere with access, exchange, or use of EHI for other purposes to which this exception does not apply.

Sub-exception #2 to proposed privacy exception: Health IT developer of certified health IT not covered by HIPAA

This proposed sub-exception recognizes as reasonable and necessary the activities engaged in by actors consistent with the controls placed on access, exchange, or use of EHI by federal and state privacy laws. Importantly, that sub-exception is limited to actors that are subject to those federal and state privacy laws; an actor that is not regulated by HIPAA or a state privacy law cannot benefit from the exception proposed.

Practice must implement privacy policy

In order to qualify for this sub-exception, the practice engaged in by the non-covered actor —the interference with access, exchange, or use of EHI—must also implement a process described in the actor's organizational privacy policy. This requires that a non-covered actor must have documented in detail in its organizational privacy policy the processes and procedures that the actor will use to determine when the actor will not provide access, exchange, or use of EHI.

Practice must have been disclosed to users

A non-covered actor that seeks to benefit from this proposed sub-exception must also ensure that it has previously disclosed the privacy-protective practice to the individuals and entities that use, or will use, the health IT.

To qualify for this sub-exception, a non-covered actor would not be required to disclose its organizational privacy policy to its customers or to the public generally. Rather, the noncovered actor need only describe, with sufficient detail and precision to be readily understood by users of the non-covered actor's health IT, the privacy-protective practices that the non-covered actor has adopted and will observe.

Practice must be tailored to privacy risk and implemented in a non-discriminatory manner
ONC proposed that in order for a practice to qualify for this sub-exception, an actor's practice must be tailored to the specific privacy risks that the practice actually addresses, and must be implemented in a consistent and non-discriminatory manner.

Sub-exception #3 to proposed privacy exception: Denial of an individual's request for their electronic protected health information in the circumstances

ONC proposes a limited sub-exception to the information blocking provision that would permit a covered entity or business associate to deny an individual's request for access to their PHI in the circumstances provided under 45 CFR 164.524(a)(1), (2), and (3). ONC believes this

exception would avoid a potential conflict between the HIPAA Privacy Rule and the information blocking provision.

Sub-exception #4 to proposed privacy exception: Respecting an individual's request not to share information

ONC proposes to establish an exception to the information blocking provision that would, in certain circumstances, permit an actor not to provide access, exchange, or use of EHI if an individual has specifically requested that the actor not do so.

Exception #3: Promoting the Security of EHI

ONC proposes to establish an exception to the information blocking provision that would permit actors to engage in practices that are reasonable and necessary to promote the security of EHI, subject to certain conditions.

To qualify for this exception, ONC proposes that an actor's conduct must satisfy threshold conditions. As discussed in detail below, the particular security-related practice must be directly related to safeguarding the confidentiality, integrity, and availability of EHI, implemented consistently and in a non-discriminatory manner, and tailored to identified security risks.

The purpose of this exception to the information blocking provision is to provide flexibility for reasonable and necessary security practices while screening out practices that purport to promote the security of EHI but that are unreasonably broad, onerous on those seeking access to the EHI, are not applied consistently across/within an organization, or otherwise may unreasonably interfere with access, exchange, or use of EHI.

The practice must be directly related to safeguarding the confidentiality, integrity, and availability of EHI.

As a threshold condition, the proposed exception would not apply to any practices that are not directly related to safeguarding the security of EHI…. ONC would also consider whether the practice served any other purposes and, if so, whether those purposes were merely incidental to the overriding security purpose or provided an objectively distinct, non-security-related rationale for engaging in the practice.

The practice must be tailored to the specific security risk being addressed.

To qualify for this exception, ONC proposed that an actor's security-related practice must be tailored to specific security risks that the practice actually addressed. This condition necessarily presupposes that an actor has carefully evaluated the risk posed by the security threat and

developed a considered response that is tailored to mitigating the vulnerabilities of the actor's health IT or other related systems.

Practice must be implemented in a consistent and non-discriminatory manner

ONC proposes that in order for a practice to qualify for this proposed exception, the actor's practice must have been implemented in a consistent and non-discriminatory manner. This condition would provide basic assurance that the purported security practice is directly related to a specific security risk and is not being used to interfere with access, exchange, or use of EHI for other purposes to which this exception does not apply.

Practices that implement an organizational security policy

ONC proposes that, where an actor has documented security policies that align with applicable consensus-based standards, and where the policies are implemented in a consistent and nondiscriminatory manner, a practice's conformity with such policies would provide a degree of assurance that the practice was reasonable and necessary to address specific security risks and thus should not constitute information blocking.

ONC proposes that to support a presumption that a practice conducted pursuant to the actor's security policy was reasonable, the policy would have to meet the following conditions.

