

## ONC Proposes to Define Conduct That is Not Information Blocking Under the Cures Act

---

Thursday, February 14, 2019

The ONC finally released its long-awaited proposed rule to implement the “information blocking” prohibition of the 21st Century Cures Act by identifying conduct that is not information blocking. If finalized, ONC’s proposed rule would have a significant impact on data sharing arrangements and other relationships among health care providers, health IT developers, and other stakeholders. In this *On the Subject*, our experienced team analyzes ONC’s information blocking proposals and suggests practical next steps for the regulated industry.

### IN DEPTH

---

#### Summary

On February 11, 2019, the Office of the National Coordinator for Health Information Technology (ONC) released its long-awaited proposed rule (Proposed Rule) that, among other things, proposes to implement the “information blocking” prohibition of the 21st Century Cures Act (the Cures Act) by identifying conduct that is not information blocking. On the same day, the Centers for Medicare and Medicaid Services (CMS) released a proposed rule on related interoperability issues. We are covering the CMS proposed rule in a separate *On the Subject*. If finalized, ONC’s proposed policies would have a significant impact on data sharing arrangements and other relationships among health care providers, health IT developers, and other stakeholders.

More broadly, these two rules emphasize the administration’s focus on ensuring patient access to data and data exchange. As CMS Administrator Seema Verma recently explained, “[t]he days of holding patient data hostage are over...Our proposed rule includes a policy to publicly identify doctors, hospitals, and other healthcare providers who engage in information blocking. Simply put, we’re going to expose the bad actors who are purposely trying to keep patients from their own information. Patient data doesn’t belong to the doctor, hospital, or electronic health record. It belongs to the patient.” ONC’s Proposed Rule reflects a similar sentiment.

The public will have 60 days to submit comments following official publication of the Proposed Rule in the Federal Register, which we expect to occur in the near future.

The following sections of this *On the Subject* address:

- The events leading up to the adoption of the Cures Act and the Proposed Rule;
- Discussion and analysis of the information blocking provisions of the Proposed Rule, including its exceptions describing permissible conduct under the Proposed Rule; and
- Practical impact and next steps for health care industry stakeholders.

#### A. Background

Since passage of the Health Information Technology for Economic and Clinical Health Act in 2009, the federal



Article By [Daniel F. Gottlieb](#)  
[James A. Cannatti III](#) [Scott Weinstein](#)  
[Karen S. Sealander](#) [Edward G. Zacharias](#)  
[Rachel Stauffer](#) [McDermott Will & Emery](#)  
[On the Subject](#) [Administrative & Regulatory](#)  
[Communications, Media & Internet](#)  
[Health Law & Managed Care](#)  
[All Federal](#)

government has invested billions of dollars to encourage the adoption of interoperable technologies in the hope that it will lead to better care and a more efficient health care system. Congress, regulators and health care industry stakeholders, have grown concerned that, despite increased adoption of technology, like electronic health record (EHR) systems, certain economic and market conditions create an incentive for some to inappropriately limit or restrict the flow of electronic health information in ways that undermine the significant investment; this conduct is commonly referred to as “information blocking.”

In 2014, Congress asked ONC to research information blocking and devise a strategy to address it. In response, ONC issued an April 2015 [Report to Congress on Health Information Blocking](#) (the Report to Congress). In its Report to Congress, ONC defined information blocking as “knowingly and unreasonably interfer[ing] with the exchange or use of electronic health information.” ONC acknowledged that not all knowing interference was improper information blocking. According to ONC, to distinguish between permissible and inappropriate limitations on the flow of information, there must be a balance of various public policy considerations, including:

- Availability of electronic health information;
- Protection and promotion of patient safety;
- Ensuring privacy and security; and
- Protection of legitimate economic interests and incentives to spur innovation and competition in order to benefit society.

ONC also acknowledged that there are certain systemic barriers that impede the flow of electronic health information that are beyond the control of any particular actor, and thus do not raise information blocking concerns. Determining whether a particular practice constitutes information blocking requires a facts and circumstances analysis.