- *Risks identified and assessed.* The actor's security policy must be informed by an assessment of the security risks facing the actor. While ONC does not propose any requirements as to a risk assessment, they note that a good risk assessment would use an approach consistent with industry standards and would incorporate elements such as threat and vulnerability analysis, data collection, security measures, likelihood of occurrence, impact, level of risk, and final reporting.
- *Consensus-based standards or best practice guidance.* The actor's policy must align with one or more applicable consensus-based standards or best practice guidance. At present, examples of relevant best practices for development of security policies include, but are not limited to: NIST-800-53 Rev. 5; the NIST Cybersecurity Framework; and NIST SP 800-100, SP 800-37 Rev. 2, SP 800-39, as updated and as interpreted through formal guidance. Best practice guidance on security policies is also developed by consensus standards bodies such as ISO, IETF, or IEC. 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. Relevant consensus-based standards and frameworks provide actors of varying size and resources with the flexibility needed to apply the right security controls to the right

information systems at the right time to adequately address risk.

- *Objective timeframes and other parameters.* ONC proposes that the actor's security policy must provide objective timeframes and common terminology used for identifying, responding to, and addressing security incidents. Examples of acceptable sources for development of a security response plan include: NIST Incident Response Procedure (https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final), US-CERT for interactions with government systems (https://www.us-cert.gov/government-users/reportingrequirements), and ISC-CERT for critical infrastructure (https://ics-cert.us-cert.gov/).

Practices that do not implement an organizational security policy

ONC recognizes that EHI security may present novel and unexpected threats that even a best-practice risk assessment and security policy cannot anticipate. If a practice that does not implement an organizational policy is to qualify for this exception, however, it must meet certain conditions. The actor's practice must, based on the particularized facts and circumstances, be necessary to mitigate the security risk. Importantly, ONC proposed that the actor would have to demonstrate that it considered reasonable and appropriate alternatives that could have reduced the likelihood of interference with access, exchange, or use of EHI, and that there were no reasonable and appropriate alternatives that were less likely to interfere with access, exchange or use of EHI.

Exception #4: Recovering Costs Reasonably Incurred

ONC proposes to establish an exception to the information blocking provision that would permit the recovery of certain costs reasonably incurred to provide access, exchange, or use of EHI.

Requirement that costs be reasonably incurred

Regardless of the type of cost at issue, a basic condition of this proposed exception is that any costs the actor seeks to recover must have been reasonably incurred to provide the relevant interoperability elements to enable access, exchange, or use of EHI.

Method for Recovering Costs

To qualify for the exception, ONC proposes that the method by which the actor seeks to recover its costs must be reasonable and non-discriminatory. This would require that the actor base its recovery of costs on objective and verifiable criteria that are uniformly applied for all substantially similar or similarly situated classes of persons and requests. ONC emphasizes that this proposal does not mean that the actor must apply the same prices or price terms for all persons or classes of persons to whom it provides the services. However, any differences in prices or price terms would have to be based on actual differences in the costs that the actor

incurred or other reasonable and non-discriminatory criteria.ONC also proposes that the method by which the actor recovers its costs must be reasonably allocated among all customers to whom the technology or service is supplied, or for whom the technology is supported… ONC proposes that the method by which the actor recovers its costs must not be based on the sales, profit, revenue, or other value that the requestor or other persons derive or may derive from the access to, exchange of, or use of electronic health information, including the secondary use of such information, that exceeds the actor's reasonable costs for providing access, exchange, or use of electronic health information. ONC emphasizes that such revenue-sharing or profit-sharing arrangements would only be acceptable and covered by the exception if such arrangements are designed to provide an alternative way to recover the costs reasonably incurred for providing services.

Costs Specifically Excluded

ONC proposes that certain costs should be explicitly excluded from this exception regardless of the method for recovering the costs. They have proposed these excluded costs, which are detailed below, in an effort to provide additional clarity about the scope of this exception and to create guardrails for preventing potential misuse of the exception.

- *Costs Due to Non-standard Design or Implementation Choices:* ONC proposes that this exception would not permit the recovery of any cost that the actor incurred due to the health IT being designed or implemented in non-standard ways that unnecessarily increase the complexity, difficulty or burden of accessing, exchanging, or using EHI.

- *Subjective or Speculative Costs:* ONC proposes to limit this exception to the recovery of costs that an actor actually incurred to provide the relevant interoperability element or group of elements (which may comprise either products or services). ONC proposes that this exception would not permit the recovery of certain types of costs that are subjective or speculative.

- *Fee Prohibited under HIPAA Privacy Rule:* ONC also proposes that the exception would not apply to fees prohibited under HIPAA's Privacy Rule. The Rule permits a covered entity to impose a reasonable, cost-based fee if the individual requests a copy of the PHI (or agrees to receive a summary or explanation of the information). The fee may include only the cost of: (1) labor for copying the PHI requested by the individual, whether in paper or electronic form; (2) supplies for creating the paper copy or electronic media (e.g., CD or USB drive) if the individual requests that the electronic copy be provided on portable media; (3) postage, when the individual requests that the copy, or the summary or explanation, be mailed; and (4) preparation of an explanation or summary of the PHI, if agreed to by the individual. The fee may not include costs associated with verification; documentation; searching for and

retrieving the PHI; maintaining systems; recouping capital for data access, storage, or infrastructure; or other costs not listed above even if such costs are authorized by state law.

- *Individual Electronic Access:* ONC proposes that this exception would not apply if the actor charged a fee based in any part on the electronic access by an individual or their personal representative, agent, or designee to the individual's EHI.

- *Export and Portability of EHI Maintained in EHR Systems:* ONC proposes that fees charged for the export, conversion, or migration of data from an EHR technology would not qualify for the exception unless they also meet two additional conditions. "1. ONC proposes that health IT developers of certified health IT would, for purposes of this exception, be precluded from charging a fee to perform an export of EHI via the capability of health IT certified to the proposed 2015 Edition "EHI export" certification criterion (§ 170.315(b)(10)) for the purposes of switching health IT systems or to provide patients their EHI. 2. ONC proposes that the exception would not apply to a fee to export or convert data from an EHR technology unless such fee was agreed to in writing at the time the technology was acquired, meaning when the EHR developer and the customer entered into a contract or license agreement for the EHR technology."

- *Compliance with the Condition of Certification Specific to API Technology Suppliers and API Data Providers.*

  ONC proposes that a health IT developer of certified health IT subject to the API Condition of Certification must comply with all requirements of that condition for all practices and at all relevant times in order to qualify for this exception.

- *Application of the Exception to Individual Practices*

  ONC clarifies that the conditions of this exception, including those governing the methodology and criteria by which an actor calculates and distributes its costs, must be satisfied for each and every fee that an actor charges to a customer, requestor, or other person.

Exception #5: Responding to Requests that are Infeasible

ONC proposes to establish an exception to the information blocking provision that would permit an actor to decline to provide access, exchange, or use of EHI in a manner that is infeasible, provided certain conditions are met.

To qualify for this proposed exception, in addition to meeting other conditions, ONC proposes that compliance with the request for access, exchange, or use must be infeasible. They propose a two-step test that an actor would need to meet in order to demonstrate that a request was infeasible.

i. Infeasibility of Request
ii. Duty to Timely Respond and Provide Reasonable Cooperation

i. Infeasibility of request:

Complying with the request would impose a substantial burden on the actor

Under the first step of the infeasibility test, the actor would need to show that complying with the particular request in the manner requested would impose a substantial burden on the actor that is unreasonable under the circumstances.

The burden imposed on the actor would be plainly unreasonable under the circumstances

The actor must also demonstrate that requiring it to comply with the request— and thus to assume the substantial burden demonstrated under the first part of the test—would have been plainly unreasonable under the circumstances. Whether it would have been plainly unreasonable for the actor to assume the burden of providing access, exchange, or use will be highly dependent on the particular facts and circumstances.

ONC proposes to rely primarily on the following key factors:

- The type of EHI and the purposes for which it may be needed;
- The cost to the actor of complying with the request in the manner requested;
- The financial, technical, and other resources available to the actor;
- Whether the actor provides comparable access, exchange, or use to itself or to its customers, suppliers, partners, and other persons with whom it has a business relationship;
- Whether the actor owns or has control over a predominant technology, platform, health information exchange, or health information network through which EHI is accessed or exchanged;
- Whether the actor maintains ePHI on behalf of a covered entity, or maintains EHI on behalf of the requestor or another person whose access, exchange, or use of EHI will be enabled or facilitated by the actor's compliance with the request;
- Whether the requestor and other relevant persons can reasonably access, exchange, or use the information from other sources or through other means; and

- The additional cost and burden to the requestor and other relevant persons of relying on alternative means of access, exchange, or use.

  ONC would consider the balancing of relative burdens in conjunction with the actor's control over interoperability elements.

ii. Duty to Timely Respond and Provide Reasonable Cooperation

In addition to demonstrating that a particular request or class of requests was infeasible, ONC proposes that an actor would have to show that it satisfied several additional conditions. Specifically, to qualify for this exception, the actor must have timely responded to all requests relating to access, exchange, and use of EHI, including but not limited to requests to establish connections and to provide interoperability elements. Further, for any request that the actor claims was infeasible, the actor must have provided the requestor with a detailed written explanation of the reasons why the actor could not accommodate the request. Finally, the actor must have worked with the requesting party in a timely manner to identify and provide a reasonable alternative means of accessing, exchanging, or using the EHI, as applicable. The actor's failure to meet any of these conditions would disqualify the actor from the exception and could also be evidence that the actor knew that it was engaging in practices that contravened the information blocking provision.