But to what end? One of the key findings in ONC’s Report to Congress was that enforcement authority gaps that would require congressional intervention prevented the federal government from addressing effectively inappropriate information blocking conduct. That changed with the 2016 passage of the Cures Act. Section 4004 of the law specifically establishes a definition of information blocking that is similar to, but more detailed than, the definition ONC developed in its Report to Congress.

The Cures Act requires the Secretary of Health and Human Services (HHS) to identify, through rulemaking, “reasonable and necessary” activities that are not information blocking under the Cures Act (*i.e.*, exceptions). ONC’s Proposed Rule is an important step in fulfilling that requirement. While ONC writes the rules, the Cures Act grants the HHS Office of Inspector General (OIG) the authority to investigate claims of information blocking.

The Cures Act also authorizes the OIG to assess significant penalties of up to \$1 million per violation—adjusted from time to time for inflation—against certain health IT developers, health information exchanges (HIEs) and health information networks (HINs) that engage in information blocking and to refer certain health care providers to an appropriate agency for “appropriate disincentives.” However, OIG has signaled that it is not planning on pursuing information blocking as a standalone issue until ONC completes its rulemaking and clarifies the scope of the Cures Act’s information blocking prohibition. However, once finalized, ONC’s rule will form the legal basis of OIG’s assessment of whether conduct constitutes information blocking and whether it meets an exception when OIG begins investigative and enforcement actions.

The Proposed Rule is notably sparse in its discussion of “appropriate disincentives,” leaving one to wonder what exactly the penalty will be for health care providers that engage in information blocking. ONC solicits feedback on disincentives generally and, without specifically identifying them, on whether modification of existing disincentives available under HHS programs and regulations would more effectively deter information blocking. ONC could perhaps defer to CMS the responsibility of implementing “appropriate disincentives” for information blocking through conditions of participation and downward payment adjustments through the Promoting Interoperability program for hospitals and downward payment adjustments for physicians and other health care professionals participating in the Medicare Quality Payment Program.

## **B. ONC’s Proposed Rule—Information Blocking**

The Proposed Rule addresses a number of topics, including establishment of conditions and maintenance of certification (including related to information blocking) and voluntary certification for pediatric health IT, modification of certification criteria and the certification program, and establishment of exceptions to the Cures Act prohibition on information blocking. This On the Subject addresses the information blocking provisions.

### **1. Who is subject to the Information Blocking Prohibition?**

The Proposed Rule identifies those parties subject to the information blocking prohibition (referred to as “actors”), including: health care providers, health IT developers, HIEs and HINs. Notably, ONC proposes to define HIN broadly enough to include health systems or other health care providers that enable, facilitate or control the flow of information among unaffiliated individuals and entities. This is important because different penalties apply to different categories of actors. Under the law, health IT developers, HIEs and HINs are potentially subject to fines of up to \$1 million per violation but health care providers are not. Rather, health care providers are potentially subject to “appropriate disincentives.” Health care providers that meet ONC’s broad definition of HIN, however, would face the same significant civil monetary penalties as health IT developers and HIEs.

## 2. What Information Is Protected?

ONC proposes a broad definition of electronic health information (EHI), to which the information blocking prohibition applies. EHI includes data that is electronic protected health information (EPHI) under the HIPAA regulations as well as other electronic individually identifiable health information. Thus, health information de-identified in accordance with the HIPAA Privacy Rule would not be EHI for purposes of the Proposed Rule and thus would not be subject to the prohibition on information blocking.

In the Proposed Rule, ONC requests input on “the parameters and implications of including price information within the scope of EHI for purposes of information blocking.” ONC also notes the broader HHS interest in the subject of price transparency and solicits feedback on an extensive series of questions. This area seems ripe for public comment.

## 3. Practices Likely to Interfere with Access, Exchange and Use of EHI

In its preamble discussion, ONC identifies five categories of practices that it considers likely to interfere with access, exchange or use of EHI, thus implicating the information blocking prohibition of the Cures Act. The categories are:

- **Restrictions on Access, Exchange or Use:** Such restrictions could be formal, like those that are expressed in the organization’s policies or license terms. ONC offers a number of examples of formal restrictions, including a situation in which an EHR developer’s software license terms prohibit its customer from sharing technical interoperability information with the customer’s IT contractor, effectively prohibiting the customer and its IT contractor from efficiently exporting and converting EHI for use in other applications. In addition, restrictions can be informal, arising from general practice or on an *ad hoc* basis. ONC describes a practice by which a health system supports its decision not to exchange EHI with unaffiliated providers by incorrectly claiming that HIPAA or other legal requirements prohibit such an exchange.
- **Limiting or Restricting the Interoperability of Health IT:** Among others, practices in this category include disabling or restricting the use of a capability that shares EHI with users of outside systems. An example of this would be a hospital that has its EHR developer configure the EHR in a way that limits users’ ability to easily send relevant information to unaffiliated providers, even when the user has information necessary to send that information (e.g., a Direct address or other identifying information).
- **Impeding Innovation and Advancements in Access, Exchange or Use of Health IT-Enabled Care Delivery:** Practices in this category include refusals to license interoperability elements when a person would require those elements to provide interoperable services, such as a health IT developer refusing to license its application programming interface (API) that provides access to EHI for continuity of care or other activities permitted by applicable law.
- **Rent-Seeking and Other Opportunistic Pricing Practices:** These practices include those that, according to ONC, artificially increase costs for accessing, exchanging and using EHI, such as a situation in which an EHR developer charges fees to provide an interface that exceeds the actual costs the developer reasonably incurs to provide that interface to its customer.
- **Non-Standard Implementation Practices:** Arises in the situations when generally accepted technical standards that could be used to achieve the objective exist, but the actor does not implement them. For example, an EHR developer uses Consolidated-Clinical Document Architecture (C-CDA) to receive transition of care summaries but only sends them in a proprietary format.

A word of caution concerning the above-described practices: As ONC acknowledges, a practice that seems to implicate the information blocking prohibition may not necessarily violate it because, for example, it could be required by law, fail to meet one or more elements of the definition of information blocking or meet an exception. Each situation requires careful consideration of the specific facts.

## 4. The Exceptions

As a starting point, *ONC takes the position that actors covered by the information blocking prohibition must share EHI unless otherwise prohibited by law or the practice meets an exception to the prohibition.* ONC then proposes the following seven limited exceptions for “reasonable and necessary” practices that would not constitute information blocking for purposes of the Cures Act:

**(1) Preventing Physical Harm to Patients and Others:** ONC proposes to protect practices that reduce the likelihood of patient harm or harm to another individual. This exception would only be available for addressing harm that arises from corrupt or inaccurate data, patient misidentification or misidentification of a patient’s EHI or when, in the professional judgment of a licensed health care professional, disclosure of information is likely to present a danger to the patient or another person. In order to be protected, the practice would have to implement an organizational policy that met a number of conditions (*e.g.*, it is in writing, based on relevant expertise, implemented consistently and in a non-discriminatory manner, and not broader than necessary). Alternatively, the practice would have to result from the actor finding, on a case-by-case basis, that the practice is necessary to mitigate a risk of harm. When implementing a case-by-case decision to not share data, the actor must implement the practice to address the specific case, and the practice must not any broader than necessary.

**(2) Promoting Privacy of EHI:** ONC proposes to protect practices that meet one of the four following separate and limited sub-exceptions designed to promote the privacy of EHI: (1) unsatisfied legal preconditions to the release of EHI; (2) documented and transparent privacy policies by those that are not regulated by HIPAA; (3) denying an individual’s request for access to their EPHI, consistent with the HIPAA Privacy Rule; and (4) honoring an individual’s privacy preferences. Each sub-exception includes additional conditions that would have to be met for protection to apply.

**(3) Promoting Security of EHI:** ONC proposes to protect practices that directly relate to protecting the security (that is, the confidentiality, integrity, and availability) of EHI. The practice would have to be tailored to the security risk, implemented consistently and in a non-discriminatory manner and be either consistent with an organizational security policy that meets certain conditions or result from an actor determining, on a case-by-case basis, that the practice is necessary and no reasonable or appropriate alternative exists.