Exception #6: Licensing of Interoperability Elements on Reasonable and Non-discriminatory Terms

ONC proposes to establish an exception to the information blocking provision that would permit actors to license interoperability elements on reasonable and non-discriminatory (RAND) terms, provided that certain conditions are met.

i. Reasonable and Non-discriminatory (RAND) Terms

ONC proposes to require, as a condition of this exception, that any terms upon which an actor licenses interoperability elements must be reasonable and non-discriminatory (RAND).

ONC proposes that, to qualify for this exception, an actor must license requested interoperability elements on RAND terms. To comply with this condition, any terms or conditions under which the actor discloses or allows the use of interoperability elements must meet several requirements set forth below. These requirements apply to both price terms (such as royalties and license fees) and other terms, such as conditions or limitations on access to interoperability elements or the purposes for which they can be used.

Responding to requests.

ONC proposes that, upon receiving a request to license or use interoperability elements, an actor would be required to respond to the requestor within 10 business days from receipt of the request.

In order to meet this requirement, the actor would be required to respond to the requestor within 10 business days from the receipt of the request by:

(1) negotiating with the requestor in a RAND fashion to identify the interoperability elements that are needed; and
(2) offering an appropriate license with RAND terms, consistent with its other obligations under this exception.

Scope of rights.

To qualify for this proposed exception, ONC proposes that the actor must license the requested interoperability elements with all rights necessary to access and use the interoperability elements for the following purposes, as applicable:

- All rights necessary to access and use the interoperability elements for the purpose of developing products or services that are interoperable with the actor's health IT or with health IT under the actor's control and/or any third party who currently uses the actor's interoperability elements to interoperate with the actor's health IT or health IT under the actor's control. These rights would include the right to incorporate and use the interoperability elements in the licensee's own technology to the extent necessary to accomplish this purpose.
- All rights necessary to market, offer, and distribute the interoperable products and services described above to potential customers and users, including the right to copy or disclose the interoperability elements as necessary to accomplish this purpose.
- All rights necessary to enable the use of the interoperable products or services in production environments, including using the interoperability elements to access and enable the exchange and use of electronic health information.

Reasonable royalty.

ONC proposes that if an actor charges a royalty for the use of interoperability elements, the royalty base and rate must be reasonable. In evaluating the actor's assertions and evidence that the royalty was reasonable, ONC proposes that they may consider the following factors:

- The royalties received by the actor for the licensing of the proprietary elements in other circumstances comparable to RAND-licensing circumstances.
- The rates paid by the licensee for the use of other comparable proprietary elements.
- The nature and scope of the license.
- The effect of the proprietary elements in promoting sales of other products of the licensee and the licensor, taking into account only the contribution of the elements themselves and not of the enhanced interoperability that they enable.
- The utility and advantages of the actor's interoperability element over the existing technology, if any, that had been used to achieve a similar level of access, exchange, or use of EHI.
- The contribution of the elements to the technical capabilities of the licensee's products, taking into account only the value of the elements themselves and not the enhanced interoperability that they enable.
- The portion of the profit or of the selling price that may be customary in the particular business or in comparable businesses to allow for the use of the proprietary elements or analogous elements that are also covered by RAND commitments.
- The portion of the realizable profit that should be credited to the proprietary elements as distinguished from non-proprietary elements, the manufacturing process, business risks, significant features or improvements added by the licensee, or the strategic value resulting from the network effects, switching costs, or other effects of the adoption of the actor's technology.
- The opinion testimony of qualified experts.
- The amount that a licensor and a licensee would have agreed upon (at the time the licensee began using the elements) if both were considering the RAND obligation under this exception and its purposes, and had been reasonably and voluntarily trying to reach an agreement.

Non-discriminatory terms.

ONC proposes that for this exception to apply the terms on which an actor licenses and otherwise provides interoperability elements must be non-discriminatory. This requirement would apply to both price and non-price terms, and thus would apply to the royalty terms discussed immediately above as well as other types of terms that may be

included in licensing agreements or other agreements related to the provision or use of interoperability elements.

To comply with this condition, the terms on which the actor licensed the interoperability elements must be based on criteria that the actor applied uniformly for all substantially similar or similarly situated classes of persons and requests.

Collateral terms.

ONC proposes five additional conditions that would reinforce the requirements of this exception discussed above. First, the actor must not require the licensee or its agents or contractors to not compete with the actor in any product, service, or market, including markets for goods and services, technologies, and research and development. Second, and for similar reasons, the actor must not require the licensee or its agents or contractors to deal exclusively with the actor in any product, service, or market, including markets for goods and services, technologies, and research and development. Third, the actor must not require the licensee or its agents or contractors to obtain additional licenses, products, or services that are not related to or can be unbundled from the requested interoperability elements. Fourth, the actor must not condition the use of interoperability elements on a requirement or agreement to license, grant, assign, or transfer the licensee's own IP to the actor. Finally, the actor must not condition the use of interoperability elements on a requirement or agreement to pay a fee of any kind whatsoever unless the fee meets either the narrowly crafted condition to this exception for a reasonable royalty, or, alternatively, the fee satisfies the separate exception proposed in § 171.204, which permits the recovery of certain costs reasonably incurred. As noted in section VIII.D.4, that exception generally does not allow for the recovery of royalties or other fees associated with intangible assets.

Non-disclosure agreement.

ONC proposes that an actor would be permitted under this exception to require a licensee to agree to a confidentiality or non-disclosure agreement (NDA) to protect the actor's trade secrets, provided that the NDA is no broader than necessary to prevent the unauthorized disclosure of the actor's trade secrets. Further, ONC proposes that the actor would have to identify (in the NDA) the specific information that it claims as trade secrets, and that such information would have to meet definition of a trade secret under applicable law.

ii. Additional Requirements Relating to the Provision of Interoperability Elements

ONC proposes that an actor's practice would need to comply with additional conditions that ensure that actors who license interoperability elements on RAND terms do not engage in separate practices that impede the use of those elements or otherwise undermine the intent of this exception.

ONC proposes that an actor would not qualify for this exception if it engaged in a practice that had the purpose or effect of impeding the efficient use of the interoperability elements to access, exchange, or use EHI for any permissible purpose; or the efficient development, distribution, deployment, or use of an interoperable product or service for which there is actual or potential demand.

ONC proposes one additional safeguard: An actor cannot avail itself of this exception if, having licensed the interoperability elements, the actor makes changes to the elements or its technology that "break" compatibility or otherwise degrade the performance or interoperability of the licensee's products or services.

iii. Compliance with Conditions of Certification

ONC proposes that health IT developers of certified health IT who are subject to the Conditions of Certification proposed in §§ 170.402, 170.403, and 170.404 must comply with all requirements of those Conditions of Certification for all practices and at all relevant times.

Maintaining and Improving Health IT Performance

ONC proposes to establish an exception to the information blocking provision for certain practices that are reasonable and necessary to maintain and improve the overall performance of health IT, provided certain conditions are met. The proposed exception would recognize as reasonable and necessary the practice of an actor making health IT under its control temporarily unavailable to maintain or improve the health IT.

Where the provision of health IT is subject to an allowance for maintenance or improvement that has been agreed to by the recipient of that health IT, we propose that neither that agreement, nor the performance of it, should constitute information blocking, provided that certain conditions are met.

Unavailability of health IT must be for no longer than necessary to achieve the maintenance or improvements for which the health IT was made unavailable

Any unavailability of health IT must be for a period of time no longer than necessary to achieve the maintenance or improvement purpose for which the health IT is made unavailable.

Unavailability of health IT for maintenance or improvements must be implemented in a consistent and non-discriminatory manner

ONC proposes that any unavailability of health IT occasioned by the conduct of maintenance or improvements must be implemented in a consistent and non-discriminatory manner.

Unavailability of health IT for maintenance or improvements must be agreed

In order to benefit from this exception, ONC proposes that the unavailability of health IT due to maintenance or improvements initiated by a health IT developer of certified health IT, HIE, or HIN, must be agreed to by the individual or entity to whom the health IT is supplied. The availability of health IT is typically addressed in a written contract or other written agreements, that puts the recipient of the health IT on notice about the level of EHI and health IT unavailability that can be expected for users of the health IT. By such agreements, the recipient of the health IT willfully agrees to that level of planned and unplanned unavailability (typically referred to in health IT contracts as “downtime”).

Interaction with Preventing Harm and Promoting Security Exceptions

When health IT is made unavailable for maintenance or improvements aimed at preventing harm to a patient or other person, or securing EHI, an actor must comply with the conditions specified in proposed § 171.201 or § 171.203 respectively, in order to qualify for an exception to the information blocking provision.

iii. Regulatory Text for Each Exception

Exception #1: Preventing Harm:

ONC proposes to establish an exception to the information blocking provision for practices that are reasonable and necessary to prevent harm to a patient or another person, provided certain conditions are met. To qualify for this exception, each practice by an actor must meet the following conditions at all relevant times.

(a) The actor must have a reasonable belief that the practice will directly and substantially reduce the likelihood of harm to a patient or another person arising from:

(1) Corrupt or inaccurate data being recorded or incorporated in a patient's electronic health record;

(2) Misidentification of a patient or patient's electronic health information; or

(3) Disclosure of a patient's electronic health information in circumstances where a licensed healthcare professional has determined, in the exercise of professional judgment, that the disclosure is reasonably likely to endanger the life or physical safety of the patient or another person, provided that, if required by applicable federal or state law, the patient has been afforded any right of review of that determination.

(b) If the practice implements an organizational policy, the policy must be:

(1) In writing;

(2) Based on relevant clinical, technical, and other appropriate expertise;

(3) Implemented in a consistent and non-discriminatory manner; and

(4) No broader than necessary to mitigate the risk of harm.