**(4) Recovering Costs Reasonably Incurred to Provide Access, Exchange or Use of EHI:** ONC proposes to allow recovery of costs that an actor reasonably incurs to provide access, exchange or use of EHI as well as a reasonable profit. As with the other exceptions, a number of specific conditions must be met for this protection to apply.

For example, the method used to recover the costs must: be based on objective and verifiable criteria, uniformly applied for similarly situated people/requests; be reasonably related to the actor’s costs; be reasonably allocated among relevant customers; not be based on competitive considerations; and not be based on sales, profit, revenue or other value that the requestor or other party may derive from the access, exchange or use (including secondary use) that exceeds the actor’s reasonable costs for providing such access, exchange or use of EHI. Additionally, ONC would explicitly exclude the following costs from potential protection under the exception:

- Costs that an actor incurs because it designed or implemented health IT in non-standard ways;
- Costs associated with intangible assets other than actual development and acquisition costs;
- Opportunity costs (other than forward-looking cost of capital);
- Fees prohibited under the HIPAA Privacy Rule for individual requests for access to their protected health information;
- Fees based in any way on electronic access by individuals (or their personal representatives, agents or designees) to the individual’s EHI;
- Fees to export EHI to switch health IT or provide EHI to patients, if done through a capability certified to the new certification criterion concerning EHI export; and
- Fees to export or convert data from an EHR, unless the parties had agreed to the fee at the time the EHR was acquired.

In addition, this exception requires developers of health IT modules that are subject to new conditions of certification related to EHI export and APIs, as well as providers of data through an API (API Data Providers) to comply with proposed new conditions of certification as a condition of meeting this exception.

The condition of certification for APIs permits only three types of fees: (1) fees to recover reasonably incurred development, deployment and upgrade costs; (2) fees to recover reasonably incurred incremental costs for supporting use of the API for purposes other than patient access, subject to certain limitations; and (3) fees for value-added services supplied in connection with software that can interact with the API as long as those services are not necessary to develop or deploy the software.

Under the condition of certification, all such fees charged by a health IT developer that offers an API (API Technology Supplier) and API Data Providers must also meet general conditions aimed at ensuring that the fees are: (1) based on objective and verifiable criteria that are uniformly applied; (2) reasonably related to the API Technology Supplier's or API Data Provider's costs, which must be reasonably allocated among all relevant customers; and (3) not based on competitive considerations.

Note that, although the regulatory text for the exception for recovering costs references "costs" only, the preamble discussion makes clear that the amount charged may include a reasonable profit and still fit within the exception. Specifically, in its preamble to the Proposed Rule, ONC states that "complying with the requirements of this exception would not prevent an actor from making a profit in connection with the provision of access, exchange, or use of EHI. Indeed, the costs recoverable under this proposed exception could include a reasonable profit, provided that all applicable conditions were met." Undoubtedly, stakeholders will wonder what profit margin is "reasonable." Like beauty, reasonableness will be in the eye of the beholder unless ONC provides further guidance.

Additionally, ONC cautions in the preamble guidance that API Technology Suppliers and API Data Providers subject to the API condition of certification must comply with those specific cost accountability provisions in addition to the general limitations included in the exception. The interaction between the cost recovery exception and the cost accountability provisions for the API conditions of certification appear to be another ripe area for public comment.

**(5) Responding to Infeasible Requests to Provide Access, Exchange or Use of EHI:** ONC's fifth proposed exception acknowledges that some requests for access, exchange or use may be infeasible due to considerations identified by ONC, such as the type of data requested and the cost to the actor of complying with the request in the manner requested. To receive protection, an actor would have to demonstrate that complying with the request in the manner requested would be an unreasonable burden. ONC also notes that certain circumstances—namely those where responding to the request would facilitate competition with the actor or prevent the actor from sharing a fee—would not be considered a burden for the actor. The exception would require timely responses to all requests, a written explanation of reasons why the request could not be accommodated, and an effort by the actor to work with the requesting party to identify and provide a reasonable, alternative method for addressing the request.