(c) If the practice does not implement an organizational policy, an actor must make a finding in each case, based on the particular facts and circumstances, and based on, as applicable, relevant clinical, technical, and other appropriate expertise, that the practice is necessary and no broader than necessary to mitigate the risk of harm.

Exception #2: Promoting the privacy of electronic health information:

To qualify for this exception, each practice by an actor must satisfy at least one of the sub-exceptions in paragraphs (b) through (e) of this section at all relevant times.

(a) Meaning of "individual" in this section. The term "individual" as used in this section means one or more of the following:

(1) An individual as defined by 45 CFR 160.103.

(2) Any other natural person who is the subject of the electronic health information being accessed, exchanged, or used.

(3) A person who legally acts on behalf of a person described in paragraph (a)(1) or (2) of this section, including as a personal representative, in accordance with 45 CFR 164.502(g).

(4) A person who is a legal representative of and can make healthcare decisions on behalf of any person described in paragraph (a)(1) or (2) of this section.

(5) An executor, administrator or other person having authority to act on behalf of a deceased person described in paragraph (a)(1) or (2) of this section or the individual's estate under state or other law.

(b) Precondition not satisfied. If the actor is **required by a state or federal privacy law to satisfy a condition prior to providing access, exchange, or use of electronic health information,** the actor may choose not to provide access, exchange, or use of such electronic health information if the precondition has not been satisfied, provided that:

(1) The actor's practice—

(i) Conforms to the actor's organizational policies and procedures that:

(A) Are in writing;

(B) Specify the criteria to be used by the actor and, as applicable, the steps that the actor will take, in order that the precondition can be satisfied; and

(C) Have been implemented, including by taking reasonable steps to ensure that its workforce members and its agents understand and consistently apply the policies and procedures; or

(ii) Has been documented by the actor, on a case-by-case basis, identifying the criteria used by the actor to determine when the precondition would be satisfied, any criteria that were not met, and the reason why the criteria were not met; and

(2) If the precondition relies on the provision of consent or authorization from an individual, the actor:

(i) Did all things reasonably necessary within its control to provide the individual with a meaningful opportunity to provide the consent or authorization; and

(ii) Did not improperly encourage or induce the individual to not provide the consent or authorization.

(3) The actor's practice is:

(i) Tailored to the specific privacy risk or interest being addressed; and

(ii) Implemented in a consistent and non-discriminatory manner.

(c) Health IT developer of certified health IT not covered by HIPAA. If the actor is a health IT developer of certified health IT that is not required to comply with the HIPAA Privacy Rule when engaging in a practice that promotes the privacy interests of an individual, the

actor may choose not to provide access, exchange, or use of electronic health information provided that the actor's practice:

(1) Complies with applicable state or federal privacy laws;

(2) Implements a process that is described in the actor's organizational privacy policy;

(3) Had previously been meaningfully disclosed to the persons and entities that use the actor's product or service;

(4) Is tailored to the specific privacy risk or interest being addressed; and

(5) Is implemented in a consistent and non-discriminatory manner.

(d) Denial of an individual's request for their electronic protected health information in the circumstances provided in 45 CFR 164.524(a)(1), (2), and (3). If an individual requests their electronic protected health information under 45 CFR 164.502(a)(1)(i) or 45 CFR 164.524, the actor may deny the request in the circumstances provided in 45 CFR 164.524(a)(1), (2), or (3).

(e) Respecting an individual's request not to share information. In circumstances where not required or prohibited by law, an actor may choose not to provide access, exchange, or use of an individual's electronic health information if—

(1) The individual requests that the actor not provide such access, exchange, or use;

(2) Such request is initiated by the individual without any improper encouragement or inducement by the actor;

(3) The actor or its agent documents the request within a reasonable time period; and

(4) The actor's practice is implemented in a consistent and non-discriminatory manner.

Exception #3: Promoting the security of electronic health information.

To qualify for this exception, each practice by an actor must meet the following conditions at all relevant times.

(a) The practice must be directly related to safeguarding the confidentiality, integrity, and availability of electronic health information.

(b) The practice must be tailored to the specific security risk being addressed.

(c) The practice must be implemented in a consistent and non-discriminatory manner.

(d) If the practice implements an organizational security policy, the policy must—

(1) Be in writing;

(2) Have been prepared on the basis of, and directly respond to, security risks identified and assessed by or on behalf of the actor;

(3) Align with one or more applicable consensus-based standards or best practice guidance; and

(4) Provide objective timeframes and other parameters for identifying, responding to, and addressing security incidents.

(e) If the practice does not implement an organizational security policy, the actor must have made a determination in each case, based on the particular facts and circumstances, that:

(1) The practice is necessary to mitigate the security risk to the electronic health information; and

(2) 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 electronic health information.

Exception #4: Recovering costs reasonably incurred.

To qualify for this exception, each practice by an actor must meet the following conditions at all relevant times.

(a) Types of costs to which this exception applies. **This exception is limited to the actor's costs reasonably incurred to provide access, exchange, or use of electronic health information.**

(b) **Method for recovering costs.** The method by which the actor recovers its costs:

(1) Must be based on objective and verifiable criteria that are uniformly applied for all substantially similar or similarly situated classes of persons and requests;

(2) Must be reasonably related to the actor's costs of providing the type of access, exchange, or use to, or at the request of, the person or entity to whom the fee is charged;

(3) Must be reasonably allocated among all customers to whom the technology or service is supplied, or for whom the technology is supported;

(4) Must not be based in any part on whether the requestor or other person is a competitor, potential competitor, or will be using the electronic health information in a way that facilitates competition with the actor; and

(5) Must not be based on the sales, profit, revenue, or other value that the requestor or other persons derive or may derive from the access to, exchange of, or use of electronic

health information, including the secondary use of such information, that exceeds the actor's reasonable costs for providing access, exchange, or use of electronic health information.

(c) **Costs specifically excluded.** This exception does not apply to:

(1) Costs that the actor incurred due to the health IT being designed or implemented in nonstandard ways that unnecessarily increase the complexity, difficulty or burden of accessing, exchanging, or using electronic health information;

(2) Costs associated with intangible assets (including depreciation or loss of value), other than the actual development or acquisition costs of such assets;

(3) Opportunity costs, except for the reasonable forward-looking cost of capital;

(4) A fee prohibited by 45 CFR 164.524(c)(4);

(5) A fee based in any part on the electronic access by an individual or their personal representative, agent, or designee to the individual's electronic health information;

(6) A fee to perform an export of electronic health information via the capability of health IT certified to § 170.315(b)(10) of this subchapter for the purposes of switching health IT or to provide patients their electronic health information; or

(7) A fee to export or convert data from an EHR technology, unless such fee was agreed to in writing at the time the technology was acquired.

(d) **Compliance with the Conditions of Certification.**

(1) Notwithstanding any other provision of this exception, if the actor is a health IT developer subject to the Conditions of Certification in § 170.402(a)(4) or § 170.404 of this subchapter, the actor must comply with all requirements of such conditions for all practices and at all relevant times.

(2) If the actor is an API Data Provider, the actor is only permitted to charge the same fees that an API Technology Supplier is permitted to charge to recover costs consistent with the permitted fees specified in the Condition of Certification in § 170.404 of this subchapter.

Exception #5: Responding to requests that are infeasible.

To qualify for this exception, each practice by an actor must meet the following conditions at all relevant times.

(a) Request is infeasible.

(1) The actor must demonstrate, in accordance with paragraph (a)(2) of this section, that complying with the request in the manner requested would impose a substantial burden on the actor that is unreasonable under the circumstances, taking into consideration—

(i) The type of electronic health information and the purposes for which it may be needed;

(ii) The cost to the actor of complying with the request in the manner requested;

(iii) The financial, technical, and other resources available to the actor;

(iv) Whether the actor provides comparable access, exchange, or use to itself or to its customers, suppliers, partners, and other persons with whom it has a business relationship;

(v) Whether the actor owns or has control over a predominant technology, platform, health information exchange, or health information network through which electronic health information is accessed or exchanged;

(vi) Whether the actor maintains electronic protected health information on behalf of a covered entity, as defined in 45 CFR 160.103, or maintains electronic health information on behalf of the requestor or another person whose access, exchange, or use of electronic health information will be enabled or facilitated by the actor's compliance with the request;

(vii) Whether the requestor and other relevant persons can reasonably access, exchange, or use the electronic health information from other sources or through other means; and

(viii) The additional cost and burden to the requestor and other relevant persons of relying on alternative means of access, exchange, or use.

(2) The following circumstances do not constitute a burden to the actor for purposes of this exception and shall not be considered in determining whether the actor has demonstrated that complying with a request would have been infeasible.

(i) Providing the requested access, exchange, or use in the manner requested would have facilitated competition with the actor.

(ii) Providing the requested access, exchange, or use in the manner requested would have prevented the actor from charging a fee.

(b) **Responding to requests.** The actor must timely respond to all requests relating to access, exchange, or use of electronic health information, including but not limited to requests to establish connections and to provide interoperability elements.

(c) **Written explanation.** The actor must provide the requestor with a detailed written explanation of the reasons why the actor cannot accommodate the request.

(d) **Provision of a reasonable alternative**. The actor must work with the requestor in a timely manner to identify and provide a reasonable alternative means of accessing, exchanging, or using the electronic health information.

Exception #6: Licensing of interoperability elements on reasonable and nondiscriminatory terms.

To qualify for this exception, each practice by an actor must meet the following conditions at all relevant times.

(a) **Responding to requests.** Upon receiving a request to license or use interoperability elements, the actor must respond to the requestor within 10 business days from receipt of the request by:

(1) Negotiating with the requestor in a reasonable and non-discriminatory fashion to identify the interoperability elements that are needed; and

(2) Offering an appropriate license with reasonable and non-discriminatory terms.