**(6) Licensing Interoperability Elements:** ONC proposed another fee-based exception that would protect reasonable royalty fees associated with licensing and use of interoperability elements. ONC's definition of "interoperability elements" includes any means by which EHI can be accessed, exchanged or used, and ONC clarifies that the definition is not limited to functional elements and technical information, but also includes technologies, services, policies and other conditions necessary to support the access, exchange or use of EHI. To receive protection under this exception, the actor would have to respond to requests within a specified period (*i.e.*, 10 business days) by negotiating in a reasonable and non-discriminatory fashion to identify the elements needed and to offer a license with reasonable and non-discriminatory terms. ONC sets out parameters concerning such terms that relate to, among other things, the scope of rights to be licensed, the royalty that would be permitted, collateral terms, and non-disclosure agreements that only narrowly protect unauthorized disclosure of the actor's trade secrets. ONC also proposes prohibiting certain actions from the actor and requires, to the extent applicable to a particular health IT developer, compliance with newly proposed conditions of certification related to assurances, communications, and APIs. For some, this will mean that additional limitations on the fees that can be charged for products or services that would otherwise fall into the definition of interoperability elements.

We expect actors to have many questions regarding whether common license agreement terms are reasonable and non-discriminatory. For example, limitations of liability and indemnification provisions allocating risk for data security breaches are often contentious and subject to varying views of commercial reasonableness, particularly in contexts where compensation is cost-based.

**(7) Maintaining and Improving Performance of Health Information Technology:** The final proposed exception would permit making health IT temporarily unavailable for maintenance or improvement purposes, subject to certain limitations. Importantly, if the health IT downtime related to preventing risk of harm to patients or others or security issues, actors would have the option of either meeting the requirements of this exception, or meeting the privacy- or security-related exception, as applicable, described above.

## C. Practical Impact and Next Steps

The policies proposed in ONC's Proposed Rule, if finalized, would have a significant impact on a broad cross-section of the health care industry. ONC is seeking feedback on its proposals and those affected should leverage the opportunity to share what they think about ONC's proposals, both favorably and unfavorably, to help inform ONC's final policy decisions. In addition to commenting on the proposed policies related to information blocking, ONC requests input on other topics covered in the rule, such as health IT and opioid use disorder prevention treatment, patient matching and exchange with registries.

Beyond identifying issues to comment on during the 60-day comment period, there are a number of practical steps that an impacted stakeholder might consider in response to ONC's proposed information blocking policies:

- Evaluate existing policies and procedures, including those related to privacy and security, to determine how they stack up to ONC's proposed exceptions. Doing so can help identify gaps between existing policies and the detailed requirements of ONC's proposed exceptions. For example, API Technology Suppliers and API Data Providers might consider developing written policies and procedures that specifically address the privacy and security conditions they have put in place for permitting access to their APIs and meeting ONC's requirements.
- Consider whether to revise existing information security risk assessment and risk management policies and practices since actors must tailor their security measures to address specific risks related to the access, exchange or use of EHI through interoperability elements in order to avoid accusations that the actor is illegitimately citing security concerns to engage in information blocking.
- Consider the potential need to refine or restructure the terms of existing or template agreements affecting access to EHI in order to ensure that practices and agreement terms fit within ONC's proposed exceptions. For example, ONC's information blocking exceptions and conditions of certification constrain the fees that can be charged, and place limits on technology downtime. These new limitations may require contract modifications.
- Begin gathering records of expenditures and other information to support pricing for APIs and other technology that must employ cost-based pricing.

Remember that each exception has a number of conditions, all of which must be met for protection to apply. The exceptions are replete with terms like "reasonable," which are anything but bright-lined. Regulated individuals and entities need to be wary of the potential trap that can result from complex and multi-conditioned exceptions. Failure to meet one of the conditions fully could result in exposure to potentially significant liability.

We encourage impacted stakeholders to submit public comments on ONC's Proposed Rule.

© 2019 McDermott Will & Emery

**Source URL:** <https://www.natlawreview.com/article/onc-proposes-to-define-conduct-not-information-blocking-under-cures-act>