(b) **Reasonable and non-discriminatory terms.** The actor must license the interoperability

elements described in paragraph (a) of this section on terms that are reasonable and nondiscriminatory.

(1) Scope of rights. The license must provide all rights necessary to access and use the interoperability elements for the following purposes, as applicable.

(i) Developing products or services that are interoperable with the actor's health IT, health IT under the actor's control, or any third party who currently uses the actor's interoperability elements to interoperate with the actor's health IT or health IT under the actor's control.

(ii) Marketing, offering, and distributing the interoperable products and/or services to potential customers and users.

(iii) Enabling the use of the interoperable products or services in production environments, including accessing and enabling the exchange and use of electronic health information.

(2) Reasonable royalty. If the actor charges a royalty for the use of the interoperability elements described in paragraph (a) of this section, the royalty must be reasonable and comply with the following requirements.

(i) The royalty must be non-discriminatory, consistent with paragraph (b)(3) of this section.

(ii) The royalty must be based solely on the independent value of the actor's technology to the licensee's products, not on any strategic value stemming from the actor's control over essential means of accessing, exchanging, or using electronic health information.

(iii) If the actor has licensed the interoperability element through a standards development organization in accordance with such organization's policies regarding the licensing of standards-essential technologies on reasonable and non-discriminatory terms, the actor may charge a royalty that is consistent with such policies.

(3) Non-discriminatory terms. The terms (including royalty terms) on which the actor licenses and otherwise provides the interoperability elements must be non-discriminatory and comply with the following requirements.

(i) The terms must be based on objective and verifiable criteria that are uniformly applied for all substantially similar or similarly situated classes of persons and requests.

(ii) The terms must not be based in any part on:

(A) Whether the requestor or other person is a competitor, potential competitor, or will be using electronic health information obtained via the interoperability elements in a way that facilitates competition with the actor; or

(B) The revenue or other value the requestor may derive from access, exchange, or use of electronic health information obtained via the interoperability elements, including the secondary use of such electronic health information.

(4) Collateral terms. The actor must not require the licensee or its agents or contractors to do, or to agree to do, any of the following.

(i) Not compete with the actor in any product, service, or market.

(ii) Deal exclusively with the actor in any product, service, or market.

(iii) Obtain additional licenses, products, or services that are not related to or can be unbundled from the requested interoperability elements.

(iv) License, grant, assign, or transfer to the actor any intellectual property of the licensee.

(v) Pay a fee of any kind whatsoever, except as described in paragraph (b)(2) of this section, unless the practice meets the requirements of the exception in § 171.204.

(5) Non-disclosure agreement. The actor may require a reasonable non-disclosure agreement that is no broader than necessary to prevent unauthorized disclosure of the actor's trade secrets, provided:

(i) The agreement states with particularity all information the actor claims as trade secrets; and

(ii) Such information meets the definition of a trade secret under applicable law.

(c) Additional requirements relating to the provision of interoperability elements. The actor must not engage in any practice that has any of the following purposes or effects.

(1) Impeding the efficient use of the interoperability elements to access, exchange, or use electronic health information for any permissible purpose.

(2) Impeding the efficient development, distribution, deployment, or use of an interoperable product or service for which there is actual or potential demand.

(3) Degrading the performance or interoperability of the licensee's products or services, unless necessary to improve the actor's technology and after affording the licensee a reasonable opportunity to update its technology to maintain interoperability.

(d) Compliance with conditions of certification. Notwithstanding any other provision of this exception, if the actor is a health IT developer subject to the conditions of certification in §§ 170.402, 170.403, or 170.404 of this subchapter, the actor must comply with all requirements of such conditions for all practices and at all relevant times.

Exception #7: Maintaining and improving health IT performance.

To qualify for this exception, each practice by an actor must meet the following conditions at all relevant times.

(a) Maintenance and improvements to health IT. An actor may make health IT under its control temporarily unavailable in order to perform maintenance or improvements to the health IT, provided that the actor's practice is—

(1) For a period of time no longer than necessary to achieve the maintenance or improvements for which the health IT was made unavailable;

(2) Implemented in a consistent and non-discriminatory manner; and

(3) If the unavailability is initiated by a health IT developer of certified health IT, HIE, or HIN, agreed to by the individual or entity to whom the health IT developer of certified health IT, HIE, or HIN supplied the health IT.

(b) Practices that prevent harm. If the unavailability of health IT for maintenance or improvements is initiated by an actor in response to a risk of harm to a patient or another person, the actor does not need to satisfy the requirements of this section, but must comply with all requirements of § 171.201 at all relevant times to qualify for an exception.

(c) Security-related practices. If the unavailability of health IT for maintenance or improvements is initiated by an actor in response to a security risk to electronic health information, the actor does not need to satisfy the requirements of this section, but must comply with all requirements of § 171.203 at all relevant times to qualify for an exception.